الممارســـات الآمنة
عبر شبكة الإنترنت

دليل للمدارس المتوسطة والثانوية

تأليف

دوغ فودمان مارجي مونرو

ترجمه ونشره باللغة العربية
مكتب التربية العربي لدول الخليج
الرياض ١٤٣٣هـ / ٢٠١٢م

فهرسة مكتبة الملك فهد الوطنية:
مكتب التربية العربي لدول الخليج
الممارسات الآمنة عبر شبكة الإنترنت دليل للمدارس المتوسطة والثانوية / دوغ فودمان، مارجي مونرو – الرياض، ١٤٣٣هـ
ص، سم
ردمك: ٩-٤٧٤-١٥-٩٩٦٠-٩٧٨
١-شبكات الحواسيب. ٢-الحواسيب والتعليم.
أ.مونرو، مارجي (مؤلف مشارك). ب. العنوان

ديوي ٠٠٤.٤٦٥ ١٤٣٣/٩٠٤٨

رقم الإيداع: ١٤٣٣/٩٠٤٨
ردمك: ٩-٤٧٤-١٥-٩٩٦٠-٩٧٨

الناشر

مكتب التربية العربي لدول الخليج
ص. ب (٩٤٦٩٣) – الرياض (١١٦١٤)
تليفون: ٤٨٠٠٥٥٥ – فاكس ٤٨٠٢٨٣٩
www.abegs.org
E-mail: abegs@abegs.org
المملكة العربية السعودية

C

First published 2008

المحتويات

تقديم

يسعى مكتب التربية العربي لدول الخليج منذ نشأته إلى تنمية العملية التربوية وإثرائها من خلال نقل التجارب والنظريات الحديثة المطروحة في الساحة العالمية إلى اللغة العربية.

ولتحقيق هذا الهدف قدم المكتب للمكتبة التربوية العربية العديد من الإصدارات التي أثرت العملية التربوية, ويأتي كتاب " الممارسات الآمنةعبر شبكة الإنترنت: دليل للمدارس المتوسطة والثانوية", الذي يسعدنا اليوم تقديمه لقراء العربية, في إطار هذا الاهتمام المتواصل, الذي يدعم أداء المعلمين والمعلمات والباحثين والباحثات التربويين عن طريق تزويدهم بخبرات متنوعة تعينهم على أداء عملهم بأسلوب علمي.

يقدم كتاب " الممارسات الآمنة عبر شبكة الإنترنت " نصيحة عملية لمساعدة الطلاب على البقاء بأمان لدى تواجدهم على شبكة الإنترنت من خلال اتخاذ خيارات أفضل لتقليل مخاطر الشبكة. إن الهدف من هذا الدليل هو مساعدة طلبتك على فهم كافة المسائل ذات الصلة ويكونون " أذكى على الشبكة الإلكترونية."

ومكتب التربية العربي لدول الخليج إذ يسعده تقديم هذا الكتاب إلى قراء العربية، فإنه يأمل أن يكون مرشدًا ودليلاً للطلاب والمعلمين والمعلمات والباحثين والباحثات التربويين وأولياء الأمور، الذين يعملون مع الأطفال الصغار.

وفي الختام لا يفوتني أن أشيد بالجهد الطيب الذي بذلته دار خضر الدولية للترجمة في ترجمة الكتاب , حتى جاء بالصورة التي هو عليها, فلهم مني جزيل الشكر والتقدير.

والله ولي التوفيق.

د. علي بن عبد الخالق القرني

مؤلفا الكتاب

منذ عام ١٩٩٧م، عمل كل من مارجي مونرو ودوغ فودمان مع مدارس المرحلة الابتدائية والإعدادية (المتوسطة) والثانوية في أنحاء البلاد لمساعدة المعلمين والمديرين وأولياء الأمور والأطفال على فهم العديد من المسائل التي تؤثر في الاطفال لدى تواجدهم على الشبكة الإلكترونية والتعامل معها. ولعدة سنوات، قاموا بإجراء استطلاعات للرأي وجمعوا البيانات المتعلقة بسلوك الأطفال والمراهقين على الشبكة الإلكترونية. نشر فودمان بعض نتائج تلك البيانات في خريف عام ٢٠٠٦م على .IndependentTeacher.org، والموقع الإلكتروني لمونرو وفودمان، و ChildrenOnline.org ، مما يدعم عملهم مع أولياء الأمور والمدارس.

دكتور دوغ فودمان

عمل دوغ فودمان مديرًا للتكنولوجيا في مدرسة Brookwood، والتي تحوي صفوفًا من مرحلة ما قبل رياض الأطفال إلى الصف الثامن في مانشستر Manchester، ماساشوستس Massachustts، منذ العام ١٩٩٦م. بالإضافة إلى ذلك، قام بتعليم علوم المدرسة الثانوية من (١٨) سنة، منذ عام ١٩٧٩م، وعمل كمدير للتكنولوجيا في مدرسة Pingree في جنوب هاملتون South Hamilton، ماساشوستس Massachustts. و قام بورش عمل حول سلسلة متنوعة من المواضيع ذات الصلة، مثل استخدام محركات البحث بشكل فاعل، وحماية الخصوصية أثناء التواجد على شبكة الإنترنت، والتعاون في مجال الاتصالات.

كان فودمان ضيفًا متحدثًا في العديد من البرامج الإذاعية، ومن ضمنها WBZ في بوسطن، وWLSAM في شيكاغو، وظهر في الأخبار المسائية على شبكة تلفزيون CBS وتحدث فيها حول موضوع خدع الهاتف المحمول التي تستهدف الأطفال بالإضافة إلى مسائل تؤثر في الأطفال أثناء تواجدهم على شبكة الإنترنت.

مارجي مونرو

مارجي مونرو هي موظفة عيادة إجتماعية ومعلمة في المدارس لأكثر من عشرين عامًا في الاستشارات والبرمجة والتدريس. عملت سابقا كعميدة لشؤون الطلبة في مدرسة ستونلاي – بيرنهام Stoneleigh-Burnham في جرينفيلد Greenfield، ماساشوستس Massachustts. كما شغلت منصب مديرة الاستشارات في خمس مدارس من ضمنها بيكنهام براون Buckingham Browne ومدرسة نيكولس Nichols في كامبريدج Cambridge، ماساشوستس Massachustts.

كما عملت كمستشارة ومنسقة لمادة سوء المعاملة في جامعة وايتنبيرغ Wittenberg University في سبرينغ فيلد Springfield، أوهايو Ohio، وكمديرة تنفيذية في مركز الشباب Youth Center في وينيتيكا Winnetka، إلينوا Illinois.

وخلال مسيرتها المهنية، درست مونرو علم النفس التقييمي المتقدم واللغة الإنجليزية وكما طورت مناهج حول التربية الجنسية و سوء المعاملة والأخلاق واتخاذ القرار.

نبذة حول
الجمعية الدولية للتكنولوجيا
في التعليم ISTE

الجمعية الدولية للتكنولوجيا في التعليم ISTE هي المصدر الموثوق للتطوير المهني وتوليد المعرفة والدعم والقيادة للابتكارات وهي الجمعية الأولى في عدد الأعضاء بالنسبة للمدرسين وقادة التربية المشاركين في تحسين التدريس والتعلم بترقية الاستخدام الفاعل للتكنولوجيا في التعليم من مرحلة رياض الأطفال إلى الصف الثاني عشـــــر وإعداد المدرسين.

و الجمعية هي مقر معايير التكنولوجيا التعليمية الوطنية National Educational Technology Standards والمؤتمرات والمعارض السنوية (والمعروفة رسميًّا بـ NECC) وتمثل الجمعية أكثر من (٨٥.٠٠٠) ألف مهني في أنحاء العالم. وتدعم أعضاءها بالمعلومات وفرص التواصل والتوجيه عندما يواجهون تحدي تحويل التعليم. من أجل معرفة المزيد حول مبادرات هذه ، يرجى زيارة الموقع التالي:www.iste.org.

وكجزء من رسالة الجمعية الدولية للتكنولوجيا في التعليم ISTE، تعمل دار النشر التابعة لها مع مربين ذوي خبرة لتطوير وإنتاج مصادر عملية لمدرسي الصفوف ومدربي المدرسين وقادة التكنولوجيا. وتراجع كل مسودة كتاب نختاره للنشر مراجعة دقيقة وتحرر على نحو مهني. نحن نبحث عن المحتوى الذي يركز على الاستخدام الفاعل للتكنولوجيا حيث يمكنها إحداث فرق – مما يزيد في إنتاجية المعلمين والمديرين؛ ومساعدة الطلاب في أساليب التعلم الفريدة من نوعها والقدرات أو الخلفيات المرجعية؛ وجمع واستخدام البيانات لاتخاذ القرار على متسويات المدرسة ومديرية التربية والتعليم؛ وإيجاد بيئات التعلم الحيوية والمرتكزة على المشروع التي تربط معلمي القرن الواحد والعشرين. ونقدر آراءكم في هذا الكتاب وغيره من منتجات الجمعية الدولية للتكنولوجيا في التعليم ISTE الأخرى على البريد الالكتروني: books@iste.org

الافتتاحية

يحتوي هذا الدليل على مئات الروابط للمواقع الإلكترونية والوثائق والمصادر المتوافرة على شبكة الإنترنت. ونظرًا للطبيعة الديناميكية للشبكة الإلكترونية، لا يمكننا تجنب كون بعض الروابط في هذا الكتاب لم تعد تعمل. نعتذر عن ذلك. إذا وجدت أن عنوان موقع على الإنترنت (URL) غير فعال، الرجاء إبلاغنا بذلك من خلال إرسال بريد إلكتروني لنا على العنوان التالي: BrokenLink@ChildrenOnline.org.

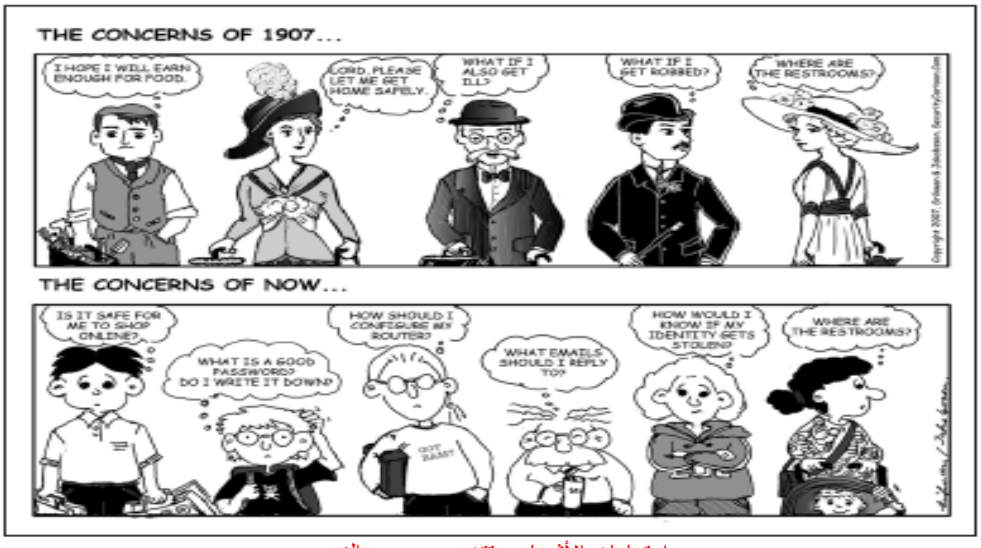
وقد تم إنشاء منطقة محمية بكلمة مرور لموقعنا الإلكتروني (www.ChildrenOnline.org) والتي تحتوي على عناوين مواقع على الإنترنت (URLs) والمتضمنة في هذا الكتاب والتي تم تنظيمها في كل فصل على حدة. إن كلمة المرور هي: 7xStG!972H. سوف نبذل أقصى جهودنا لاستبدال الروابط المعطلة فور الإبلاغ عنها وإضافة مصادر إضافية.

دوغ فودمان ومارجي مونرو
المؤلفان والمديران المشاركان في ChildrenOnline.org.

المقدمة

بدأ طلابك بلا شك لقدسماع أمور تتعلق بالسلامة على الشبكة الإلكترونية بمجرد بلوغهم العمر المناسب لقضاء الوقت على الشبكة الإلكترونية. لكن قد لا يدركون أنهم يخاطرون لدى استخدامهم الإنترنت تمامًا مثل عبور شارع مزدحم بالسيارات، أو ركوب دراجة، أو ممارسة رياضة، أو قيادة سيارة. قد يعتقد العديد من الطلاب أن لديهم خبرة كافية في معرفة المخاطر، وأنهم أذكياء لدرجة كافية لتجنبها، ولكن أوضحت الأبحاث بأن هذا ليس هو الحال لمعظم الطلبة، لأن المخاطر قد لا تكون دائمًا واضحة.

يقدم كتاب *الممارسات الآمنة عبر شبكة الإنترنت* نصيحة عملية لمساعدة طلبتك على البقاء بأمان لدى التواجد على الشبكة الإلكترونية من خلال اتخاذ خيارات أفضل وتقليل مخاطرها. إن الهدف من هذا الدليل هو مساعدة طلبتك على فهم *كافة* المسائل ذات الصلة ليكونوا " أذكى على الشبكة الإلكترونية".



اهتمامات الأشخاص تتغير مع مرور الزمن

يمتلك المؤلفان خبرة مجتمعة تبلغ أكثر من خمسين عامًا من العمل مع الطلاب، ومنذ العام ١٩٩٧م يعبران بقولهما" ركزنا اهتمامنا على فهم المسائل المتعلقة بالعمل على شبكة الإنترنت والتي تؤثر على الأطفال والمراهقين. لقد قمنا باستطلاعات للرأي وتحدثنا إلى آلاف الطلبة والمعلمين والإداريين من عشرات المدارس حول مسائل يواجهونها متعلقة باستخدام طلابهم للإنترنت.

نأمل أن تولد التمارين في هذا الكتاب نقاشًا وأفكارًا بين طلابك حول نشاطاتهم على شبكة الإنترنت. في الواقع، لا يفكر العديد من الطلبة حول سلوكياتهم على شبكة الإنترنت. ولهذا السبب، فإنه من المهم جدًّا للطلبة تعلم حماية أنفسهم، وأصدقائهم، وحتى أولياء أمورهم، لأن بعض الآباء لا يعرفون الكثير حول ما في هذا الدليل. سوف يسجل الطلبة الكثير من النقاط في المنزل من خلال تدريس آبائهم حول ما يتعلمونه كالتالي: التوضيح لهم كيفية حماية حاسوبهم المنزلي من الفيروسات؛ أو مساعدتهم على تطوير كلمات سر أكثر أمنًا. سترغب بمحاولة أداء تمارين مع طلابك قبل استخدامها ليصبحوا أكثر اعتيادًا على الدروس وتقليل الروابط المعطلة والنتائج غير المرغوبة.

تهديدات الماضي مقابل تهديدات الوقت الحالي

(تم إعادة طباعتها بعد الحصول على تصريح. للحصول على المزيد من المواد، الرجاء زيارة www.SecurityCartoon.com)

للبدء بتعلم السلامة لدى التواجد على شبكة الإنترنت وتوليد نقاش بين الطلاب، سترغب في مشاهدة عرضين مصورين فيديو تم إنتاجهما من قبل Ad Council. يجب أن تشاهدهما لتحديد ملائمتها لجمهورك. يمكنك العثور عليهما على الموقع الإلكتروني: Cybertipline.com:

- فكّر قبل نشر تعلقيك Think Before You Post (http://tcs.cubertipline.com/psa/BulletinBoard_60.mov)
- الجميع يعرفون اسمك Everyone Knows Your Name (http://tcs.cybertipline.com/psa/Everyone_60.mov)

الفصل الأول

اختيار أسماء المستخدمين وكلمات المرور
Choosing Names and Passwords

كلمات المرور التي يستخدمها معظم الأشخاص ليست أمنة جدا ويمكن "اختراقها" بسهولة من قبل الآخرين.

أسماء المستخدمين

يفشل الطلاب بشكل روتيني في فهم السبب الذي يجعل الأشخاص الآخرين المتواجدين على الإنترنت يحكمون عليهم على الفور إستنادًا على أسماء المستخدمين التي يختارونها لأنفسهم. لا يختلف ذلك عن الأحكام التي يمكن أن يصدرها طلاب الصف عن طالب جديد بالاستناد بشكل كامل على مظهره.

لم يفهم "BoogerDude" لماذا يتم الاستهزاء به على الشبكة الإلكترونية، بينما كانت "Puppygirl32" صغيرة جدًا لمعرفة أن اسم المستخدم الذي اختارته لنفسها قد جعلها هدفًا جذابًا لمن يسيئون استغلال الأطفال. إن العديد من الطلاب ساذجون جدًا أو يافعون أو غير متمرسين لفهم أن الأسماء التي يختارونها لأنفسهم يمكن أن تؤثر كثيرًا في تجاربهم على شبكة الإنترنت.

بالطبع، يفهم العديد منا أن الانطباعات الأولى التي نحصل عليها في الصور قد تكون خاطئة. لا تكشف الطريقة التي ننظر بها أو نلبس بها دائمًا إن كنا نزيهين أو وضيعين أو أصدقاء جيدين. ومع ذلك، لا يحكم الآخرين علينا بما نلبس أو الطريقة التي ننظر بها. الأشخاص في كل مكان، بما فيهم أنت وأنا، يحاولون أن يصدروا أحكامًا. ننظر إلى ملابس إن الأشخاص التي يلبسونها؛ وشعرهم، ومكياجهم الذي يضعونه، والمجوهرات وحتى الطريقة التي يقفون بها أو البسمة، ومن ثم نبني آراءً حولهم. هل هم أشخاص جيدون؟ هل يمكنك الوثوق بهم؟ هل نرغب في أن نكون أصدقاء معهم؟
الحقيقة أننا لا نفهم فعليًا إذا كانت الأحكام التي نصدرها حول الآخرين صحيحة أم لا حتى نتعرف عن قرب على هؤلاء الأشخاص.

التمرين (١-١): الانطباعات الأولى: يطلب من الطلاب مشاركة انطباعاتهم الأولى التي تتعلق باثنين من الأولاد بناء على صورهم. هل يرون أحدهما كطالب ذكي يحصل دائمًا على علامات كاملة دائمًا وهو نجم لامع في فريق لعبة الكروس؟ هل يرون الولد الآخر يعاني صعوبة في مواد متعددة أو يغش باستمرار في الاختبارات؟ هل أحد الولدين شرس الطباع؟ إن النقطة هنا هي أنهم ببساطة لا يمكنهم الحكم بمجرد النظر عليهم.

وبصورة مشابهة، يصدر الأشخاص الأحكام على المتواجدين على شبكة الإنترنت في كل الأوقات، وتستند في أغلب الأحيان على معلومات أقل. عندما يلتقي الطلاب بأحد ما للمرة الأولى على شبكة الإنترنت، فإن الشيء الوحيد الذي سيرونه هو اسم المستخدم. (لا يستخدم معظم الطلاب المحادثة الصوتية أو المرئية للالتقاء بأحدهم للمرة الأولى). يبني الأشخاص آراءهم بناءً على اسم المستخدم قبل التعرف عليهم أكثر، لذلك تعد الأسماء التي يختارها الطلاب في غاية الأهمية.

التمرين (٢-١): ما الذي يوجد في اسم المستخدم؟ يطلب من الطلاب مناقشة سبب كون بعض أسماء المستخدم ضعيفة جدًّا.

سيختار الطلاب في العادة أسماء المستخدمين من أجل الحصول على الانتباه بشكل خاص. وحتى الطلاب اليافعين سيختارون في بعض الأحيان أسماء قد تحتوي على محتوى عامي ومبتذل أو محتوى جنسي أو محتوى ذي تلميحات جنسية من أجل جذب الانتباه إليهم. ومع مجموعة من الطلاب الأكبر سنًّا، تتطلب هذه القرارات الضعيفة منافشة إضافية. هل يحتوى اسم المستخدم على إهانة للنساء أو الرجال؟ لعرق معين؟ إلى الذات؟ إن فتاة تبلغ من العمر ١٤ عامًا واسم المستحدم لديها هو "IMAHottie" قد لا تدرك المخاطر التي تقوم بها باستخدام ذلك الاسم. وبينما تتوقع هذه الفتاة أقوالاً غزلية، فهي غير مستعدة على الصعيد التنموي والعاطفي لملاحظات جنسية حقيقية أو ملاحظات تتحوي على تحرش جنسي والتي تحصل عليها بسبب اسم المستخدم الخاص بها. من المهم معالجة هذه الإهتمامات بطريقة ملائمة لعمر الطلاب الذين تقوم بتدريسهم.

التمرين (١-٣): يمكن أن يجذب اسم المستخدم انتباهًا سلبيًّا: يطلب من الطلاب الأخذ بعين الاعتبار أسماء المستخدمين التي تجتذب التحرش الجنسي أو المضايقة.

تكشف بعض أسماء المستخدمين عن كثير من المعلومات. لا يفهم الطلاب في العادة كيف يمكن أن تكون معلومة صغيرة في منتهى الخطورة. وعلى ذلك، فإن معرفة بأن أحدهم يأخذ دروسًا في الكاراتية أو يعزف على آلة موسيقية يمكن أن يجعل الشخص موضع خطر. إن بعض المتطفلين والآخرين الراغبين بالاستفادة من الأطفال يكونون خبراء في التلاعب، وفي العادة، يستخدمون أسلوب المحاباة مع الأطفال والمراهقين من خلال اكتشاف أمور عنهم والتي يمكن استخدامها لبناء علاقة. إن كل معلومة يجمعها المتطفلون تزودهم بوسائل إضافية للمحافظة على الطفل مرتبطًا بمحادثة وتمنحهم فرصة متنامية في إنشاء علاقة على مستوى أكبر. يجب أن يتعلم الأطفال والمراهقون أن يكونوا حذرين جدًّا في الإفصاح عن المعلومات الشخصية. تظهر الأبحاث أنهم في العادة يقدمون الكثير من المعلومات بسهولة بالغة.

على الإنترنت، يحاول بعض الأشخاص في معظم الأحيان خداع الآخرين من أجل إنفاق الأموال، والقيام بأشياء لا يجب فعلها، أو الإفصاح عن معلومات شخصية يمكن استخدامها بغية الربح أو الكسب. إن أسهل طريقة يعمل بها الغرباء هذا الشيء هو إثارة

فضول الطفل أو اهتمامه بشكل كاف للتحدث معهم. إذا قال أحد الغرباء في التراسل الفوري، أو غرفة محادثة، أو في لعبة على الإنترنت لـ "AndyKarateKid"إنه "يتعلم الكاراتية أيضًا!"، فمن المرجح أن يتكلم آندي Andy مع هذا الغريب بشكل أكثر.

التمرين (١-٤): هل يقدم اسم المستخدم معلومات؟ يطلب من الطلاب كيف يمكن العثور على الكثير من المعلومات حول الأشخاص من أسمائهم.

في عام ٢٠٠٦، الآلاف من مستخدمي MySpace انخدعوا بالكشف عن هويتهم في استخدام MySpace وكلمات المرور بوساطة النقر على رابط لبريد الكتروني ينقلهم إلى صفحة دخول مزيفة لـ MySpace.

إن المعلومات التي يتم منحها على شبكة الإنترنت تساوي قيمتها مالاً. يحتاج الطلاب إلى فهم هذه الحقيقة. على سبيل المثال، يمكن بيع عنوان للبريد الإلكتروني إلى مرسلي الرسائل غير المرغوب فيها والذين يقومون بدورهم بإرسال رسالة إلكترونية غير المرغوب فيها في محاولة لبيع أشياء أو خداع المستلم من خلال الكشف عن أسماء التسجيل وكلمات المرور. إذا كان أحد مرسلي الرسائل غير المرغوب فيها يعلم أن شخصًا على الأرجح يلعب على آلة موسيقية، مثل: التمرين (١-٤) "ViolinGurl" والتي تعني "فتاة الكمان"، ثم يستطيع مرسل الرسائل غير المرغوب فيها تعقب ذلك الشخص برسالة إلكترونية دخيلة أو خدع تركز على موضوع العزف على آلة الكمان. كلما عرف المزيد من الغرباء عن الطلاب، كلما أصبح من السهل التلاعب والاحتيال على الطلاب. وحتى البالغين الذي يشعرون أنهم أذكياء جدًّا على الإنترنت يمكن أن يتعرضوا للخداع والتلاعب.

إن أسماء المستخدمين التي تكشف عن أقل كمية من المعلومات والتي تكون أقل استفزازية أو جذبًا للانتباه تكون هي أفضل الاختيارات. يقدم التمرين (١-٥) – اختيارات جيدة أو سيئة لاسم المستخدم قائمة بأسماء المستخدمين ويطلب من الطلاب مناقشة الخيارات الجيدة والسيئة. (ملاحظة: في الفصل الرابع، سوف نناقش لماذا قد يرغب الطلاب في تجنب استخدام الرموز ١ و I وl و o وO و٠ في أسماء المستخدم.) التمرين (١-٦) – كن ذكيا عندما تختار اسم مستخدم يطلب من الطلاب ابتكار أسماء مستخدمين ومن ثم مناقشة إن كانت الأسماء اختيارات جيدة أو سيئة. قد يندهش الطلاب بما يراه الآخرون في أسمائهم.

كلمات المرور

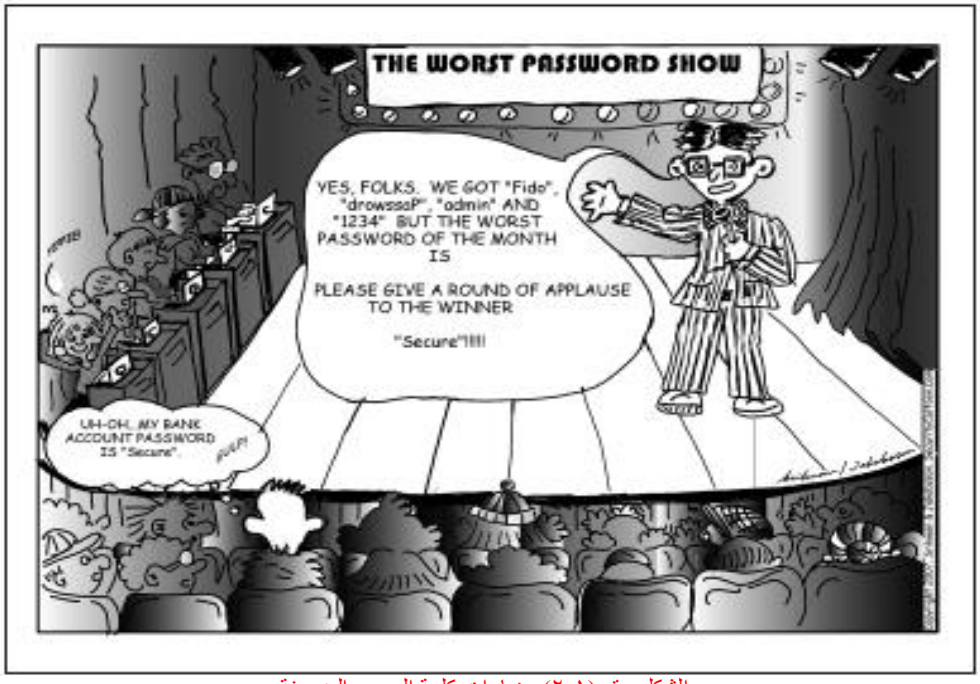
في حياتنا على شبكة الإنترنت، نحتاج إلى كلمات المرور للعديد من الأمور المختلفة. نستخدم كلمات المرور للبريد الإلكتروني، والتراسل الفوري، والمدونات، ومواقع الألعاب، ومواقع التواصل الإجتماعي، وحسابات مشاركة الصور، والـ iTunes، وغيرها من مواقع التسوق. لسوء الحظ، معظم الأشخاص لا يستخدمون كلمات مرور آمنة جدًّا ويمكن بسهولة "اختراقها" من قبل الآخرين. في الحقيقة، إن كلمات المرور المستخدمة

الأكثر شيوعًا بسيطة جدًّا بحيث لا تتطلب سوى القليل من الجهد لمعرفتها. هل يستطيع طلابك أن يحزروا ما كلمات المرور المستخدمة الأكثر شيوعًا؟ وهي:

- أسماء منتخبات البيسبول أو كرة القدم أو كرة السلة.
- تواريخ ميلاد أحد أفراد العائلة.
- سنة حدوث مناسبة رياضية خاصة، مثل السنة التي فازت فيها شرطة شيكاغو Chicago Cubs بلقب البطولة الرياضية.
- كلمة password أو القيام بتغيير بسيط عليها مثل *password1*
- تسلس الأرقام ١٢٣٤٥٦ أو القيام بدمج لحرف/ رقم مثل *abc123* أو *123abc*.
- اسم أحد أفراد العائلة أو حيوان أليف أو شخصية تلفزيونية مفضلة أو شخص مشهور أو علامة تجارية.

الشكل رقم (١-١): مثال على كلمة مرور يسهل معرفتها

توجد برامج مصممة لاختراق حسابات الأشخاص على شبكة الإنترنت. إن هذه البرامج قادرة على تجربة كل كلمة في قاموس اللغة الإنجليزية، وكذلك قواميس اللغات الأجنبية، خلال محاولاتها لاختراق حساب. يمكنها أيضا البحث عن كلمات يتم تهجئتها بالعكس. سوف يحاول البعض بعض تركيبات الكلمات الشائعة أو كلمات مرفق معها أرقام، مثل "school222". يمكن أن تختبر هذه البرامج ملايين كلمات المرور خلال بضع دقائق.



الشكل رقم (١-٢): خيارات كلمة المرور الضعيفة

يمكن أن يستخدم الطلاب الاختبار المقدم في التمرين رقم (١-٧) اختبار كلمة المرور لمشاهدة كيف يمكن اختراق كلمات السر الخاصة بهم وكلمات المرور المستخدمة من قبل أفراد عائلتهم. يمكن بعدها مناقشة نتائج التمرين في الصف. قد يجد الطلاب أنهم بحاجة لابتكار كلمات مرور جديدة.

يمكن أن يتابع طلابك عدة إرشادات بسيطة لابتكار كلمات مرور آمنة جدًّا والتي يكون اختراقها أمرًا في غاية الصعوبة ولكن تذكرها ليس صعبًا جدًّا.

- استخدم دائمًا مزيجًا من الحروف والأرقام.
- استخدم مزيجا من الحروف الكبيرة والصغيرة. معظم كلمات المرور حساسة بالنسبة للحروف.
- استخدم رموزا لا تكون حروفا أو أرقاما، مثل = أو ! أو $ أو #.

لا تسمح بعض المواقع الإلكترونية باستخدام علامات الترقيم في ابتكار كلمات المرور، يجب أن تكون خبيرًا في اكتشاف ما الحروف والأرقام غير المسموحة.

- قم بابتكار اختصارات. إن الاختصار هو عبارة عن كلمة يتم ابتكارها بأخذ الحرف الأول من كل كلمة في تسلسل الكلمات.
- استخدم دائما كلمة مرور تحتوي على ستة رموز أو أكثر. أفضل شيء هو ثمانية!

فيما يلي مثالاً حول كيف يمكن للطلاب ابتكار كلمات مرور آمنة جدًّا، ومع ذلك يمكن تذكرها بسهولة:

١. استخدم أول خمس كلمات من النشيد الوطني للولايات المتحدة الأمريكية – "Oh, say can you see" – من أجل ابتكار الإختصار *oscys*.
٢. قم بإضافة رقمين يعنيان شيئًا لك، مثل رقم الشارع الذي تقطن فيه جدتك.
٣. قم بالتلاعب بالحروف الكبيرة والحروف الصغيرة، قم باستبدال S بـ $، وقم بإضافة = ليصبح الرمز المبتكر كالتالي: *22=oCy*

ومن الأمثلة الأخرى الجيدة:

!mYdoG8it	("My dog ate it" من)
iPa2tf!	("I pledge allegiance to the flag" من)
=u$oA=	("United States of America" من)

قم بتدريس طلابك طرقا أخرى يمكنهم استخدامها لتطوير كلمات مرور آمنة من خلال العمل على التمرين رقم (١-٨) – ابتكار كلمة مرور لا يمكن اختراقها، والتمرين رقم (١-٩)– نفس الإرشادات، كلمات مرورمختلفة، والتي توضح التغييرات المحتملة في ابتكار كلمة مرور. لدى الموقع الإلكتروني PC Tools (www.pctools.com/guide/password) مولد كلمة مرور آمنة والتي تسمح لك بتغيير بعض أجزاء كلمة المرور التي يبتكرها لك. وبمجرد أن يقوم الطلاب بابتكار كلمات المرور الجديدة الخاصة بهم، يمنحهم التمرين رقم (١-١٠) – اختبر كلمة المرور الخاصة بك الفرصة للتحقق من كلمات المرور الخاصة بهم من خلال مدقق قوة كلمة المرور Password Strength Checker في جامعة كورنويل Cornell.

وفيما يلي مشروع يصلح أن يكون واجبًا منزليًا لطلابك. أخبر طلابك بأن مهمتهم هي تعليم أولياء أمورهم أو الأوصياء عليهم ما الذي يجعل كلمة المرور جيدة أو سيئة. أخبرهم بأن يتأكدوا من أن والديهما لا يستخدمان أسماء أطفالهم أو تواريخ الميلاد في أي من كلمات المرور الخاصة بهم. إجعل الطلاب يشجعون أولياء أمورهم على ابتكار كلمات مرور جديدة لحساباتهم على شبكة الإنترنت باستخدام المهارات التي تعلمها الطلاب اليوم. قد يندهش العديد من طلابك من اكتشافهم بأن أولياء أمورهم يمتلكون مهارات ضعيفة في ابتكار كلمات المرور. يساعد هذا المشروع الطلاب على حفظ وممارسة المهارات التي تعلموها في هذا الفصل، كما أنه سيساعد على توليد نقاش في المنزل حول هذه المسائل الأمنية.

قد لا يعلم الطلاب ما الذي يشكل أكبر المخاطر التي تهدد أمنهم على شبكة الإنترنت. التمرين (١-١١)– كيف فعلوا ذلك؟ يطلب من الطلاب الأخذ بعين الاعتبار أكثر وأقل المسائل الأمنية الشائعة للحساب. وخلال هذا التمرين، سوف يكتشف الطلاب أن أكبر تهديد لأمنهم على شبكة الإنترنت يحدث عندما يعطون كلمات المرور الخاصة بهم إلى الآخرين والذي يسيئون استخدامها في حساباتهم. يحدث ثاني أكبر تهديد عندما يختار طالب كلمة مرور يسهل معرفتها.

كما يحتاج الطلاب أيضًا إلى تعلم احترام حاجة الآخرين للخصوصية عندما يدخلون كلمات المرور على جهاز حاسوب. على الرغم من أن برامج اختراق كلمة المرور ليست أكثر تهديد شائع للأمن، نحن نعلم أن بعضًا من طلاب الصف الخامس حاولوا استخدام برامج لإختراق كلمة المرور للوصول إلى حسابات الآخرين على شبكة الإنترنت.

اسأل الطلاب: هل تشاركون بطاقة الائتمان لأولياء أموركم أو معلومات البنك مع أصدقائكم؟ يجب أن يكون الجواب بالتأكيد هو *لا*.

إن كلمات المرور ذات قيمة أيضا أخبر طلابك ألا يجب عليهم مشاركة كلمات المرور الخاصة بهم أيضا! أبدًا!

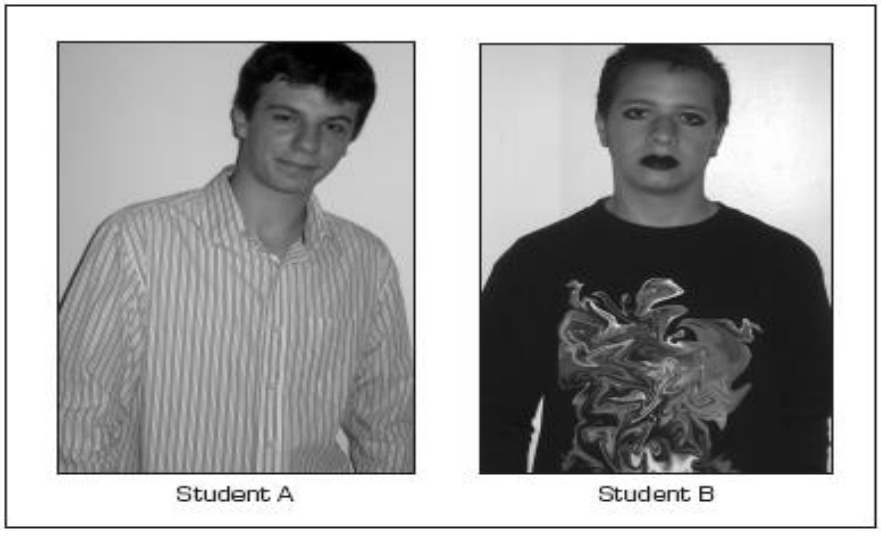
ملاحظتنا النهائية... قم بتحذير طلابك من ألا يستخدموا كلمات المرور الموجودة في هذا الفصل!

التمارين

التمرين (١-١):
الانطباعات الأولى

اطلب من الطلاب إلقاء نظرة على صورتي الطالبين وإعداد لائحة من خمس كلمات يعتقدون أنها الأفضل لوصف كل طالب. قم بإثارة ردود فعل من خلال طرح الأسئلة التالية:

١. أي من الأولاد تعتقد أنه على الأرجح صادق؟
٢. أي من الأولاد تعتقد أنه على الأرجح وضيع؟
٣. أي من الأولاد تعتقد أنه على الأرجح صديق جيد؟
٤. أي من الأولاد تعتقد أنه على الأرجح أفضل طالب في المدرسة؟



الطالب (أ) الطالب (ب)

التمرين (١-٢) :
ما الذي يوجد في اسم المستخدم؟

فيما يلي أسماء مستخدمين حقيقة للطلاب تم استخدامها بالفعل. إسأل طلابك لماذا قد تكون هذه الأسماء اختيارات غير جيدة.

Trashmouth
IHaveOnePairPants
Boogerdude
Pig

التمرين (١-٢) :
يمكن أن تجذب أسماء المستخدمين
انتباهًا سلبيًّا

قد يختار الطلاب في بعض الأحيان أسماء تجذب انتباهًا قد يكون سلبيًّا أو مؤذيًّا أو قد يجعلهم يشعرون بعدم الإرتياح. يمكن أن يشجع اختيار اسم المستخدم الخاطئ الآخرين على معاملتهم بشكل سيء. إن هذا الانتباه السلبي يعد شكلاً من أشكال سوء المعاملة والمضايقة. اسأل طلابك إن كان بإمكانهم معرفة لماذا قد يتضايق أحد أولئك الذي يحملون أسماء مثل:

InYoFace
Badboy2U
Looki4Luv
IMAHottie
FatMama
suPaFlirt

التمرين (١-٤) :
هل يكشف اسم المستخدم أية معلومات؟

في بعض الأحيان يقوم الطلاب باختيار أسماء مستخدمين تكشف الكثير من المعلومات حولهم. اسأل طلابك عن المعلومات التي قد تكشفها الأسماء التالية:

Tom_Evans34
Missy-13
AndyKarateKid
ViolinGurl
restlinmatch

التمرين (١-٥) :
اختيارات جيدة أو سيئة لأسماء المستخدمين

اطلب من طلبتك النظر إلى أسماء المستخدمين التالية. اطلب منهم مناقشة سبب اعتقادهم بأن هذه اختيارات جيدة أو سيئة، واشرح السبب.

AmrcanIdol2	i8sushi2
BellaIsabella	Soccerstar
DarkAnge1666	Puppygir1234
Karla-Love-1996	KeKe1995
SimplyMe	Bookworm
gUn4hiRe	2BorNot2b
babyfaceLA	Choco-holic
Watup?	CapitlOfens

إن SimplyMe، 2BorNot2B، وWatup؟ تعتبر اختيارات جيدة في القائمة. Bookworm، i8sushi، AmrcanIdol2، Soccerstar، و Choco-holic هي أيضًا خيارات جيدة إلى حد ما، ومع ذلك يجب أن نشير إلى أنها تكشف شيئا ما حول اهتمامات المستخدم. أما الأسماء الأخرى في القائمة تعتبر خيارات ضعيفة لأنها استفزازية وتكشف العديد من المعلومات أو قد تجذب انتباها غير مرغوب.

التمرين (١-٦) :
كن ذكيا عندما تختار اسم مستخدم

اطلب من طلابك محاولة ابتكار اسمين مختلفين على الأقل والتي تعتقد أنهما يلبيان كافة التوجيهات التالية:

- لا تجذب على الأرجح انتباهًا سلبيًّا.
- خالية من الكلمات السيئة.
- لا تكشف الكثير من المعلومات الشخصية.
- لا تكشف الإسم الحقيقي أو العمر أو الجنس.

إذا سمح الوقت:

قم بجمع أسماء المستخدمين التي ابتكرها طلابك في هذا التمرين وضعها على اللوح/ الشاشة. اطلب من صفك التصويت على هذه الأسماء التي تعتقد أنها أفضل الخيارات. هل يعتقدون أن أي من أسماء المستخدمين المعلقة كانت خيارات ضعيفة؟ لماذا؟

التمرين (١-٧) :
اختبار كلمة المرور

كيف يمكن اختراق كلمة مرور؟ اطلب من الطلاب تقديم هذا الاختبار الخاص بكلمة المرور لعائلاتهم. يجب أن يسألوا كل فرد في العائلة يستخدم كلمات المرور الأسئلة التالية. يجب أن يواصل الطلاب تعقب نتائجهم. إن النتائج من (٨) وأكثر تعتبر نتائج ممتازة. أما الدرجة الأقل من (٤) فتعتبر ضعيفة جدًّا. إن الدرجة الضعيفة تعتبر تحذيرًا لابتكار كلمة مرور جديدة على الفور. قم بمناقشة نتائج التمرين خلال الحصة الصفية. إن هذا التمرين يعد تمرينًا رائعًا لتوضيح كيف يمكن تطبيق الدروس المستفادة في المدرسة على الحياة في المنزل.

١. هل تتضمن كلمة المرور الخاصة بك اسم أحد أفراد العائلة أو حيوان أليف؟ (-٣).
٢. هل تتضمن كلمة المرور الخاصة بك تاريخ ميلاد أحد أفراد العائلة؟ (-٣).
٣. هل تتضمن كلمة المرور الخاصة بك كلمة واحدة أو أكثر والتي يمكن العثور عليها في قاموس (والتي تتضمن القواميس الفرنسية أو الأسبانية أو الإيطالية أو الألمانية)؟ (-١).
٤. هل تتضمن كلمة المرور الخاصة بك مجموعة أرقام عشوائية؟ (+٢).
٥. هل تتضمن كلمة المرور الخاصة بك حروفا وأرقام؟ (+٢).
٦. هل تتضمن كلمة المرور الخاصة بك ثمانية رموز أو أكثر؟ (+٢).
٧. هل تتضمن كلمة المرور الخاصة بك أقل من ستة رموز؟ (-١).
٨. هل تتضمن كلمة المرور الخاصة بك رمزًا واحدًا أو أكثر من غير الأرقام أو الحروف مثل ! أو =؟ (+٣)
٩. هل تتضمن كلمة المرور الخاصة بك تاريخ حدوث مناسبة خاصة مشهورة، مثل التاريخ الذي فاز به فريق بيسبول معين بالبطولة؟ (-١).
١٠. هل تتضمن كلمة المرور الخاصة بك ثلاثة أرقام على الأقل ذات تسلسل رقمي، مثل "١٢٣"؟ (-٢).
١١. هل تتضمن كلمة المرور الخاصة بك أية كلمة مكتوبة بالعكس؟ (-١).
١٢. هل كلمة المرور الخاصة بك مكتوبة على ورقة تبعد (١٥) قدمًا عن جهاز الحاسوب الخاص بك؟ (-٢).
١٣. هل تتضمن كلمة المرور الخاصة بك كلمة مكررة أكثر من مرة؟ (-١).
١٤. هل تتضمن كلمة المرور الخاصة بك رقم الهاتف الخاص بك، أو رمز بريدي أو رمز المنطقة أو أي جزء منها؟ (-٢).

١٥. هل تتضمن كلمة المرور الخاصة بك مزيجا من الحروف الكبيرة والحروف الصغيرة؟ (+٢).

١٦. هل تشاركت أبدا كلمة المرور الخاصة بك مع صديق؟ (-٣).

التمرين (١-٨) :
ابتكار كلمة مرور لا يمكن اختراقها

اطلب من الطلاب إنشاء كلمة مرور لا يمكن اختراقها من خلال اتباع الإرشادات التالية لهاتين الإستراتيجيتين:

الإستراتيجية الأولى:

١. فكر في سطر من أغنية من خمس أو ست كلمات وقم بكتابتها.
٢. قم بابتكار كلمة اختصار من خمسة أو ستة حروف والتي تتكون من الحرف الأول لكل كلمة في السطر.
٣. قم بتغيير حرف واحد على الأقل (ليس أول حرف) إلى حرف كبير.
٤. قم بإضافة رمز بحيث لا يكون رقما أو حرفا أو بديلا (! تفيد مكان الحرف i، و $ تفيد مكان الحرف s).
٥. قم بإضافة رقمين أو ثلاثة يكون لهما بعض الأهمية الشخصية لك.

الإستراتيجية الثانية

١. فكر في اسم شخصية مشهورة وقم بكتابته.
٢. قم بابتكار كلمة اختصار من أربعة حروف والتي تتكون من أول حرفين من الاسم الأول والأخير للشخص.
٣. قم بتغيير حرف واحد على الاقل (ليس الأول) إلى حرف كبير.
٤. قم بإضافة رمز بحيث لا يكون رقما أو حرفا أو بديلا (! تفيد مكان الحرف i، و $ تفيد مكان الحرف s).
٥. قم بمزجهما مع رقمين من عمرك. لا تضعهما بجانب بعضهما البعض.

التمرين (١-٩) :
نفس الإرشادات، كلمات مرور مختلفة

والآن وبعد أن أصبح لدى طلابك موهبة ابتكار كلمات مرور آمنة، دعونا نرى كيف يمكن ابتكار كلمات مرور مختلفة في صفك عندما يتبع الجميع نفس التعليمات. اطلب من طلابك ابتكار كلمة مرور باتباع هذه الإرشادات:

١. قم بابتكار كلمة مختصرة باستخدام أول حرفين من اسم بلدتك أو مدينتك وقم بدمجهما مع مختصر الولاية التي تقطن فيها.
٢. قم بتحويل واحد من الحرفين إلى حروف كبيرة.
٣. قم بإضافة ثلاثة أرقام من رمز المنطقة الخاص ببلدتك او مدينتك، ولكن لا تستبدل أي رقمين مع بعضهما البعض. يجب ان يتم الفصل بين كل رقم باستخدام حرف.
٤. قم بإضافة أي من الرموز التالية أينما تحب: = ! $.

قم بسؤال طلابك القيام بمقارنة كلمة المرور الخاصة بهم مع كلمات المرور المبتكرة من الطلاب الآخرين في الصف. كم كلمة مرور مختلفة تم ابتكارها؟

التمرين (١-١٠) :
اختبر كلمة المرور الخاص بك

ما مدر جودة كلمة المرور؟ قم بالطلب من الطلاب اختبار كلمات المرور الخاصة بهم، أو كلمة مرور أعجبتهم، باستخدام مدقق قوة كلمة المرور في موقع الآمان الإلكتروني في جامعة كورنيل: http://netid.cornell.edu/NetIDManagement/PasswordCheck/. شجعهم أيضا على النقر على رابط مزايا كلمة المرور.

التمرين (١-١١) :
كيف فعلوا ذلك؟

اطلب من الطلاب الإختيار من القائمة أدناه أكثر سبب مألوف لاختراق حسابات الطلاب على شبكة الإنترنت كل سنة:

- يتم استخدام برنامج اختراق كلمة المرور لاختراق كلمة المرور الخاصة بهم.
- يحزر الآخرون الذي يعرفون أمورًا شخصية عن الطلاب كلمات المرور الخاصة بهم.
- يكتب الطلاب كلمات المرور الخاصة بهم في الوقت الذي يتمكن فيه الآخرين من مشاهدتها.
- يعطي الطلاب كلمات المرور الخاصة بهم إلى أصدقائهم، والذين يفكرون فيما بعد باستخدامها أو إعطائها لآخرين ليستخدموها.
- يرى الطلاب الآخرين كلمة المرور عندما يقوم الطالب بإدخالها على لوحة المفاتيح.

قم بإخبار طلابك بأن أكثر قضايا السلامة شيوعًا للطلاب هي:

- يقوم الطلاب بإعطاء كلمة المرور الخاصة بهم إلى أصدقائهم، والذي يقررون استخدامها أو إعطائها للآخرين ليستخدموها.

قم بإخبار طلابك بأن أقل قضايا السلامة شيوعًا للطلاب هي:

- شخص يستخدم برنامج اختراق كلمة مرور لاختراق كلمات المرور الخاصة بهم.

هل شعر طلابك بالدهشة؟

المصادر

Evers, J. (2006). *Report: Net users picking safer passwords.* Available from ZDNet: http://news.zdnet.com/2100-1009_22-6144312.html

Granger, S. (2002, January 17). *The simplest security A guide to better passwordpractices*. Available from SecurityFocus: www.securityfocus.com/infocus/1537/

Krebs, B. (2007, January 15). *Note to MySpace users: Get better passwords.* Available from WashingtonPost.com: http://blog.washingtonpost.com/securityfix/2007/01/myspace_phishers_hook_hundreds.html

Powerful passwords. (2005, November 2). Available from PCMag.com: www.pcmag.com/article2/0,1895,1880305,00.asp

Scalet, S. D. (2005, December 1). *How to write better passwords*. Available from CSOonline: www.csoonline.com/read/120105/ht_passwords.html

University of Michigan, Information Technology Central Services. (2006,April). *Choosing and changing a secure password*. (R1162). Available from www.itd.umich.edu/itcsdocs/r1162/

الفصل الثاني

حماية خصوصيتك أثناء التواجد
على شبكة الإنترنت
Protecting Your Privacy Online

على شبكة الإنترنت, تعتبر المعلومات الشخصية في غاية الأهمية.

على شبكة الإنترنت، تعتبر المعلومات الشخصية في غاية الأهمية. يقوم كل من الشركات والمسوِّقين والمحتالين ومرسلي الرسائل غير المرغوب بها بكل ما بوسعهم للحصول على انتباه طلابك والمعلومات الخاصة بهم. يكون بعضهم صادقين في الطريقة التي يتبعونها ولكن العديد منهم ليسوا كذلك. قد يكذب بعضهم على الزوار ويحاولون التلاعب بهم للكشف عن معلومات الاتصال الشخصية أو الوصول إلى بطاقات الائتمان العائلية أو مختلف الحسابات على شبكة الإنترنت. يقوم بعضهم بابتكار إعلانات تقوم بتثبيت برامج ضارة للحصول على هذه المعلومات بطريقة مخفية أكثر. لحسن الحظ، يوجد العديد من الأدوات والتقنيات والإقتراحات التي يستطيعون استخدامها لمكافحتهم وحماية خصوصيتهم.

النوافذ المنبثقة والبنرات الإعلانية

في كل مكان على شبكة الإنترنت، نتعرض لهجوم من قبل النوافذ المنبثقة pop-ups والبنرات الإعلانية Banner Ads والتي تحاول جذب انتباهنا: " قم بركوب لوح التزلج وفز بجهاز آيبود iPod ! (الشكل ٢-١) – "لقد فزت للتو بحاسوب محمول!" – "فز بالسباق" (الشكل ٢-٢) – "لقد فزت بأي فون iPhone" – "أنت الفائز رقم ٩.٩٩٩.٩٩٩"! لا يوجد نهاية للقائمة.

هل يفوز أحد ما بالفعل؟

الشكل (٢-١): هل يفوز أحد ما بالفعل بأي بود iPod؟

الشكل (٢-٢): إعلان تفاعلي

قم بإجراء استطلاع للرأي في صفك. قم بسؤال طلابك ما يلي:

١. كم منكم قام بالنقر على إعلان ترويجي أو نافذة منبثقة تقول أنك فزت بأمر ما؟
٢. كم منكم فاز فعليًا بشيء ما؟

لقد طرحنا هذين السؤالين على آلاف الطلاب في المدارس في كافة أرجاء الدولة، وكان الجواب دائمًا هو نفسه: لم يفز أحد بأي شيء مطلقًا.

نرغب جميعًا في أن نصدق بأننا سنفوز بشيء ما، لكن يجب أن يعلم الطلاب بأنه حتى إعلانات "نغمة الهاتف المجانية" التي نحصل عليها على هواتفنا أو نجدها على مئات المواقع الإلكترونية المألوفة هي أيضًا مواقع شبيهة. وقامت دائرة الشؤون الطلابية برفع دعاوي قضائية ضد هذه الشركات مثل بيلينكو Blinko، بوينغيورنو Buongiorno، جامستر Jamster وإم كيوب MQube، بالإضافة إلى العديد من الشركات الأخرى بسبب خصم العملاء مبلغ ٩.٩٩دولارات وأكثر من العملاء على ما يسمى بالنغمات المجانية الخاصة بالأجهزة المحمولة. إن العديد من هذه الشركات التسويقية يخضع للتحقيق في عدد من الولايات بسبب ممارساتهم الخادعة والكاذبة.

التمرين (٢–١) – البنرات الإعلانية والنوافذ المنبثقة: تستخدم مواقع إلكترونية مألوفة لتوجيه العديد من الإعلانات النوافذ المنبثقة المصممة لجذب انتباه المستخدم.
التمرين (٢–٢)– لقد فزت! أو هل فزت؟ يوضح كيف تقوم خطط معينة على شبكة الإنترنت والتي تقدم جوائز باستغلال المستخدم. إن الهدف من التمرينين هو زيادة وعي الطالب حول الحيل الموجودة على شبكة الإنترنت وتؤكد على أهمية السلامة والخصوصية على شبكة الإنترنت.

الشكل رقم (٢-٣): يدعي هذا الإعلان أنه يقدم أجهزة حاسوب محمولة مجانًا

سوف يرى الطلاب من التمرينين الأولين أن كل ما عليهم عمله هو للوصول إلى الخدمات والألعاب والحسابات والمصادر هو مجرد القيام بالتسجيل. وعليه، يعني التسجيل في العادة الإجابة على العديد من الأسئلة الشخصية. التمرين (٢–٣) – المطلوب: معلوماتك الشخصية: يطلب من الطلاب التفكير في ماهية المعلومات التي تحاول الإعلانات الحصول عليها منهم، وكيف يمكن استخدام هذه المعلومات. يشير هذا التمرين إلى كيف أن النوافذ المنبثقة التي تبدو مضحكة وغير مؤذية هي في الحقيقة حيل مصممة بشكل جيد لاستدراجهم للبوح عن معلومات شخصية في غاية الأهمية.

اطلب من طلابك أنه أينما يطلب منهم هذه المعلومات، يجب عليهم القضاء عليها او الامتناع عن الإجابة. قم بتوجيههم لحماية خصوصيتهم من خلال عدم الإفصاح عن العنوان الحقيقي للبريد الإلكتروني أو الاسم أو عنوان المنزل او المدينة أو رقم الهاتف.

الشكل رقم (٢-٤): إعلان تضليلي شائع على شبكة الإنترنت

قم بإخبار الطلاب أنه من السهل اختلاق معلومات حول أنفسهم مثل الاسم والعنوان أو الرمز البريدي. إذا وجد الطلاب أنفسهم بحاجة إلى إدخال رمز بريدي حقيقي، يمكنهم العثور على رمز حقيقي من خلال صفحة البحث عن الرموز البريدية لخدمات البريد الأمريكية (www.usps.com/zip4/). يمكنهم النقر على البحث عبر المفتاح الخاص بالمدينة ومن ثم إدخال اسم مدينة أو ولاية. سوف يمنحهم هذا الخيار رمزًا بريديًّا صالح المفعول.

ولكن، ماذا عن عناوين البريد الإلكتروني؟ إن أسهل طريقة لحماية الخصوصية وفي نفس الوقت الدخول إلى المواقع الإلكترونية والمصادر التي تطلب عناوين بريد إلكتروني هو قيام الطلاب بإنشاء حسابات لبريد إلكتروني "يمكن التخلص منها". إن العديد من حسابات البريد الإلكتروني مجانية، ويسهل إعدادها من خلال خدمات مثل الياهو Yahoo وجي ميل Gmail وهوت ميل Hotmail. عندما يقوم الطلاب بإعداد حسابات يمكن التخلص منها، قم بالتأكيد عليهم بألا يقوموا بتزويد معلومات شخصية حقيقية. يجب أن يستخدموا هذه العناوين الإلكترونية المؤقتة فقط عندما يحتاجون إلى تزويد عنوان بريد إلكتروني ويشتبهون بأنه سيتم إساءة استخدام عنوان البريد الإلكتروني. إن حسابات البريد الإلكتروني غير المستخدمة في هذه الخدمات المجانية سوف تنتهي صلاحيتها بكل بساطة بعد مدة من الزمن بسبب عدم التفعيل المستمر.

يتوافر استعراض لأفضل خدمات البريد الإلكتروني على About.com على الرابط http://email.about.com/od/freeemailreviews/tp/free_email.htm.

الحشو

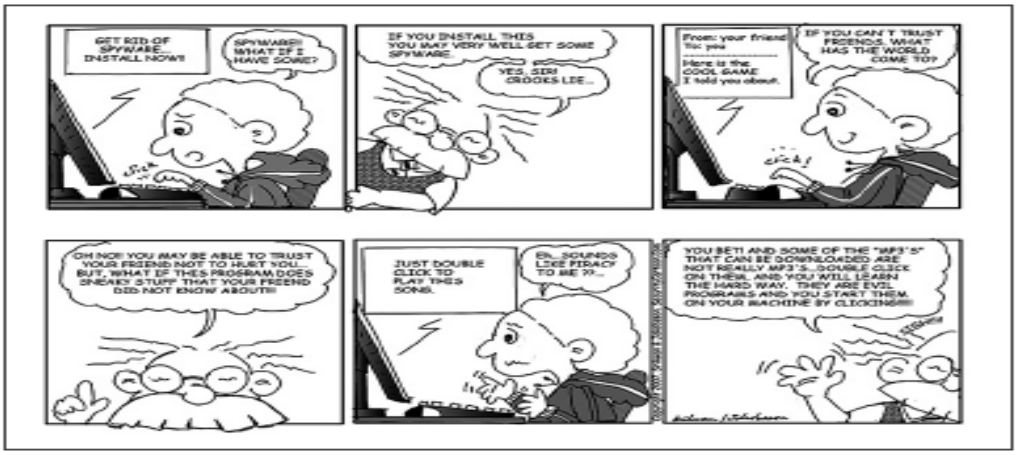
يشير مصطلح الحشو إلى قيام إحدى الشركات بإضافة رسوم غير مرخصة ومضللة أو احتيالية على فواتير الهاتف الشهرية. اطلب من الطلاب القيام بالنشاط التالي. أخبر الطلاب بأنهم قد يبلغون آبائهم بهذه المعلومات:

اسأل والديك إذا كان بإمكانهم النظر على فاتورة الهاتف الخلوي الخاصة بالعائلة ومراجعة الرسوم. إذا شاهدت أية رسوم عامة أو غامضة مدرجة فيها – على سبيل المثال، "تحميل،" "بيانات،" أو "خدمات مميزة" – ولا يوجد أي تفسير لها، اطلب من والديك أن يسمحوا لك بالاتصال على مركز خدمات شركة الهاتف الخلوي واطلب من الشركة تفسير هذه الرسوم. عندما تتصل، اطلب من الشركة تحديد أي "شركة كطرف ثالث" تقوم بإصدار الفواتير لهم من خلال ناقل فاتورة الهاتف الخلوي. ثم اطلب من عائلتك إن كان قد طلب أي منهم هذه الخدمات بالفعل. إن لم يقم أحد منهم بذلك، أخبر عائلتك بأن فاتورتهم قد تم حشوها!

برامج الحاسوب الخبيثة للتجسس Spyware

إن شبكة الإنترنت مليئة بالعديد من عمليات التحميل والألعاب وحافظات الشاشة ونغمات الرنين المقاطع الفلمية والبرمجيات مجانية التحميل ولكن ماذا تعنى كلمة "مجاني"؟ إن العديد مما يدعى أشياء مجانية يكون مصحوبًا بثمن باهظ. يقومون بغزو خصوصيتك – أو الأسوأ من هذا هو تحميل برامج خبيثة للتجسس على جهاز الحاسوب الخاص بك (انظر الشكل رقم ٢-٥).

يعرف معجم تكنولوجيا المعلومات على الموقع الإلكتروني للمعهد الجنائي في جامعة أركنساس University of Arkansas Criminal Justice Institute (www.tjss.net/glossary_s.html) برامج الحاسوب الخبيثة للتجسس spyware بأنها: "أي برنامج على الحاسوب يقوم بجمع معلومات المستخدم سرًا من خلال اتصال المستخدم بالإنترنت بدون معرفته أو معرفتها، وتكون في العادة لأهداف دعائية. إن تطبيقات برامج الحاسوب الخبيثة للتجسس spyware هي في العادة مجمعة على هيئة مكون مخفي لبرمجيات مجانية أو برامج التشغيل التي يمكن تحميلها من شبكة الإنترنت.



الشكل رقم (٢-٥): العديد من المخاطر موجودة على شبكة الإنترنت.

(تم إعادة طباعتها بعد الحصول على تصريح. للحصول على المزيد من المواد، الرجاء زيارة www.SecurityCartoon.com)

حصان طروادة Trojan Horse

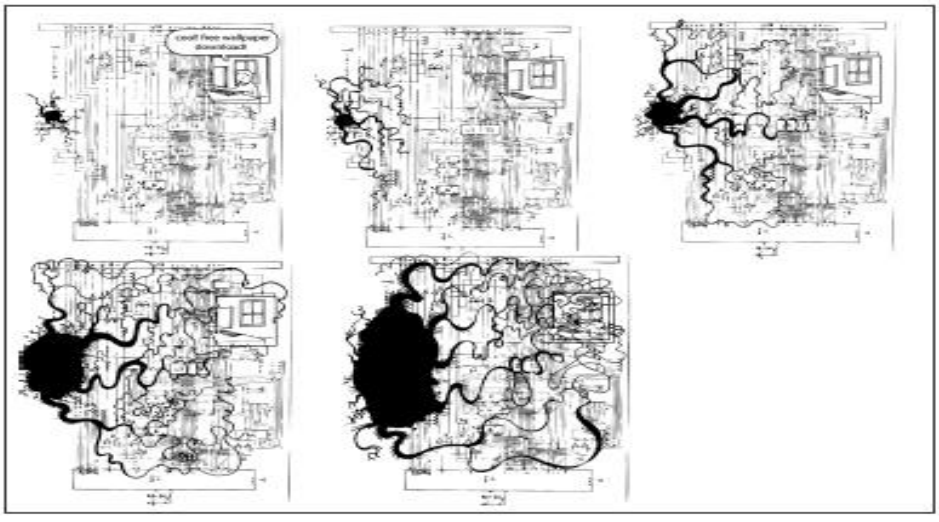
إن حصان طروادة Trojan Horse هو نوع عام من البرمجيات الخبيثة (برمجيات ضارة) والتي يتم تحميلها بدون معرفة وموافقة المستخدم. وما أن يكون اسم حصان طروادة Trojan Horse هو Smitfraud. سوف يقوم Smitfraud بتحميل منتجات تتعلق بأمن الحاسوب غير صادقة وتغير سطح المكتب الخاص بالمستخدم ليقوم بعرض إنذارات كاذبة بأن جهاز الحاسوب متأثر ببرنامج خبيث للتجسسspyware . ومن ثم يتم مطالبة المستخدم لكي يدفع ويحمل ويثبت برنامج مزيف يقول بأنه سيتم تحديد وإزالة برنامج الحاسوب الخبيث للتجسس spyware. على الرغم من الإنذار الكاذب يتم إزالته بالفعل، لكن لا يزال حاسوب المستخدم يحتوي على برنامج الحاسوب الخبيث للتجسس spyware الذي تم تثبيته على الجهاز.

وما أن يتم تحميله على الحاسوب، يراقب برنامج الحاسوب الخبيث للتجسس spyware نشاط المستخدم على شبكة الإنترنت وينقل تلك المعلومات إلى شخص آخر لاستخدامها. يمكن أن يجمع برنامج الحاسوب الخبيث للتجسس spyware كذلك معلومات حول عناوين البريد الإلكتروني وكلمات المرور وأرقام بطاقات الائتمان". التمرين (٢-٤) ما برنامج الحاسوب الخبيث للتجسس spyware؟ يطلب من الطلاب البحث عن مصطلح "برنامج الحاسوب الخبيث للتجسس spyware"، ومقارنة نتائجهم وذلك ضمن الجهود

الهادفة إلى تعميق معرفتهم بالمصطلح وكيفية عمل برنامج الحاسوب الخبيث للتجسس spyware على شبكة الإنترنت.

لا يتم توصيل برنامج الحاسوب الخبيث للتجسس spyware إلى الحاسوب من خلال شبكة الإنترنت فقط. من المحتمل أن يتعرض الجهاز لبرنامج الحاسوب الخبيث للتجسس spyware من خلال عمليات تنزيل التراسل الفوري IM، وعمليات التنزيل من الهاتف الخلوي، والمرفقات الموجودة على البريد الإلكتروني. أينما يجد الطلاب ألعاب ترفيهية "مجانية" أو عروض مجانية، يجب أن يشتبهوا بوجود برنامج الحاسوب الخبيث للتجسس spyware.

يتعرض الطلاب في العادة للخداع من خلال تجميل وتجهيز المنتجات أو الخدمات أو التطبيقات المجانية. على سبيل المثال، يطلب العديد من مواقع استعراض الموسيقى الغنائية من مستخدمي الحاسوب الشخصي لتشغيل إحدى مميزات برنامج يدعى "activeX" وتثبيت تطبيق صغير لمشاهدة استعراضات الموسيقى الغنائية. ولكن هذا التطبيق يثبت أيضًا برنامج الحاسوب الخبيث للتجسس spyware. يوفر مقال PC Pitstop المعنون بـ " هل أطفالك بأمان من برامج الحاسوب الخبيثة للتجسس spyware"Are Your Children Safe from Spyware" " بقلم الكاتب روبرت ب ليبسشوتس Robert P. Lipschutz وجون كلايمان John Clayman (www.pcpitstop.com/spycheck/Children.asp) المزيد من المعلومات حول التعرض لبرامج الحاسوب الخبيثة للتجسس spyware. يركز التمرين (٢–٥) – اختبر نفسك على أمن الحاسوب وكلمة المرور مما يسمح للطلاب باختبار مدى تحصين حواسيبهم ضد برامج الحاسوب الخبيثة للتجسس spyware وتحديد قوة سلوكهم على شبكة الإنترنت لتجنب هذه التهديدات.



الشكل رقم (٢-٦): برنامج الحاسوب الخبيث للتجسس spyware يسيطر على الجهاز

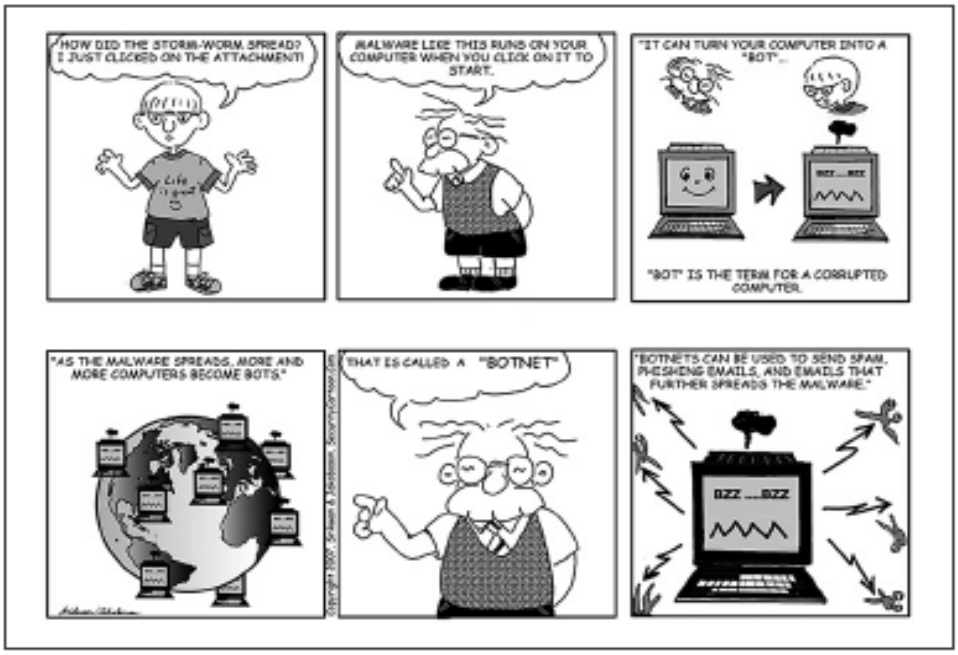
وما أن يبدأ برنامج الحاسوب الخبيث للتجسس spyware بالعمل على جهاز الحاسوب، يبدأ المستخدمون في ملاحظة زيادة النوافذ المنبثقة عندما يستخدمون متصفح الإنترنت، وفي بعض الأحيان عندما لا يفعلون ذلك. وفي بعض الأحيان ترتبط النوافذ بأي شيء يعمله المستخدمون على الإنترنت. على سبيل المثال، إذا كانوا يبحثون في جوجل Google عن ملفات موسيقى MP3 أو مقاطع فيديو على يوتيوب YouTube، فقد يشاهدون إعلانات لمواقع للموسيقى والفيديو. يستطيع أن يرسل برنامج الحاسوب الخبيث للتجسس spyware تقريرا عن نشاطات الطالب على شبكة الإنترنت إلى الكمبيوتر الرئيس المركزي الذي يراقب ما يفعله الطالب على شبكة الإنترنت. يمكن أن يؤثر برنامج الحاسوب الخبيث للتجسس spyware في استقرار وأداء جهاز الحاسوب، وفي العادة يقوم بإبطائه إلى درجة منخفضة جدًّا. بعض أجهزة الحاسوب، وبخاصة تلك التي تشغل برنامج تشغيل ويندوز Windows، يمكن أن تصبح محجوبة ومسدودة جدًّا ببرنامج الحاسوب الخبيث للتجسس spyware بحيث تصبح هذه الأجهزة غير مفيدة من الناحية العملية.

التمرين (٢–٦) التهديدات الحالية في الأخبار تنقل موضوع سلامة الإنترنت إلى مستوى عالمي أكثر، حيث يقوم الطالب بالبحث عن الكميات الهائلة للاحتيال والنصب التي يتم حاليًا الإبلاغ عنها.

Zombies وBotnet

تقدر عاملة في الشركات العاملة على سلامة الإنترنت بأن ٥٠% إلى ٨٠% من كافة الرسائل غير المرغوبة على شبكة الإنترنت تأتي من أجهزة الحاسوب..... zombies (ربيع عام ٢٠٠٥م).

متى يكون حاسوبك بالفعل ملكًا لشخص آخر؟ قد يعتقد طلابك أن أجهزة الحاسوب الخاصة بكم هي بالفعل قيد السيطرة. وعليه، إذا كان الحاسوب موصولاً بشبكة الإنترنت، فهنالك فرصة بأن يكون أحد آخر قد اكتسب سيطرة جزئية أو كاملة على الجهاز بدون معرفة المالك. إن حاسوب zombie هو عبارة عن جهاز حاسوب موصول بالإنترنت وتم تعرضه لبرمجيات ضارة والتي أتاحت بدورها لشخص آخر السيطرة على الحاسوب. يستخدم في العادة مرسلو الرسائل غير المرغوبة spammers أجهزة الحاسوب zombies لإرسال آلاف الرسائل الإلكترونية بدون معرفة مالك الحاسوب. إن botnet هو عبارة عن شبكة آلية لأجهزة الحاسوب zombies، والتي تم استخدامها بشكل تقليدي لخدمة هدف واحد مثل إرسال آلاف الرسائل الإلكترونية غير المرغوبة أو القيام بأعمال هجومية على الكمبيوتر الرئيس الشبكة الإلكترونية (على سبيل المثال، إنكار خدمة الأعمال الهجومية Denial of Service attacks). التمرين (٧–٢) ما هو حاسوبZombie؟ ما هو الـbotnet؟ يسمح للطلاب بتعميق فهمهم لأجهزة الحاسوب zombies والـbotnets من خلال البحث المستقل ومشاركة المجموعة.



الشكل رقم (٧-٢): كيف يتم تشكيل الـbotnet

zombies في الأخبار!

تم اتهام رجلين من تكساس باحتيال جماعي بأجهزة حاسوب zombie.

"وفقًا للتقارير، أدان قسم الشكاوي في لجنة الأوراق المالية والبورصات داريل اسيلتون Darrel Uselton البالغ من العمر ٤٠ عامًا وعمه جاك اسيلتون Jack Uselton والبالغ من العمر ٦٩ عامًا، كلاهما من تكساس، بتأليف سلسلة من حملات الرسائل غير المرغوبة المصممة لخداع المستثمرين الغافلين والتلاعب بسوق الأسهم. يزعم بأن الرجلين قد استخدما شبكة زومبي Zombie للحواسيب الواقعة تحت القرصنة في كافة أنحاء البلاد لتوزيع هذه الرسائل الإلكترونية، وفي نهاية المطاف خداع مستخدمي الحاسوب الذين لا يشتبهون بشيء بما يقدر بـ ٤.٦ مليون دولار أمريكي. بدأ التحقيق بعد أن استلم أحد المحامين في لجنة الأوراق المالية والبورصات إحدى هذه الرسائل الإلكترونية الاحتيالية في العمل." (لقراءة القصة الكاملة المؤرخة في ١٠ يوليو/ تموز من عام ٢٠٠٧، على الرابط التالي:

(www.sophos.com/pressoffice/news/articles/2007/07/texan-scam.html

أكثر من مليون ضحية محتملة لجريمة الـ botnet على الشبكة العنكبوتية.

أعلنت وزارة العدل ومكتب التحقيقات الفيدرالية اليوم نتائج مبادرة الجريمة المستمرة على

الشبكة للإخلال ونزع "الإرتباك والقلق"ورفع وعي الأمن العام لـ botnets على الشبكة العنكبوتية. إن عملية *Operation Bot Roast* هي عبارة عن مبادرة قومية وتحقيقيات مستمرة حيث حددت أكثر من مليون ضحية على الحاسوب نتيجة سرقة عناوينهم الشخصية. يعمل مكتب التحقيقات الفيدرالي مع شركائنا في الصناعة، والتي تتضمن مركز فريق تنسيق الإستجابة الطارئة للحاسوب Computer Emergency Response Team Coordination Center في جامعة كارنيجي ميلون Carnegie Mellon University، لإشعار الضحية وهو مالك الحاسوب. وخلال هذه العملية، قد يكشف مكتب التحقيقات الفيدرالي عن حوادث إضافية والتي تم فيها استخدام botnets لتسهيل نشاط إجرامي آخر." (لقراءة القصة كاملة، والمؤرخة في ١٣ يونيو/ حزيران لعام ٢٠٠٧، على الرابط التالي (www.fbi.gov/pressrel/pressrel07/botnet061307.htm)

ملفات تعريف الارتباط Cookies

إن ملفات تعريف الارتباط cookies هي عبارة عن رسائل يتم إرسالها إلى ومن الكمبيوتر الرئيس على شبكة الإنترنت وزائر متصفح الشبكة الإلكترونية. تحتوي هذه الرسائل على معلومات عن الزائر، والإعدادات الخاصة بالموقع الإلكتروني الذي يتم زيارته ومعلومات إضافية تقوم بتعقب استخدام الزوار للموقع الإلكتروني. لا تعتبر ملفات تعريف الارتباط cookies دائما سيئة. ومع ذلك يمكن للأشخاص استخدام ملفات تعريف الإرتباط cookies لتعقب نشاط الطلاب على الشبكة الإلكترونية، حيث تكون أداة قيمة للأشخاص الذين يرغبون في مراقبة ما يفعله الطلاب ومن ثم القيام بالتسويق أو إرسال إعلانات إليهم وبالتالي التلاعب بقرارات الشراء الخاصة بهم. قد يجد الطلاب التفكير بأن أحدًا يرقب بالفعل المواقع الإلكترونية التي يزورونها أو الكلمات التي يدخلونها في حقول البحث على المواقع الإلكترونية أمرًا مخيفًا. من الممكن أن تقوم بتغيير إعدادات المتصفح الخاص بك بحيث لا يتم قبول ملفات تعريف الإرتباط cookies؛ لسوء الحظ، معظم المواقع الإلكترونية التي تستخدم ملفات تعريف الإرتباط cookies لا تسمح لك باستخدام موقعها أو قد تقاطع باستمرار نشاطاتك إذا قمت بإغلاق ملفات تعريف الإرتباط cookies. إن التمرين(٢–٨) – ما هو ملف تعريف الارتباط cookie؟ والتمرين (٢–٩) – المزيد عن ملفات تعريف الإرتباط cookies مصممان لمساعدة الطلاب على تحديد ملفات تعريف الارتباط cookies وتعريفها والتمييز بين صفاتها الإيجابية والسلبية.

عمليات التنزيل الموجهة على الحاسوب Drive-by Downloads

إن عمليات التنزيل الموجهة على الحاسوب Drive-by Downloads هو عبارة عن برنامج يتم تنزيله تلقائيًا وتثبيته على الحاسوب الشخصي بدون معرفة المستخدم أو موافقته لدى زيارة المستخدم لصفحة على الشبكة الإلكترونية. ومن ثم يقوم التطبيق الذي تم تنزيله

على الجهاز في العادة بتوجيه تثبيت تطبيقات برنامج الحاسوب الخبيث للتجسس spyware والتطبيقات الضارة، أو قد تحول جهاز الحاسوب إلىzombie. كما قد تقوم بتثبيت برنامج keylogging الذي يقوم بسرقة كلمات المرور من خلال القيام بتسجيل ما يتم طباعته تمامًا على لوح المفاتيح.

دع الطلاب يشاهدون شريط الفيديو الذي تبلغ مدته ١٢ دقيقة، "تحليل البرامج الضارة": عمليات التنزيل الموجهة،" عبر زيارة الرباط التالي:

http://video.google.com/videoplay?docid=335151277240238297

الذي تم إنتاجه من قبل WatchGuard.com، يستعرض الفيديو عمليات التزيل الموجهة والتأثير الذي يمكن أن تمتلكه على أجهزة الحاسوب الخاصة. كما تلخص معظم المفاهيم الموجودة في الفصل الثاني وتوضح ما يمكن أن يحدث على الحاسوب الشخصي عبر الإنترنت.

يتم تقديم هذا الفيديو من قبل رجل شاب يدعى كوري Cory، الذي بدأ باللعب على أجهزة الحاسوب منذ صغره ومر بتجارب تتعلق برموز الحاسوب والتطبيقات بطريقة غير لائقة. وما أثار دهشة والديه عندما حضر مكتب التحقيقات الفيدرالي FBI إلى منزلهم عندما كان كوري Cory بعمر الرابعة عشر للتحدث معه حول محاولات القرصنة التي يقوم بها. ومنذ ذلك الوقت، أصبح يتصرف بمسؤولية أكثر ويعمل الآن لدى شركة WatchGuard.com.

وعوضا عن ذلك، يمكن أن يشاهد الطلاب شريط الفيديو المعنون بـ " فكر قبل أن تقوم بالنقر Think before You Click"، والمنتج أيضا من قبل WatchGuard.com. يتضمن هذا الفيديو بضع دقائق عن عمليات التنزيل الموجهة بالإضافة إلى معلومات إضافية حول مخاطر برنامج الحاسوب الخبيث للتجسس spyware. الرجاء زيارة الرباط التالي: http://video.google.com/videoplay?docid=-4094518401580008932 لمشاهدة هذا الفيديو. (ملاحظة: في هذا الفيديو، يقوم أحد الأشخاص الذين تم مقابلتهم "العبث مع الآخرين" أو "ارتكاب أخطاء فادحة").

كما يوجد أيضا شريط فيديوعلى شبكة الإنترنت على يوتيوب YouTube من McAffee (UNUnet.com) والذي يبين تثبيت عمليات التنزيل الموجهة. الرجاء زيارة الرباط التالي لمشاهدة الفيديو: www.youtube.com/watch?voU1gcprFEPU.

تقنية التحكم الخفي في الحاسوب rootkit هي عبارة عن برنامج أو مجموعة من البرامج لقرصنة الوصول الموجه (الخفي) للحاسوب. إن القراصنة – الذين يقومون بتثبيت تقنيات التحكم الخفي في الحاسوب rootkits على حاسوب شخص ما – يحصلون على قدرة الوصول والقوة للسيطرة بشكل كامل على ذلك الحاسوب. التمرين (٢–١٠) – تقنيات التحكم الخفي في الحاسوب Rootkits يبني على الدروس المستفادة في الفيديو بينما يبحث الطلاب في تقنيات التحكم الخفي في الحاسوب Rootkits ويتشاركون نتائجهم مع زملائهم.

إعدادات لحماية الخصوصية على متصفحي الشبكة الإلكترونية

هل يعلم طلابك أنه في مكان ما في قائمة عناصر متصفح الشبكة الإلكترونية أو عناوين التصفح المفضلة لديهم يمكنهم توجيه المتصفح لشطب بياناتهم الخاصة؟ وقد تكون هذه طريقة أخرى قيمة لحماية خصوصيتهم بعد كل جلسة على الإنترنت. سوف تقوم بشطب مثل هذه الأمور مثل ملفات تعريف الارتباط Cookies والبيانات المحفوظة في نماذج مثل الأسماء والعناوين، وكلمات المرور المحفوظة. قم بتذكير الطلاب بأنهم يجب ألا يقوموا نهائيًا بحفظ كلمة المرور الخاصة بهم على أي حاسوب.

اطلب من الطلاب القيام بالبحث في تفضيلات متصفح الشبكة الإلكترونية على حاسوبهم. هل يمكنهم العثور على إعدادات التحكم بالخصوصية والأمن؟

تمرين ٢-١١: إعدادات الأمان والخصوصية: أطلب من طلابك تقييم أدوات الخصوصية الموجودة في أنظمة الكمبيوتر لديهم وتحديد مواطن الخطر فيها.

تمرين ٢-١٢: مقالات حول أمن الإنترنت.

أطلب من طلابك توسيع معرفتهم حول الأمان إلى منظور عالمي وهم يقومون بالبحث في القضايا الحالية فيما يتعلق بأمن الإنترنت حول العالم.

أدوات لحماية خصوصيتك

يتوافر العديد من الأدوات واقتراحات الأمن لمساعدة طلابك على حماية خصوصيتهم الشبكة الإلكترونية قم باستعراض كل من العناصر التالية مع طلابك. ثم تحقيق أي منها يتم استخدامها على الحواسيب في منازلهم وتقديم تقرير لك.

١. برنامج الحماية ضد الفيروسات

قم بسؤال الطلاب إن كانت الحواسيب الموجودة في منازلهم تحتوي على برنامج مثبت عليها للحماية ضد الفيروسات. إن كان كذلك، هل برنامج الحماية ضد الفيروسات محدَّث؟ متى كانت آخر مرة تم تنزيل تعريفات للفيروسات بحيث يستطيع البرنامج الخاص بهم من التعرف على أحدث الفيروسات وديدان الإنترنت worms وأحصنة طروادة Trojan horses الموجودة على الإنترنت؟ (ملاحظة: على الرغم من أن فيروسات أبل ماكنتوش Apple Macintosh نادرة، ما زالت حواسيب أبل Apple تمرر الفيروسات للأصدقاء والعائلة ممن لديهم أنظمة تشغيل ويندوز Windows operating systems على حواسيبهم). تنتج كل من جريسوفت Grisoft (www.free.grisoft.com) وسورس فاير SourceFire (www.clamwin.com) تطبيق مجاني وأساسي ضد الفيروسات للحواسيب الشخصية. كلام إكس أف ClamXav (www.clamxav.com) هو عبارة عن تطبيق مجاني ضد الفيروسات لنظام تشغيل ماكنتوش Macintosh operating system.

٢. برنامج الحماية ضد برامج التجسس الخبيثة spyware

يُنصح بأن يقوم مستخدمو الحاسوب الشخصي التي تعمل بنظام تشغيل ماكنتوش بامتلاك برنامجين مختلفين ضد الفيروسات على حواسيبهم في آن واحد. لسوء الحظ، بعض برامج مكافحة الفيروسات عديمة الفائدة، وبعضها الآخر هي في الواقع برامج تجسس مقنعة. أي برنامج يستطيع الطلاب الوثوق به؟ هنالك مكان رائع للبحث فيه عن معلومات غير متحيزة حول برنامج مكافحة التجسس الفعال وهو Spyware Warrior (www.spywarewarrior.com). في الماضي، كانوا ينصحون بمنتجات مجانية من:

- Windows Defender :www.microsoft.com/athome/security/spyware/software
- Ad-Aware من شركة Lavasoft، :www.lavasoftusa.com
- Spybot – Search & Destroy :www.spybot.net

٣. رُقع وتحديثات نظام التشغيل ومتصفح الشبكة الإلكترونية

إن هذه حماية قيِّمة لكل من مالكي حواسيب ماكنتوش Mac والحاسوب الشخصيPC. يجب أن يحافظ الطلاب على نظام التشغيل لحواسيبهم وبرنامج الشبكة الإلكترونية مُحدَّث بشكل دائم. بعض متصفحات الشبكة الإلكترونية، مثل Firefox تقوم بإجراء التحديثات بشكل ذاتي تمامًا مثل نظام التشغيل.

٤. إعدادات أمان متصفح الشبكة الإلكترونية

قم بإخبار الطلاب بما يلي: لا تبقوا إعدادات الأمان الخاصة بكم منخفضة المستوى. عليكم رفعها للأعلى باستمرار!

٥. معدات وبرامج جدران الحماية

إن العديد من حلول المعدات والبرامج التي تعمل كواجهة أمان تفصل الحاسوب عن الإنترنت يمكن تثبيتها على حاسوبك، فهي تعمل كحراس حماية تحمل قائمة أسماء "مطلوب بشدة" وتراقب كافة التحركات التي تدخل وتخرج من الحاسوب. يمكنك الاختيار من منتجات ذات جودة مختلفة للحاسوب الشخصي، مثل Comodo Firewall Pro (www.personalfirewall.comodo.com) وZoneAlarm من قبل Check Point (www.zonealarm.com).

قد يتضمن نظام تشغيل الحاسوب جدار حماية أساسي، ولا يشترط أن يكون قيد التشغيل بالضرورة. على سبيل المثال، يمتلك مالكي أبل ماكنتوش Apple Macintosh بأنظمة تشغيل ١٠.٣ وأعلى جدار حماية من الإنترنت التي تكون في العادة غير مفعلة. إذا فتحت أفضليات النظام System Preferences وانقر على أيقونة المشاركة Sharing، سوف ترى علامة تبويب تدعى جدار الحماية Firewall. ببساطة انقر على ابدأ Start لتشغيله.

إن مالكي الحاسوب الشخصي PC الذين يستخدمون Windows XP Service Pack 2 أو Vista يمتكلون أيضًا جدار حماية مبني داخليًا. اخبر الطلاب أن يحددوا جدار الحماية في أفضليات النظام والتأكد من تشغيلها.

٦. حماية المعلومات الشخصية

قم بتذكير الطلاب بإرشادات الأمان الأخرى في هذا الفصل، مثل خاصية حذف البيانات في متصفح الشبكة الإلكترونية، واستخدام عناوين بريد إلكتروني يمكن التخلص منها عند الضرورة.

إن أكبر حماية منفردة ضد معظم برامج التجسس وضد كافة البرامج الضارة تقريبا والفيروسات وأحصنة طروادة Trojan horses ودود الحاسوب computer worms والمحتالين على الإنترنت هي ببساطة استخدام حاسوب أبل ماكنتوش Apple Macintosh للدخول إلى الإنترنت. إن كافة التهديدات التي تم وصفها سابقًا يتم توجيهها إلى الحواسيب الشخصية التي تشغل أية نسخة من نظام تشغيل ويندوز Windows. وحتى تاريخ كتابة هذا الكتاب، يؤثر القليل جدًا من هذه التهديدات على مستخدمي ماكنتوش Mac. في شهر حزيران من عام ٢٠٠٨م، تم التحقق من أول ثلاثة تطبيقات موجهة ضد نظام تشغيل ماكنتوش Mac. ومنذ ذلك الحين، تم اكتشاف معظم الأجزاء الجديدة من المواد الجديدة المضافة ومتصفح معدات التجسس. كما إن أجهزة ماكنتوش Macs عرضة لفقدان الخصوصية من ملفات تعريف ارتباط متصفح الشبكة الإلكترونية مثل أجهزة الحاسوب الشخصي PCs (انظر التمرين٢–٨). ومع ذلك، يواجه نظام تشغيل ماكنتوش Mac العديد من تهديدات الإنترنت على المدى البعيد أكثر من نظام تشغيل ويندوز Windows. تذكر أنه إذا كانت حواسيب أبل Apple تستخدم Boot Camp، و Parallels أو بعض برامج الحاسوب الأخرى التي تشغل ويندوز Windows على حاسوب ماكنتوش Macintosh، يصبح عندها الحاسوب عرضة لتهديدات على شبكة الإنترنت مثل أي حاسوب شخصي PC.

التمارين

التمرين (٢-١):

البنرات الإعلانية Banner Ads
والنوافذ المنبثقة Pop-ups

مهم: لا يجب القيام بهذا التمرين إلا إذا كنت تستخدم جهاز حاسوب Apple Macintosh أو حاسوب شخصي مثبت عليه برنامج الحاسوب الخبيث للتجسس spyware قوي أو برنامج الحماية ضد الفيروسات. إذا كنت تستخدم حاسوب شخصي بدون حماية أو حمايته ضعيفة، فإنك تكون عندئذ عرضة لخطر كبير بتعرض حاسوبك للبرامج الضارة بدون قصد. قم بالتحقق مع منسق التكنولوجيا في مدرستك إن لم تكن متأكدًا إن كان هذا التمرين آمنًا أم لا.

قد تقرر تزويد الطلاب بمواقع محدد للقيام بزيارتها لتجنب أية نتائج غير متوقعة أو اختيارات الطلاب الضعيفة. قد يعتمد هذا التمرين بشكل كبير إن كانت مدرستك تمتلك مرشح للشبكة الإلكترونية للمساعدة في الحماية ضد المحتوى غير اللائق العرضي.

ابدأ التمرين(٢-١) بالطلب من طلابك قضاء ١٠ دقائق على الإنترنت للبحث عن مواقع مألوفة، مثل مواقع الألعاب. قد تختار عمل هذا من جهاز حاسوب مركزي مع شاشة عرض ليتمكن الجميع من المشاهدة. انظر أدناه على أمثلة المواقع الإلكترونية للقيام بزيارتها والتي تتضمن:

(www.cheatcodes.com) CheatCodes.com
(www.freearcade.com) FreeArcade.com
(www.coolquiz.com) Cool Quiz
(www.cheatcodesglore.com) Cheat Codes Galore
(www.blitzgamer.com) BlitzGamer

في نهاية الدقائق العشر، اسأل الطلاب كم عدد النوافذ المنبثقة أو لافتة الإعلانات التي يعثرون عليها والتي تقول لهم بأنهم فازوا بمنتج مجاني، أو التي تغريهم للتفاعل كأسئلة مثل "من تحب؟" أو "من أفضل شخص بالمقارنة معك؟" أو "هل أنت شخص لطيف؟". تذكروا أن بعض الإعلانات قد تكون "نوافذ منبثقة مخفية pop-unders،" والتي تخفي تحتها نافذة مفتوحة. كم عدد النوافذ المنبثقة، النوافذ المنبثقة المخفية، البنرات الإعلانية التي وجدها طلابك؟

التمرين (٢-٢):
لقد فزت! أو هل فزت!

يقول الإعلان: لقد فزت!، هل أنت فعلا محظوظ لهذه الدرجة لتكون *الفائز*؟ يرغب المعلنون في العادة في أن تصدق بأنك وحدك الفائز المميز وذلك ضمن جهودهم لجذب انتباهك. إحدى الطرق التي يقومون فيها بذلك هي بوضع لافتة إعلاناتهم بشكل غير مستمر بحيث لا يحصل زائر الموقع الإلكتروني على إعلان "الفائز" في كل مرة يقوم فيها بالوصول إلى الموقع.

قم بتزويد طلابك ببعض الأمثلة على المواقع الإلكترونية المختارة مسبقًا ليقوموا بزيارتها. إن مواقع الألعاب ومواقع سرقة رموز الألعاب تعتبر ذات سمعة سيئة فيما يتعلق بوضع إعلانات الفائز. من الأمثلة على هذه المواقع التي يمكن استخدامها لهذا التمرين هي: blitzgamer.com، freearcade.com، cheatcodes.com، runescape.com، coolgames.com cheatcc.com، crazymonkeygames.com، rebubbled.com.

إن لم يظهر إعلان الفائز من المرة الأولى، دع الطلبة ينقرون على زر تحديث refresh إلى أن يظهر الإعلان. كم عدد عمليات إعادة التنزيل التي قمت بها ليظهر مثل هذا الإعلان؟

التمرين (٢-٣):

مطلوب: معلوماتك الشخصية

مهم: لا يجب القيام بهذا التمرين إلا إذا كنت تستخدم جهاز حاسوب Apple Macintosh أو حاسوب شخصي مثبت عليه برنامج الحاسوب الخبيث للتجسس spyware قوي أو برنامج الحماية ضد الفيروسات. إذا كنت تستخدم حاسوب شخصي بدون حماية أو حمايته ضعيفة، فإنك تكون عندئذ عرضة لخطر كبير بتعرض حاسوبك للبرامج الضارة بدون قصد. قم بالتحقق مع منسق التكنولوجيا في مدرستك إن لم تكن متأكد إن كان هذا التمرين آمنًا أم لا.

ما الهدف الذي تسعى ورائه البنرات الإعلانية والنوافذ المنبثقة عندما تنقر عليها؟ لمعرفة ذلك، اطلب من طلابك زيارة احدى البنرات الإعلانية أو النوافذ المنبثقة والنقر عليها، ولكن تأكد في البداية من أنهم يفهمون ألا يقوموا بإدخال أية معلومات شخصية.

ما المعلومات التي يرغب المسوقون في معرفتها من الطلاب؟

قم بعمل قائمة بالأسئلة المطروحة من قبل الطلاب؟

هل فاز أي من الطلاب بأي جائزة بعد كل هذا العناء؟

قم بطرح أسئلة المناقشة التالية على الطلاب:

١. لماذا ترغب المواقع الإلكترونية بجمع هذه المعلومات؟
٢. ماذا تتوقع أن يفعل مالكو المواقع الإلكترونية بهذه المعلومات؟
٣. كيف يمكن أن يجني مالكو المواقع الإلكترونية من هذه المعلومات؟

التمرين (٢-٤):

ما برامج الحاسوب الخبيثة للتجسس spyware؟

اطلب من طلابك زيارة Google.com وإدخال مقطع البحث التالي: define:spyware
قم بقراءة خمسة تعريفات على الأقل. ما الأمور المشتركة بين هذه التعريفات؟

التمرين (٢-٥):
اختبر نفسك

اطلب من الطلاب زيارة

Looks Too Good To Be True.com
(www.lookstoogoodtobetrue.com/risktest/test7.aspx).

دعهم يقومون بالاختبار المعنون بـ " هل حاسوبك محمي؟" " Is Your Computer Protected?" لمشاهدة مدى درجة حماية حواسيبهم ضد الأعمال الهجومية من قبل برنامج الحاسوب الخبيث للتجسس spyware وعمليات التسلل على الإنترنت أو فيروسات الحاسوب.

أو اطلب من الطلاب زيارة

Stay Safe Online (http://staysafeonline.org/basics/quiz.html).

دعهم يقومون باختبار "ما هي درجة الأمان الموجودة لديك " " How Safe Are You?" للحصول على فكرة حول درجة الأمان الموجودة لديكم على الحاسوب وعلى الإنترنت.

التمرين (٢-٦):
التهديدات الحالية في الأخبار

يمكن العثور على أحدث التحذيرات من وزارة العدل Department of Justice حول عمليات الغش والاحتيال على الإنترنت، مثل سرقة المعلومات الشخصية على الموقع التالي Looks Too Good To Be True.com (www.lookstogoodtobetrue.com/alert.aspx).

دع طلابك يختارون إحدى المقالات الموجودة على هذا الموقع الإلكتروني، ويقومون بمراجعتها وتقديم تقرير حول النتائج التي يتوصلون إليها إلى الصف. وبدلاً عن ذلك، يستطيع الطلاب النقر على رابط قصص الضحايا Victims' Stories وقراءة بعض عمليات الاحتيال التي تم الإبلاغ عنها من قبل الآخرين وتقديم تقرير عنها. بالإضافة إلى ذلك، يستطيع الطلاب زيارة Sophos (www.sphos.com)، شركة أمان على الإنترنت، والنقر على أي بند في آخر الأخبار والتحقق من لائحة معلومات الأمان لديهم حول أحدث البرامج الضارة أو برامج الحاسوب الخبيثة للتجسس وتقديم تقرير عن النتائج التي توصلوا إليها إلى الصف.

التمرين (٢-٧):

ما جهاز الحاسوب Zombie؟ ما الـ Botnet؟

أطلب من الطلاب الذهاب إلى answers.com، وقم بإدخال مقطع البحث التالي "zombie computer،" ومن ثم قدم تقريرًا حول النتائج التي يتوصلون إليها.

التمرين (٢-٨):
ما ملف تعريف الإرتباط على جهاز الحاسوب Computer Cookie؟

اطلب من الطلاب الذهاب إلى www.google.com وقم بإدخال مقطع البحث التالي:
define:cookie

قم بقراءة خمسة تعريفات على الأقل. ما الأمور المشتركة بين هذه التعريفات؟

التمرين (٢-٩):
المزيد حول ملفات تعريف الإرتباط Cookies

اطلب من الطلاب فتح متصفح الإنترنت والبحث في القائمة عمَّا تسميه معظم متصفحات الإنترنت بـ "المفضلة" "Preferences". دعهم يبحثون عن مفتاح أو زر يتعلق بالخصوصية أو الأمان (قد تضع متصفحات الإنترنت المتعددة مفتاح الوصول لملفات تعريف الارتباط في مواقع مختلفة). إن لم تستطع تحديد زر أو مفتاح "المفضلة" "Preferences" بسهولة، قم بعمل بحث على جهاز الحاسوب الخاص بك عن "المفضلة" "Preferences" أو "ملفات تعريف الإرتباط" "cookies" وقم بالنقر عليها لإظهار "ملفات تعريف الإرتباط" "cookies". سوف يجد الطلاب "ملفات تعريف الإرتباط" "cookies" من العديد من المواقع الإلكترونية المختلفة، كل منها يحتوي على معرِّف فريد من نوعه قد يبدو له معنى ضعيف أو ليس له معنى على الإطلاق. وعليه، قد يشعر الطلاب بالدهشة لمشاهدة كم عدد ملفات تعريف الارتباط الموجودة على أجهزة الحاسوب الخاصة بهم من قبل المعلنين!

قم بإخبار طلابك بأن إحدى الطرق لحماية خصوصيتك هو حذف ملفات تعريف الارتباط من جميع المواقع الإلكترونية باستثناء المواقع الموثوقة.

التمرين (٢-١٠):

تقنيات التحكم الخفي في الحاسوب Rootkits

ما تقنية التحكم الخفي في الحاسوب rootkit ولماذا أهم أداة في صندوق أدوات المتسلل أو المحتال على الإنترنت؟

اطلب من الطلاب الذهاب إلى www.google.com وإدخال مقطع البحث التالي:

define: rootkit

اطلب منهم تقديم تقرير عن نتائجهم.

التمرين (٢-١١):
إعدادات الأمان والخصوصية

اطلب من الطلاب إعداد قائمة بأنواع ميزات الأمن والخصوصية التي يوفرها متصفح الإنترنت الخاص بهم. على سبيل المثال، هل يستطيع متصفح الإنترنت الخاص بهم حجب النوافذ المنبثقة؟ هل تستطيع إبلاغهم متى تشتبه بأنهم يزورون مواقع إلكترونية مزيفة مثل بنك وهمي والفيسبوك Facebook أو صفحة MySpace.

التمرين (٢-١٢):
مقالات حول

يمكن تنزيل وطباعة عدة مقالات من عشر صفحات حول أمن الإنترنت التي ظهرت في صحيفة USA Today خلال العام ٢٠٠٦ باستخدام الرابط التالي:
www.usatoday.com/educate/cybersecurity/datamining_case_study.pdf

اطلب من الطلاب اختيار إحدى المقالات لقرائتها والاختيار إما القيام بإعداد تقرير أو الإجابة عن الأسئلة التي تقوم بوضعها.

المصادر

Brain, M. (n.d.). *How Internet cookies work*.
متوفر في الموقع الإلكتروني :How Stuff Works
http://computer.howstuffworks.com/cookie5.htm

Cookies and privacy.FAQ. (n.d.)
متوفر في الموقع الإلكتروني :cookiecentral.com
www.cookiecentral.com/n_cookie_faq.htm

EPIC.org website: http://www.epic.org
كما تم وصفه على موقعهم الإلكتروني، EPIC (مركز المعلومات الإلكترونية الخاصة) هو مركز أبحاث للمنفعة العامة في واشنطن Washington، مقاطعة كولومبيا.D.C. تم إنشاؤه في العام ١٩٩٤م للتركيز على الانتباه العام حول إبراز قضايا الحريات المدنية وحماية الخصوصية، التعديل الأول، والقيم الدستورية".

Help safeguard your privacy on the Web. (2003).
متوفر في الموقع الإلكتروني :Microsoft
www.microsoft.com/windows/ie/ie6/using/howto/privacy/config.mspx

How Web servers' cookies threaten your privacy. (n.d.)
متوفر في الموقع الإلكتروني Junk-busters: www.junkbusters.com/cookies.html
Looks Too Good To Be True.com website: www.lookstoogoodtobetrue.com
إن هذا موقع لتثقيف المستهلك مصمم لمساعدة المستهلكين ليتجنبوا أن يكونوا ضحايا عمليات الإحتيال على الإنترنت.
National Cyber-Forensics & Training Alliance (NCFTA) website: www.ncfta.net
Salomon, S. (2005). *The GRC.com attacks*.
متوفر في الموقع الإلكتروني:
Assyrian Café: www.articles.assyriancafe.com/documents/grc_attacks.pdf
تم كتابة هذا المقال حول هجومات رفض الخدمة ضد شركة GRC

Sanders, T. (2005, October 21). *Botnetoperation controlled 1. 5m PCs*.
متوفر في الموقع الإلكتروني
vnunet.com :www.vnunet.com/news/2144375/botnet-operation-ruled-million
كما تحتوي هذه الصفحة أيضًا على روابط للمعلومات المتعلقة بتهديدات الإنترنت.
Security at home. (n.d.).

متوفر في الموقع الإلكتروني لمايكروسوفت Microsoft: www.microsoft.com/protect/
تحتوي هذه المقالة على معلومات لمساعدتك على تجنب تحديد السرقة والتجسس والفيروسات.

الموقع الإلكتروني لسوفس Sophos: www.sophos.com
سوفس Sophos هي عبارة عن شركة للأمن على الإنترنت. إحدى التمارين في قضايا التزوير/ الرسائل غير المرغوبة/الأدوات المضافة/ الفيروس سوف يكون القيام بزيارة موقعهم الإلكتروني والنقر على بند في أحدث الأخبار Latest News أو التحقق من معلومات الأمن الخاصة بهم حول آخر البرامج الضارة أو الأدوات المضافة.

Spammers continue innovation: Iron Port study shows image-based spam, hit & run, and increased volumes latest threat to your inbox. (2006, June 28).
متوافر من الموقع الإلكتروني لـ:
IronPort :www.ironport.com/company/ironport_pr_2006-06-28.html.

Spring, T. (2005, June 20). *Spam Slayer: Slaying spam-spewing zombie PCs.*
متوفر في الموقع الإلكتروني
PC World :www.pcworld.com/article/121381/spam_slayer_slaying_spamspewing_zombie_pcs.html.

الموقع الإلكتروني لـ StaySafeOnline.org: www.staysafeonline.info
هذا الموقع، من التحالف الوطني للأمن على الشبكة العنكبوتية National Cyber Security Alliance، والذي يوفر مصادر للسلامة والأمن على الشبكة العنكبوتية مجانية وغير تقنية للعامة بحيث يتمكن المستهلكون وأصحاب الأعمال الصغيرة المعلمون من معرفة كيفية تجنب الجريمة على الشبكة العنكبوتية. تتوفر مصادر محددة للمعلمين على الرابط التالي:
www.staysafeonline.org/basics/educators.html

Sunbelt Malware Research Lab: http://reserach.sunbelt-software.com
يضع Sunbelt Malware Research Lab روابط عن أعلى عشرة تهديدات حالية للتجسس. يستطيع الزوار أيضا تصفح الأنواع المتعددة من التهديديات حسب الفئات والعثور على المقالات وروابط أخرى مدرجة تحت مصادر التجسس.

Zombies and botnets: Help keep your computer under your control. (2007, January 3).
متوفر في الموقع الإلكتروني لمايكروسوفت
Microsoft: www.microsoft.com/protect/computer/viruses/zombies/mspx

الفصل الثالث

تجنب سرقة الهوية وانتحال الشخصية

تتمحور الغالبية العظمى لسرقة الهوية بين المراهقين حول أعمال التحرش.

قصة الفتاة آنا Anna

تتوق آنا إلى الوصول إلى المنزل وتسجيل الدخول على الإنترنت. لقد عاشت يوما صعبًا في المدرسة وكانت مشتاقة للتحدث مع أعز صديقاتها والتي تدعى شيلي Shelley. صعدت درج المنزل بسرعة كبيرة، دخلت إلى غرفتها وصفعت الباب وقامت بتشغيل حاسوبها المحمول. كانت تداعب أذن قطتها بيد وتقوم بتوجيه الفأرة باليد الأخرى، قامت بتشغيل برنامج التراسل الفوري وكانت تفكر بأنه مهما كانت سرعة تشغيل الحواسيب كبيرة فهي ليست كافية بالنسبة لها. قامت بطباعة كلمة المرور الخاصة بها والمكونة من ثمانية رموز ونقرت على دخول. وبدلا من مشاهدة قائمة أصدقائها، تفاجأت آنا لدى مشاهدتها رسالة وجود خطأ أفزعتها (الشكل رقم ٣-٢).

الشكل رقم (٣-١): هل يقوم أحد بانتحال شخصيتك على الشبكة الإلكترونية؟

من كان ينتحل شخصيتها على الشبكة الإلكترونية؟ التقطت آنا الهاتف لتتحدث مع شيلي.

سرقة الهوية

تحدث عملية سرقة الهوية عندما يسرق أحد ما أو يحصل بطريقة ما على المعلومات الشخصية بالطالب ويقوم بالادعاء بأن ذلك الطالب على الشبكة الإلكترونية ويسجل الدخول إلى حساباته الشخصية.

ومنذ بداية عام ٢٠٠٥م، كانت هنالك زيادة هائلة في حدوث عملية سرقة الهوية وانتحال الشخصية بين الطلاب على الشبكة الإلكترونية. قم بإجراء استطلاع سريع للرأي في صفك. قم بسؤال طلابك ما يلي:

١. كم منكم يعرف أن أحدًا ما تعرض لاستخدام حساباته على الشبكة الإلكترونية من قبل شخص آخر (غير مخوَّل)؟
٢. كم منكم يعرف أحدًا قام بالإدعاء أنه طالب آخر على الشبكة الإلكترونية؟

إن الأسباب التي تدفع الطلاب لسرقة الهويات هي في العادة إحدى النقاط التالية:

- للتحرش أو الإحراج أو الإهانة أو إلحاق الأذى بطالب آخر.
- لسرقة الأموال من الحسابات المصرفية للطالب على الشبكة الإلكترونية أو حسابات بطاقات الائتمان أو تلك الخاصة بوالدي الطالب.
- للدخول إلى حسابات أخرى ذات قيمة على الشبكة الإلكترونية مثل حسابات eBay، والنوادي، والألعاب على الشبكة الإلكترونية، ومجموعات RCG (لعب الأدوار)..إلخ.

إن الغالبية العظمى من عمليات سرقة الهوية بين المراهقين تتمحور حول التحرش. وبسبب قضاء الطلاب قسمًا كبيرًا من وقتهم في ابتكار وإنشاء عالم الألعاب الخاص بهم وعالمهم الاجتماعي على الشبكة الإلكترونية، أصبحت الإنترنت بشكل متزايد سلاحًا للسلوكيات السيئة من قبل الأشخاص الذين يتعمدون التحرش بهم أو إحراجهم. يتعلم الطلاب المزيد حول سرقة الهوية وكيف يكونون بمأمن منها عبر إجراء الاختبار في التمرين ٣–١ – البقاء بمأمن من سرقة الهوية، والذي يقدمه مركز مصادر سرقة الهوية Identity Theft Resource Center.

يقوم المحتالون في أغلب الأحيان بإغراء الطلاب بغية الإفصاح عن معلوماتهم الشخصية من خلال عرض أشياء "مجانية". إن عملية الإحتيال المعنونة "احصل على أي بود iPod مجانًا" موصوفة في الموقع الإلكتروني لمكافحة سرقة الهوية (http://fightidentitytheft.com/blog/scam/are-free-ipod-offers-a-scam/). قم بتذكير طلابك بما يلي: إذا كانت تبدو حقيقية إلى حد كبير، فإنها عملية احتيال بالفعل!

التمرين ٣–٢– كيف تحدث سرقة الهوية على الشبكة الإلكترونية؟ يساعد الطلاب على استيعاب أن سرقة الهوية تحدث كل يوم وفي بعض الحالات التي لم تظهر لهم. التمرين ٣–٣ – سرقة الهوية: ما الذي يجب عمله؟ يجعل الطلاب يناقشون إجراءات ما يجب عمله إذا تم الإفشاء عن هوياتهم.

انتحال الشخصية

لا تتطلب عملية انتحال الشخصية أن يقوم أحد ما بسرقة كلمات المرور للطالب واختراق حساباته. فهي تحدث أيضًا عندما يدعي أحد ما وببساطة أنه شخص آخر على الشبكة الإلكترونية. يخبرنا الطلاب أن هذا الأمر يحدث في أغلب الأحيان. يتم القيام بهذه العمليةفي العادة بغية إحراج طالب آخر أو التحرش به.

بقية قصة آنا Anna...

لقد أحست شيلي بالقلق في صوت آنا بينما كانت تستمع لمشكلتها. كانت شيلي ذكية جدًّا في الامور المتعلقة بالإنترنت، وبينما كانت آنا تتحدث حول من يكون قد سجل الدخول بوصفه هي، كانت شيلي تفكر في كيفية حصول ذلك.

" آنا "، قاطعتها شيلي قائلة: " عندما كنت في الخارج في عطلة نهاية الأسبوع الماضية، ألم تستخدمي الحاسوب الموجود في بيتنا لتسجيل الدخول في التراسل الفوري؟"

"نعم، وماذا في ذلك؟" أجابت آنا

" كنت أتسائل... هل طلبت من الحاسوب بحفظ كلمة المرور الخاصة بك؟

فكرت آنا للحظة وأجابت: " شيلي ، أنا متأكدة أنني لم أطلب من الحاسوب حفظ كلمة المرور الخاصة".

" لكن آنا، أخي الصغير قام بإعداد الحاسوب ليقوم دائمًا بحفظ كلمة المرور!" أسرعت شيلي إلى الطابق السفلي إلى حجرة الحاسوب". يجب أن تقومي دائمًا بالإلغاء التأشير عن المربع، وإلا قام الحاسوب بحفظ كلمة المرور الخاصة بكِ".

دخلت شيلي إلى حجرة الحاسوب. ووجدت أخاها الصغير البالغ من العمر إحدى عشر سنة على التراسل الفوري. اختفت الابتسامة عن وجه مات Matt عندما رأى اخته تمعن النظر فيه. وقبل أن يسجل الخروج من التراسل الفوري، نظرت إلى الشاشة وشاهدت أن الاسم المسجل هو:" anAbNanA".

" آنا ، سأعاود الاتصال بك بعد دقيقة."

إن التحايل يحدث عندما يصبح شخص أو برنامج ما التي يكون فيها قادرًا على التنكر بنجاح بأنه شخص آخر. قام طلاب من العديد من المدارس بتقديم تقارير حول هجومات التحايل والتي تكون فيها أسماء المستخدمين تشبه إلى حد قريب أسماء المستخدمين التي يعرفها الطلاب ويثقون بها. تكون عمليات انتحال الشخصية ناجحة جدًّا عندما يتم استخدام الرموز التالية:

1 I l and o O 0

أخبر الطلاب بأن يتجنبوا استخدام هذه الرموز في أسماء المستخدمين. يكون من الصعب استبعاد هذه الرموز من متصفح الشبكة الإلكترونية أو أي تطبيق آخر على الشبكة الإلكترونية مثل مكتشف الإنترنت Internet Explorer، فايرفوكس FireFox، سفاري Safari، IChat، أو MSN Messenger.

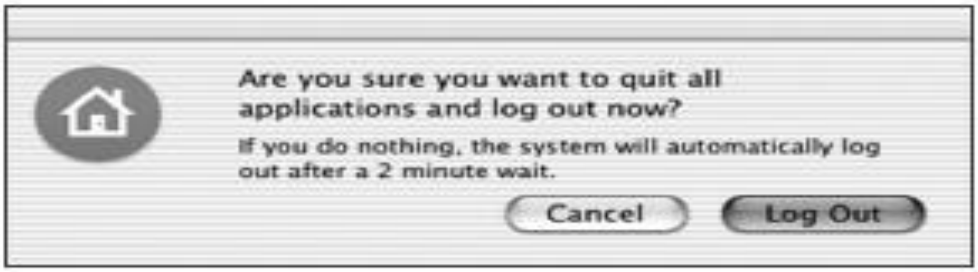
التمرين ٤–٣ – كيف يتأكد الطلاب؟ يساعد الطلاب على التفكير بممارسات وقائية لضمان تواصلهم مع أشخاص يعرفونهم ويثقون بهم. التمرين ٥–٣ – التحايل يساعد الطلاب على تمييز آليات الأشخاص للتسلل على الشبكة الإلكترونية والذين يحاولون تضليل الطلاب.

احتياطات ضد سرقة الهوية وانتحال الشخصية

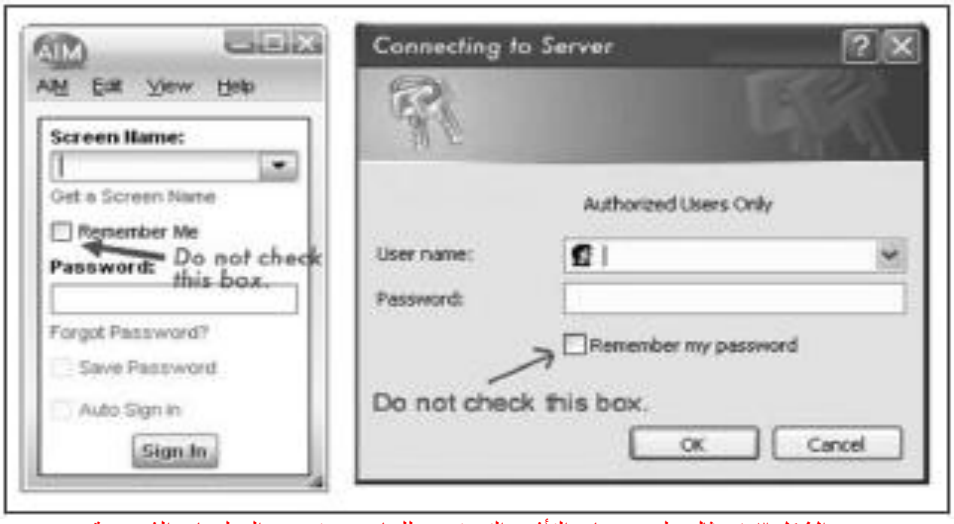
ليس من الصعب على الطلاب حماية أنفسهم ضد سرقة الهوية على الشبكة الإلكترونية. فيما يلي بعض الإجراءات الوقائية البسيطة التي يمكنهم القيام بها:

- أخبر الطلاب بألا يقوموا أبدا بإعطاء كلمات المرور الخاصة بهم للآخرين، وحتى لأفضل أصدقائهم.
- أخبرهم بأخذ الحذر ممن يقوم بمراقبتهم بينما يقومون بإدخال كلمات المرور الخاصة بهم. فقد يكون هنالك طالب آخر يقف ورائهم ويقوم بالنظر عليهم.
- قم بتذكيرهم بالقيام بتسجيل الخروج من حساباتهم بطريقة سليمة دائمًا. إن هذا يعني عدم إغلاق النافذة عندما تنتهي منها. يجب أولاً الخروج من التطبيق ومن ثم تسجيل الخروج من الحاسوب (الشكل ٢–٣ والشكل ٣–٣)

الشكل رقم (٣-٢): شاشة تسجيل الخروج في ويندوز Windows



الشكل رقم(٣-٣): شاشة تسجيل الخروج على ماكنتوش Mac



الشكل ٤.٣ مثال على مربعات التأشير التي تسمح للحاسوب بتخزين المعلومات الشخصية مثل اسم المستخدم وكلمة المرور

- لا يجب أن يقوم الطلاب ابدًا بالتأشير على مربعات مثل " تذكر كلمة المرور الخاصة بي" أو " تذكرني" والتي تقوم بتخزين المعلومات الشخصية على الحاسوب.
- يجب أن يتعلم الطلاب كيفية ابتكار كلمات مرور آمنة وتغييرها بشكل منتظم. (انظر التمارين ٧–١، ٨–١ ، ٩–١ و ١١–١ في الفصل الأول).
- يجب ألا يترك الطلاب على الإطلاق كلمة المرور مكتوبة على ورقة بالقرب من جهاز الحاسوب الخاص بهم أو في دفاتر ملاحظاتهم.
- قد ينخدع الطلاب بإدخال كلمات المرور الخاصة بهم في مواقع مزيفة مثل الموقع المزيف لـ MySpace، وFacebook أو صفحات البنوك. وهم في العادة يصلون إلى مثل هذه المواقع من خلال النقر على رابط مزيف في بريد الكتروني. أخبر الطلاب بأن يكونوا متيقظين جدا من الرسائل الإلكترونية التي تدعوهم لتسجيل الدخول في حساب على الشبكة الإلكترونية. وحتى إن كان الموقع الإلكتروني الذي يقومون بزيارته يبدو حقيقيًّا بشكل أكيد، إن الطريقة الوحيدة للتأكد هو بالتحقق من عنوان الموقع في شريط العناوين.

حقائق تتعلق بالتزييف

يحدث التزييف عندما يخدعك المجرمون لزيارة مواقع مزيفة مصممة لتبدو مثل المواقع الحقيقية تمامًا. ومن ثم يقوم الزوار بإدخال المعلومات الشخصية مثل: اسم مستخدم الحساب، رقم

البطاقة الائتمانية، ورقم الضمان الاجتماعي والتي يتم إرسالها على الفور إلى المجرمين.

٨.٥ بليون عدد الرسائل الإلكترونية المزيفة المرسلة في كافة أنحاء العالم كل شهر. (SonicWALL, 2008)

$٨٨٦ معدل خسارة كل شخص يتم الإحتيال عليه بنجاح. (Gartner Research, 2007)

٣٢.٤١٤ عدد المواقع الإلكترونية الفريدة في الإحتيال في مايو/ أيار ٢٠٠٨م(Anti-Phishing Working Group, 2008)

٣.١ متوسط عدد الأيام التي يبقى فيها الموقع الإلكتروني المزيف على الشبكة الإلكترونية (Anti-Phishing Working Group, 2008)

التمارين

التمرين (٣-١):

أنت في أمان من سرقة هويتك

اطلب من الطلاب أن يقوموا باختبار معلومات الأمن المثالية على الحاسوب للوقاية من سرقة الهوية Identity Theft PC Perfect Information Safety Quiz الموجود على الموقع الإلكتروني في مركز مصادر سرقة الهوية Identity Theft Resource Center وقم بجمع نتائجهم في الاختبار. قم بزيارة المركز على الرابط التالي:
www.idtheftcenter.org/artman2/publish/c_theft_test/Fact_Sheet_118_PC_Perfect_-_information_Safety_Quiz.shtml

وهنالك اختبار بديل أقصر لتقييم المخاطر على الشبكة الإلكترونية لسرقة الهوية والمتوفر من قبل TDBankNorth على www.tdbanknorth.com/bank/onlinerisks1.aspx

لمزيد من المعلومات أو لأبحاث الطلاب، يستطيع الطلاب زيارة مركز مصادر سرقة الهوية Identity Theft Resource Center (www.idtheftcenter.org) والنقر على Scams و Consumer Alerts.

التمرين (٣-٢):
كيف تحدث سرقة الهوية على الشبكة الإلكترونية

اطلب من طلابك إعداد قائمة بجميع الطرق التي يستطيعون التفكير بها والتي يستطيع من خلالها شخص ما بالوصول إلى حساباتهم الشخصية على الشبكة الإلكترونية. تتضمن هذه الطرق البريد الإلكتروني، والتراسل الفوري IM، والبنوك، والألعاب، وحسابات التواصل الاجتماعي. قد يختار المعلمون قيام الطلاب بالعمل في مجموعات صغيرة للنقاش. إذا كانوا بحاجة لمساعدة في تطوير الأفكار، اطلب منهم التفكير في خبراتهم الشخصية في تسجيل الدخول. أين توجد الحواسيب التي يقومون بتسجيل الدخول عليها؟ كيف يصلون إلى المواقع الإلكترونية الخاصة بهم ومن ثم يسجلون الدخول؟ هل من الممكن بالنسبة لهم ترك سجل لعمليات التسجيل الخاصة بهم للآخرين ليراقبوا ما يعملونه بدون معرفتهم؟ هل يستطيعون الوثوق بجميع أصدقائهم؟

يجب أن تتضمن القائمة التي يعدها الطلاب معظم ما يلي:

- يقوم الطلاب بإعطاء كلمات المرور الخاصة بهم إلى أصدقائهم، والذين بدورهم قد يمرروها لآخرين. إن هذا هو أكبر سبب لسرقة الهوية بين الطلاب.
- يرى أحدهم الطالب وهو يدخل كلمة المرور. تعد عملية سرقة الهوية الملقبة بـ "من وراء الكتف" يتم ارتكابها بسهولة لأن الطلاب في العادة لا يأخذون بعين الاعتبار أو يحترمون خصوصية الآخرين بينما يتواجدون على الحاسوب.
- لا يقوم الطلاب بتسجيل الخروج بشكل ملائم من الحاسوب، مما يسمح لأحد ما بالوصول إلى حساباتهم بعد ذهابهم.
- يقوم الطلاب بالتأشير على مربعات مثل "تذكرني على هذا الحاسوب" و "تذكر كلمة المرور الخاصة بي".
- يستخدم الطلاب كلمات المرور التي يستطيع الاشخاص الذين يعرفونهم التكهن بها أو التي يمكن اختراقها بمساعدة برنامج لاختراق كلمة المرور.
- قد يترك الطلاب، مثل العديد من المراهقين، كلمة المرور مكتوبة على ورقة بالقرب من أجهزة الحاسوب الخاصة بهم أو في دفتر ملاحظاتهم.
- قد يلتقط مسجل المفاتيح أو برنامج التجسس أو تطبيقات القرصنة الأخرى على جهاز حاسوب كلمة مرور. تزداد الخطورة عندما يقوم الطلاب بالتأشير على مربعات مثل "تذكر كلمة المرور الخاصة بي".

- قد ينخدع الطلاب ويدخلون كلمات المرور الخاصة بهم على موقع مزيف، مثل الموقع المزيف لـ MySpace، وFacebook أو صفحات البنوك. وهم في العادة يصلون إلى مثل هذه المواقع من خلال النقر على رابط غير حقيقي في بريد الكتروني. إن المواقع الوهمية مصممة لتبدو تمامًا مثل المواقع الحقيقية.

التمرين (٣-٣):

سرقة الهوية: ما الذي يجب عمله؟

قم بسؤال الطلاب السؤال التالي: إذا شككت في أن كلمة المرور الخاصة بك أو هويتك قد سرقت، ما الذي يجب عمله بخصوص ذلك؟ يجب أن تتضمن إجابات الطالب ما يلي:

- أقوم على الفور بتغيير كلمة المرور الخاصة بالحساب الذي تم اختراقه.
- أقوم على الفور بتغيير كلمة المرور لجميع الحسابات الأخرى والتي استخدم فيها نفس كلمة المرور.
- أقوم بالاتصال بإدارة الموقع الإلكتروني أو مركز خدمة العملاء لإبلاغهم، وإذا كنت أعرف كيف حصل، أقوم بإعلامهم بذلك.
- أقوم بإخبار والدي!
- إذا كان حسابا من المدرسة، أقوم بإعلام مشرف المدرسة.
- أقوم بالاتصال مع أصدقائي وبقية أفراد عائلتي في حال قام أحد يدعي أنه أنا بالتواصل معهم.

التمرين (٣-٤):
كيف يتأكد الطلاب؟

اطلب من الطلاب العمل في أزواج للتوصل إلى طريقة يستطيع فيها صديقان التأكد من أنهما يقومان بالتراسل الفوري مع بعضهما او إرسال الرسائل الإلكترونية لبعضهما البعض وليس أحد آخر يدعي أنه أحدهما. قم بمشاركة هذه الأفكار مع الصف.

التمرين (٣-٥):
التحايـل

يحاول منتحلو الشخصية في بعض الأحيان خداع الآخرين على الشبكة الإلكترونية من خلال اختيار أسماء مستخدمين تبدو تمامًا مثل أسماء المستخدمين التي يعرفها الطلاب ويثقون بها. افترض بأن اسم المستخدم الخاص بأفضل صديق لأحد الطلاب هو Cooldude123.

ما مدى سرعة اكتشاف الطلاب الفرق بين اسم الصديق والأسماء المشابهة أدناه:

أ. C00ldude123
ب. Coo1dudel23
ت. Cooldude1123

المفتاح

- الاختيار "أ" يستخدم الأصفار بدلا من الحرف o في كلمة cool.
- الاختيار "ب" يستخدم الرقم ١ بدلا من الحرف "l" والعكس صحيح في مكان وجودهما في الاسم.
- الاختيار "ت" يستخدم رقم ١ إضافي.

ماذا إذا كان اسم المستخدم لصديق الطالب هو Holygrail012؟

ما مدى سرعة اكتشاف الطلاب الفرق بين اسم الصديق والأسماء المشابهة أدناه:

أ. Holygrail0l2
ب. Holygrai1O12
ت. Ho1ygrai10l2
ث. Hollygrail012

المفتاح

- الاختيار "أ" يستخدم الحرف l بدلا عن الرقم ١.
- الإختيار "ب" يستبدل الحرف O بدلا من الصفر.
- الإختيار "ت" يستخدم الرقم ١ بدلا من الحرف l في موقعين ومن ثم يستخدم الحرف l بدلا من الرقم ١ قبل الرقم ٢ مباشرة.
- الإختيار "d" يكتب كلمة Holy كالآتي Holly

المصادر

Anti-Phishing Working Group (APWG) website: www.antiphishing.org
إن مجموعة مكافحة الإحتيال هي عبارة عن مؤسسة مكرسة للحد من سرقة الهوية والتزوير التي تنتج عن الاحتيال وانتحال الشخصية. توفر هذه المؤسسة منتدى لمناقشة قضايا الإحتيال ومجموعة قيمة وكبيرة من المعلومات حول هذا الموضوع.

Facet sheet 127: Blog sense. (2007, April 22).
متوفر في الموقع الإلكتروني لـ ITRC (مصدر مصادر سرقة الهوية):
www.idtheftcenter.org/artman2/publish/t_facts/Fact_Sheet_127.shtml

الموقع الإلكتروني لمحاربة سرقة الهوية Fighting Back Against Identity Theft:
www.ftc.gov/bcp/edu/microsites/idtheft/
يوفر هذا الموقع الحكومي معلومات مفصلة لمساعدة الزوار على اكتشاف ومكافحة سرقة الهوية.

Gartner Research. (2007, September 17). *Gartner survey shows phishing attacks escalated in 2007; More than $3 billion lost to those attacks.*
متوفر في الموقع الإلكتروني لـ Gartner:
www.gartner.com/it/page.jsp?id=565125

الموقع الإلكتروني لـ Identity Theft Prevention and Survival: www.identitytheft.org
تم إنشاء هذا الموقع الإلكتروني من قبل محامي يركز على قضايا الخصوصية ويوفر مجموعة متنوعة من المعلومات حول الوقاية والأمان من سرقة الهوية.

Phishing facts (n.d.)
متوفر في الموقع الإلكتروني لـ SonicWALL: www.sonicwall.com/phishing/

preventing identity theft online. (n.d.)
متوفر في الموقع الإلكتروني لـ TD Banknorth:
www.tdbanknorth.com/bank/preventingidtheft_online.html

teen space. (n.d.)
الموقع الإلكتروني لمحاربة سرقة الهوية Fighting Back Against Identity Theft:
www.idtheftcenter.org/teen/teen.html

الفصل الرابع

الاستجابة لأوضاع غير مريحة على شبكة الإنترنت
Responding to uncomfortable Online Situations

يتردد معظم البالغين بالاعتراف بشعورهم بالخوف أو عدم الراحة على الشبكة الإلكترونية.

يقدم الإنترنت عالمًا من الإثارة والفرص التعليمية للأطفال والمراهقين والبالغين. لسوء الحظ، عندما يشعر الطلاب بارتياح متزايد في الدخول إلى الإنترنت، تتنامى مخاطر التحرش والصور الغرافيكية غير الملائمة والإرهاب بشكل مطرد.

في الأيام الأولى للإنترنت، كانت المواد الإباحية والتحرش هي أكثر ما يتكلم عنه الناس عندما يتعلق الأمر بالشعور بعدم الارتياح على الشبكة الإلكترونية. واليوم، تكون فرصة تعرض الأطفال والمراهقين للأذى والقلق أو الشعور بعدم الارتياح واقعية جدًّا وشائعة جدًّا ويمكن أن تتولد من التراسل الفوري وحسابات البريد الإلكتروني ومواقع التواصل والتواصل الاجتماعي وغرف المحادثة ومناطق اللعب ومواقع العنف أو المواقع الإباحية التي يمكن العثور عليها بالصدفة.

> واحد من ثمانية طلاب تقريبا ممن تتراوح أعمارهم ما بين ٨ ـ١٨ عامًا اكتشف أن الشخص الذي يتواصل معه على الشبكة الإلكترونية كان شخصًا بالغًا يتظاهر بأنه أصغر منه سنًّا (Polly Klaas Foundation, 2006).

من خلال خبرتنا مع آلاف طلاب المدارس، وجدنا انه يمكنك التوجه بالسؤال إلى أية مجموعة من الأطفال أو المراهقين بما في ذلك طلاب المرحلة الثانوية- سوف يجيب بعض الطلاب بأنهم شعروا بعدم الإرتياح خلال الأسبوع الماضي. التمرين ٤–١ – التجارب السلبية على الشبكةالإلكترونية يطلب من الطلاب مناقشة الطرق التي قاموا بها ليشعروا بعدم الراحة عند وجودهم على الشبكة الإلكترونية. وعلى المستوى العالمي، سوف يجيب الطلاب بأنهم تمازحوا مع آخرين أو تم التواصل معهم من قبل أشخاص غرباء في غرف المحادثة أو مواقع التواصل الاجتماعي. بصرف النظر عن أعمارهم، سوف يقوم الطلاب بالإبلاغ عن التجارب السلبية التالية:

- التعرض للمواد الإباحية.
- الاتصال من قبل غرباء.
- التهديدات وأعمال التحرش والسخرية.

- التعرض للخداع او الاستغباء أو الاستغلال.

قم بالتأكيد على طلابك أنهم دائما مسيطرين عندما يكونون على الشبكة الإلكترونية. وإن لديهم القوة للخروج من التطبيق أو المتصفح أو إغلاق الحاسوب عندما يشعرون بعدم الإرتياح. عندما يكونون على الشبكة الإلكترونية، لا يجب عليهم الاستجابة لأي وضع سلبي. يجب أيضًا تشجيع الطلاب للإبلاغ عما حصل إلى والدهم أو أي شخص بالغ آخر يثقون به. التمرين ٤–٢ – الحوارات على الشبكة الإلكترونية تسمح للطلاب باكتشاف الحوارات غير المريحة على الشبكة الإلكترونية ومناقشة الحلول الممكنة.

التمارين

التمرين (٤-١):

التجارب السلبية على الشبكة الإلكترونية

اطلب من الطلاب عمل قائمة بالطرق المختلفة التي يقوم بها الأطفال المراهقون للوصول إلى الشعور بعدم الإرتياح على الشبكة الإلكترونية. سوف يتردد معظم المراهقين بالاعتراف بالشعور بالخوف أو عدم الارتياح على الشبكة الإلكترونية. من الأفضل في العادة الطلب منهم التفكير بالشروط العامة أو شروط التعامل مع الأصغر سنًّا.

التمرين (٤-٢):
الحوارات على الشبكة الإلكترونية

قم بمناقشة الحوارات التالية مع طلابك. اطلب منهم كتابة أفكارهم الخاصة قبل الإجابة كمجموعة. قم بالإشارة إلى أن الطلاب يجب أن يقوموا دائمًا بإخبار والدهم أو أي شخص بالغ حول شعورهم بعدم الارتياح. إن هذا الأمر صعب جدًّا للعديد من الأشخاص اليافعين، لذلك يحتاجون إلى التشجيع.

الحوار (أ)

سارة طالبة في الصف الثامن وتقوم بعمل بحث لمشروع للدراسات الإجتماعية حول الحقوق المدنية. وخلال قيامها بالبحث، وجدت سارة موقعًا إلكترونيًا يبدو أنه يتحدث عن مارتن لوثر كنغ الإبن ولكنه في الواقع موقع معادي تم إنتاجه من قبل مجموعة يسودها حكم البيض. شعرت بإنزعاج جديد ولكنها كانت خائفة من إخبار أحد لأنها لا ترغب بإحداث مشاكل.

قم بسؤال طلابك ما يلي:

١. ما الذي تعتقد أنه أهم شيء يجب أن تقوم به سارة؟

الحوار (ب)

جاك، طالب بالسنة الثانية في الكلية، يجلس على مكتبه في المنزل ويرسل رسائل فورية. تلقى رسالة من شخص ما يدعي أنه صديقه.تقول الرسالة: " أنا أكرهك يا جاك." لم يكن جاك متأكدا من أنه يعرف اسم المستخدم.

قم بسؤال طلابك ما يلي:

١. ماذا يمكن أن يكون قد حصل لجاك؟
٢. ما الذي تعتقد أنه أهم شيء يجب أن يقوم به جاك؟

الحوار (جـ)

إيمي ، طالبة في السنة الأولى في الجامعة، تقوم بالتراسل الفوري مع صديقة مقربة لها. وفجأة، أصبحت المتعة والتواصل الذي لا يقاوم مع صديقتها إلى وضع وضيع ووقح. لم تفهم إيمي ما الذي كان يحدث.

قم بسؤال طلابك ما يلي:

١. ماذا يمكن أن يكون قد حصل لإيمي ؟
٢. ما الذي تعتقد أنه أهم شيء يجب أن تقوم به لإيمي ؟

بناء على الإجابات المقدمة على هذه الحوارات، اطلب من الطلاب كتابة قائمة بأفضل الإستراتيجيات المناسبة للأطفال والمراهقين عندما يوجهون أوضاعًا غير مريحة على الشبكة الإلكترونية. يجب ان تركز إجابات الطالب على إيقاف التحرش أو التسلط فورًا وإزالة المحتوى العدائي من الشاشة. بناء عليه، يجب أن تتضمن الإجابات ما يلي:

- مغادرة المتصفح.
- مغادرة التطبيق.
- إغلاق الحاسوب.
- القيام دائما بإخبار شخص بالغ أو الوالد.

سوف يميز معظم الطلاب على الفور بأن ما يمكن أن يكون قد حدث لأيمي على الأرجح هو أن شخصا آخر قد جلس على شاشة التراسل الفوري بدلاً من صديقتها المقربة. إن هذا الأمر يحدث دائمًا، على سبيل المثال عندما يكتب صديق "س.أ.ف" "brb" والتي تعني "سأعود على الفور" "be right back" من أجل الذهاب إلى الحمام ويجلس أحد أشقاءه ويتظاهر أنه الشخص الذي غادر للتو. اطلب من الطلاب كيف يكونون متأكدين بشكل مطلق بأنهم يعرفون دائما مع من يتكلمون عندما يستخدمون التراسل الفوري. إحدى الإقتراحات، التي تم تزويد المؤلفين بها من قبل إثنين من طالبات الصف السابع في نيويورك، والتي مفادها أن لديهن مجموعة من كلمات المرور التي لا يتشاركنها ابدًا مع أي أحد. وفي اللحظة التي قامت إحداهن بالتواصل مع أخرى عبر التراسل الفوري، فإن أول شيء كتبتاه هو إحدى كلمات المرور. وإن تركتا الحاسوب لدقيقة واحدة فقط أو دقيقتين، فإن أول شيء يبدأن به محادثتهن هو تبادل كلمات المرور. كانت هذه فكرة فعالة جدًّا.... ما دام لا يعرف كلمات المرور الخاصة بهن أي شخص آخر.

المصادر

Polly Klaas Foundation. (2006) *Internet safety: Realistic strategies & messages for kids taking more and more risks online*.

متوفر في الموقع الإلكتروني:
www.pollyklaas.org/internet-safety/internet-pdfs/pkfsummary.pdf

الموقع الإلكتروني لـ Stop Bullying Now: www.stopbullyingnow.com
يصف هذا الموقع الإلكتروني ما يعرضونه بوصفه "الإستراتيجيات القائمة على البحث العملي لتقليل الإرهاب في المدارس".

الفصل الخامس

الاستجابة للمضايقة على الشبكة العنكبوتية
Responding to Cyberbullying

قم بالتأكيد على الطلاب أن القدرة على السيطرة بين أيديهم ويمكنهم إيقاف المضايقة فورًا أثناء التواجد على الشبكة الإلكترونية.

هل يعتقد طلابك أنهم يعرفون ما يعنيه المضايقة على الشبكة العنكبوتية؟ هل عاملوا أحد بطريقة يمكن اعتبارها مضايقة؟ اطلب من الطلبة القيام باختبار قصير حول المضايقة من خلال زيارة الصفحة الإلكترونية Directgov للمضايقة على الشبكة العنكبوتية (http://yp.direct.gov.uk/cyberbullying/) والنقر على الرابط "Are you part of it?"

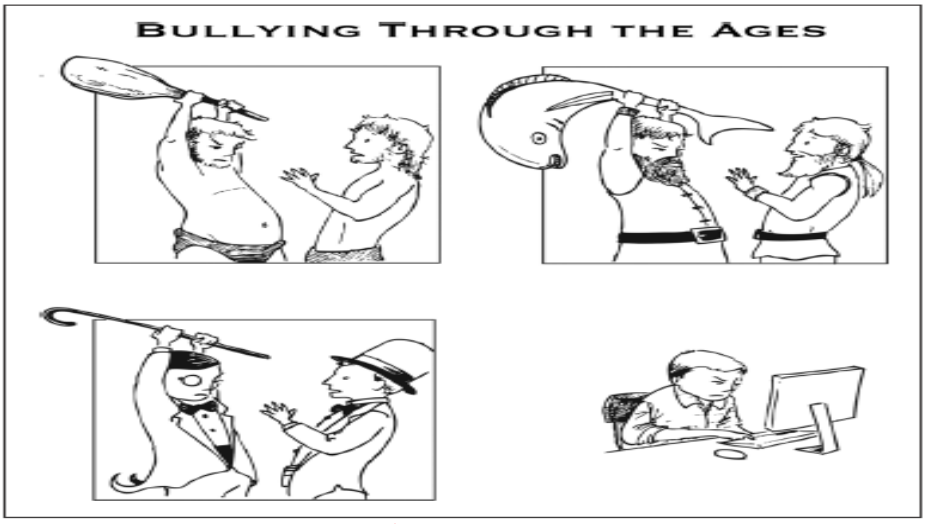
إن المضايقين على الشبكة الإلكترونية هم عبارة عن أشخاص يحاولون إلحاق الأذى والتخويف والتضييق بشكل مؤذي للآخرين. يقومون بعمل هذا الأمر بوساطة ما يقولونه وما يفعلونه للآخرين على الشبكة الإلكترونية. تتضمن جهودهم الإساءة اللفظية مثل الاستحقارات ونعتهم بألقاب والتهديدات واستخدام لغة التحرش. في بعض الأحيان، يكون المضايقة على الشبكة العنكبوتية، وفي أحيان أخرى تكون لغة بذيئة. التمرين ١–٥ – ما الذي يريده المتسلطون على الشبكة الإلكترونية؟ يكشف العقليات وطرق التفكير المحتملة التي تقف وراء المضايقة؟

> يعاني ما يقارب ثلث المراهقين المتواجدون على الشبكة الإلكترونية من بعض أشكال التسلط. تتعرض الفتيات بشكل أكبر للتسلط من الأولاد (Lanhart, 2007).

إن شخصا تعرض يوما ما للمضايقة يعرف مدى سوء التعرض للمضايقة وقد يشعر بأن لا قوة له وليس بيده حيلة لإيقافه. إن الأطفال والمراهقين على حد سواء يستجيبون للمضايقة بإحدى الطريقتين التاليتين. إحدى الإجابات هي أنهم يحاولون تغيير أو إعادة توجيه المحادثة أو توجيه أسئلة للمضايقة. الإجابة الثانية التقليدية هي أنهم يحاولون "رد الإساءة" من خلال التحدث بنفس الأشياء المزعجة. إن كلاً من هاتين الإجابتين هما تمامًا ما يريده المضايقة! التمرين ٥–٢ – لا تشعروا المضايق بالرضا، يساعد على تزويد الطلبة بآليات لتجنب المضايقة وكيفية الاستجابة بشكل أفضل.

معظم الألعاب المؤلفة من عدة لاعبين على الشبكة الإلكترونية والشبكات الاجتماعية وخدمات المحادثة ومنتديات الحوار تزود الأعضاء بتقرير للإساءة أو التحرش

من قبل أي عضـــــــــــو آخر. تتضمن هذه المواقع مواقع الأطفال المألوفة مثل : Club Penguin، و NeoPets، و Webkinz والشبكات الاجتماعيـــــــــــــــــــــة مثل: الفيسبوك Facebook و MySpace و LiveJournal.



الشكل (٥-١): تطور المضايقة

وحتى المواقع مثل YouTube و Flickr توفر طريقة للزوار للتأشير على المحتوى بأنه غير ملائم. التمرين ٥–٣ – الإبلاغ عن الإساءة على الشبكة الإلكترونية يساعد الطلاب على فهم أهمية الإبلاغ عن الإساءة على الشبكة الإلكترونية وكيفية توثيق الإساءة في تقرير.

كما يمكنك تخصيص التمرين ٥–٣ كواجب منزلي للطلاب وتقديم تقرير للصف. إن أهم شيء حول هذا التمرين هو أن الطلاب يفهمون أن معظم المواقع الإلكترونية توفر وسيلة للإبلاغ عن الإساءة. يجب أن تؤكد أنه إن حدثت الإساءة على موقع إلكتروني، يجب أن يشرك الطلاب أولياء أمورهم أو الأوصياء عليهم.

يوفر مجلس الإعلانات Ad Council ومجلس الوقاية من الجريمة National Crime Prevention Council تحقيقًا واقعيًا حول المضايقة على الشبكة العنكبوتية في المقطعين المصورين التاليين:

- www.youtube.com/watch?v=QYaWNYXpBis
- www.youtube.com/watch?v=OQyMvG99w

إذا كنت ترغب بتجنب بعض عمليات التشويش المتعلقة بإحدى صفحات YouTube يمكنك استخدام أحد التطبيقات التي تحول المقاطع ذات الإمتداد FLV وهي خدمة موجودة على الإنترنت وحفظ مقطع اليوتوب على سطح مكتب حاسوبك الخاص. وتتضمن هذه كل

مـــــــــــــــن Vixy.net، ConvertDirect.com، و Catchvideo.net.ويوفر لك محرك البحث في غوغل عن الكلمات "FLV YouTube converter" بقائمة طويلة من الاختيارات.

دليل إيجابي: توثيق الإساءة

أخبر طلابك بالأخذ بعين الا عتبار إن كان يجب عليهم توثيق إن كان أحد ما يتحرش بشخص آخر. إذا كان هنالك شخص يهددك في الواقع لإلحاق الأذى بالآخرين، يكون من الضروري قيامهم بتوثيقها. يمكن القيام بذلك إما بوساطة: ١) طباعة ما تم قوله في التواسل الفوري أو في بريد إلكتروني أو في الرسائل في غرفة محاثة أو في منتدى على الشبكة الإلكترونية، أو ٢) نسخ وحفظ هذه الوثائق إلى ملف منفصل. قد يكون هذا السجل مفيدًا جدًّا للشرطة وكذلك لأولياء الأمور.

التماريـــن

التمرين (٥-١):
ما الذي يريده المضايقون على الشبكة الإلكترونية

اسأل طلابك أي نوع من الإجابات العاطفية التي يتوقعون أن المضايق على الشبكة الإلكترونية يرغب بالحصول عليها من ضحيته سواء أكان ذكرًا أم أنثى. اطلب من الطلاب التركيز على الإجابة العاطفية للضحية. قد تتضمن الإجابات الغضب أو الأذى أو الألم أو الإحراج.

والآن، قم بتذكير الطلاب أن أية إجابة لمضايق على الشبكة الإلكترونية تبعث الرسالة التي يرغب المضايق في سماعها. يعرف المضايق أن الضحية منزعج أو غاضب، وهو تماما ما يرغب به المضايق.

التمرين (٥-٢):
لا تشعروا المضايق بالرضا

قم بسؤال طلابك السؤال التالي: إذا تعرضت للمضايق على الشبكة الإلكترونية، ما أفضل إجابة لا تمنح المضايق الإجابة التي تشعره بالرضا على الإطلاق؟

يجب أن تتضمن الإجابات تسجيل الخروج أو الخروج من التطبيق أو إغلاق التطبيق وهكذا. إن الهدف هو إنهاء الاتصال على الفور وعدم الاستجابة للمضايق، وبالتالي لا يحصل المضايق على أية تغذية راجعة بأن الضحية المحتملة قد إستجاب له.

قم بالتأكيد على الطلاب أنهم يتولون السيطرة ويمكن إيقاف المضايق على الفور. قم بتذكير الطلاب بأن لا أحد يستحق أن يعامل بصورة سيئة. كما قم بالتأكيد على أهمية إخبارهم بشخص بالغ بالأمر بحيث لا يسمح للمضايق بالتحرش بالآخرين. أخبر طلابك بعدم منح المضايق أي نوع من الرضا عبر اتباع طريقة أن عدم توفير أي إجابة هي أفضل إجابة. اطلب منهم تسجيل الخروج على الفور.

إذا استمر الطلاب بالتعرض للاتصال من قبل مضايق كلما سجلوا الدخول، فإن هنالك العديد من الخطوات التي يمكنهم القيام بها:

- تقديم تقرير عن المضايق للموقع الإلكتروني أو الخدمة على الشبكة الإلكترونية.
- طباعة الرسائل من المضايق أو حفظها كدليل للسلطات.
- إخبار شخص بالغ يمكن الوثوق به مثل أحد الوالدين أو معلم والذي يستطيع التحدث مع السلطات.
- قم بابتكار اسم مستخدم جديد ووقف استخدام الاسم المستهدف من قبل المضايق.

التمرين (٥-٣):
الإبلاغ عن الإساءة على الشبكة الإلكترونية

إسال الطلاب إن كانوا يعرفون كيفية الإبلاغ عن الإساءة على المواقع الإلكترونية التي يستخدمونها باستمرار. اطلب منهم اختيار أكثر ثلاثة مواقع يستخدمونها عندما يتفاعلون مع الآخرين. اطلب منهم زيارة الصفحة الرئيسة لكل موقع ومشاهدة إن كانوا يستطيعون العثور على كيفية الإبلاغ عن الإساءة. قد تختار تقسيم الطلاب في مجموعات لزيارة مواقع متعددة ومن ثم يتشاركون نتائجهم مع الصف. سوف تختلف الإجابات حسب المواقع الإلكترونية المختارة.

المصـــادر

Bullying myths and facts. (n.d.)
متوفر في الموقع الإلكتروني Bullying.org:
www.bullying.org/external/documents/Bullying/.org_Bullying_Myths-facts%20Pamphlet.pdf

الموقع الإلكتروني Bullying.org: www.bullying.org
هذا الموقع الإلكتروني مخصص لزيادة الوعي حول التسلط وتعليم طرق لتجنبه.

الموقع الإلكتروني للمضايق على الشبكة العنكبوتية Cyberbullying:
http://yp.direct.gov.uk/cyberbullying/
إن هذا موقع ممتاز تم إنتاجه من قبل الحكومة البريطانية ومصمم بشكل رئيس للمراهقين كمصدر للتعامل مع التسلط على الشبكة العنكبوتية.

Dealing with cyberbullying. (n.d.)
متوفر في الموقع الإلكترونيDirectgov:
www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/DG_070502

Lenhart, A. (2007, June *27). Cyberbullying and online teens.*
متوفر في الموقع الإلكتروني PEW/INTERNET:
www.pewInternet.org/PPF/r/216/report_display.asp
إن هذا عبارة عن تقرير من Pew Internet و American Life Project

الموقع الإلكتروني Pacer Center's Children Against Bullying:
www.pacerkidsagainstbullying.org
تم إنشاء هذا الموقع من قبل المركز القومي للوقاية من المضايق National Center for Bullying Prevention وهو مصمم للطلاب الشباب. تتضمن المصادر المحتويات ومقاطع الفيديو حول ما يعنيه التسلط وكيف يبدو وما الذي تستطيع القيام به تجاهه.

What is bullying? (n.d.).
متوافر في الموقع الإلكتروني لـ Bullying.org:
www.bullying.org/external/documents/Bullying.org_Bullying_Myths-facts%20Pamphlet.pdf

الموقع الإلكتروني لحماية الشباب ضد العنف Youth Violence Prevention:
www.safeyouth.org/scripts/topics/bullying.asp

تم إنشاء هذا الموقع من قبل المركز القومي لمصادر حماية الشباب ضد العنف National Youth Violence Prevention Resource center ويتم تمويله من قبل مراكز السيطرة على الأمراض والوقاية Centers for Disease Control and Prevention. كما انه يحتوي على العديد من المقالات والمصادر ووثائق حول الحقائق المتعلقة بالتسلط وكيفية الإستجابة له.

الفصل السادس

التراسل الفوري
Instant Messaging

يعد التراسل الفوري أداة ضعيفة للتعرف على أشخاص للمرة الأول ومحاولة بناء صداقة.

ما الذي يجعل التراسل الفوري شيئًا فريدًا من نوعه؟

لا يمكن مقاومة التراسل الفوري IM من قبل الطلاب بسبب وجود شخص ما دائمًا على الشبكة الإلكترونية يرغب في التحدث معهم. الرسالة الضمنية هي أن شخصًا ما يجدهم مهمين أو معجب بهم. ويقدر ما يكون التراسل الفوري ممتعًا، إلا أنه في الواقع شكلاً ضعيفًا جدًّا للتواصل وذلك لأسباب عديدة سوف نناقشها في هذا الفصل. إن الأطفال والمراهقين في العادة غير مستعدين من الناحية التنموية لاتخاذ قرارات حكيمة على الشبكة الإلكترونية، وبخاصة عندما يستخدمون التراسل الفوري حيث يمكن أن ينتقل الاتصال بسرعة الضوء. التمرين ٦–١–محادثة تقليدية على التراسل الفوري يطلب من الطلاب مناقشة محادثات تقليدية على الشبكة الإلكترونية والأخذ بعين الاعتبار محاسن ومساوئ التراسل الفوري.

إن أدوات التراسل الفوري هي بالتأكيد ليست سيئة بالفطرة، ولكن الأطفال والمراهقين يستخدمون بشكل متزايد أدوات الاتصالات المعنية بطرق مؤذية. فهم ما زالوا صغارًا جدًّا ليتوقعوا عواقب سلبية محتملة. بالنسبة للأطفال حتى الصف الثامن، يكون التراسل الفوري في العادة بمحض الاختيار عندما تكون نيتهم إلحاق الأذى بمشاعر شخص ما. في بعض الأحيان، يستخدم الطلاب لغة وضيعة ومؤذية في التراسل الفوري والسبب في ذلك انهم يستطيعون عمل ذلك فقط. وتغير النبرة المؤذية والوضيعة في العادة للتراسل الفوري الطريقة التي يرى بها الأطفال اللغة والسلوك. فهم يصبحون وبشكل متزايد أقل حساسية للغة التحرش. فعندما يتعرضون للغة التحرش، فقد تسمح وبشكل مستمر تعليقات مثل "الجميع يتحدث بهذه الطريقة" أو "إنه ليس أمرا مهما". التمرين ٦–٢ – الإتصال:التراسل الفوري بين شخصين يطلب من الطلاب التمعن في الأسباب التي تجعل من السهل على الطلاب الآخرين التحدث بأمور وضيعةعندما قيامهم بالتراسل الفوري.

كما يلجأ الطلاب أيضًا إلى التراسل الفوري لحل الخلافات مع أصدقائهم، والعثور على أصدقاء جدد. لسوء الحظ، فإن محددات التراسل الفوري تجعله أداة ضعيفة لعمل أي منهما. إن نقص النماذج الاجتماعية (على سبيل المثال: نبرة الصوت والتعبير) من

المشاركين يمكن ان يؤدي بسهولة إلى إساءة فهم النية. إن الإحساس بالغفلة أثناء استخدام التراسل الفوري ووتترافق مع الفظاظة الاعتيادية والتبادل السريع للرسائل والتي تدفع بعض الطلاب للتحدث بأمور لا يجب التحدث بها في العادة شخصيًا. قد يؤدي هذا الأمر إلى تصاعد الخلاف بدلاً من التوصل إلى حل. عندما يستخدم الطلاب التراسل الفوري للعثور على أصدقاء جدد، قد لا يدركون أنه يكون في غاية الصعوبة تطوير أهم مميزات الصداقة مثل الثقة والولاء أثناء استخدام التراسل الفوري. يحتاج الطلاب إلى تمييز الاوقات التي لا يكون فيها التراسل الفوري افضل طريقة للتواصل. التمرين ٦–٣ – محددات التراسل الفوري يطلب من الطلاب إعداد قائمة بالأوقات التي يكون من الأفضل القيام فيها بمحادثات عبر الهاتف أو بلقاء شخصي. كما أنه يطلب من الطلاب إعداد قائمة بأنواع ومميزات الصداقة ومن ثم الاخذ بعين الإعتبار مدى صعوبة اكتشاف هذه المميزات عبر التراسل الفوري.

وبشكل متزايد، يتجه المراهقون نحو التراسل الفوري والبريد الإلكتروني وشبكات التواصل الاجتماعي لتجنب المحادثات الصعبة في الحياة مثل إنهاء علاقة مع صديق أو صديقة أو التعبير عن غضب من حدث ما أو التحدث عن جرح المشاعر. إذا واصلوا الاعتماد على الوحدة على جهاز الحاسوب بوساطة استخدام الحاسوب لتجنب المواجهة، فإنهم سيتأخرون أو يتجنبون مع بعضهم بناء مهارات الحياة في الإتصال التي يرغب كل شخص في تطويرها. التمرين ٦–٤ – طرق عديدةلتوصيل رسالة يناقش حقيقة ان التراسل الفوري يتيح للاشخاص الإختبار وراء الحاسوب ويمنحهم إحساسا مزيفا بعدم المسؤولية.

أخيرًا، يجد معظم المدرسين جوانب أخرى لخيبة الامل من التراسل الفوري لأن أضراره تكون على تطور اللغة:

- لا توجد حاجة للتهجئة الصحيحة.
- لا يوجد بناء للقواعد أو الجملة
- استخدام الرموز العاطفية (وهي عبارة عن رموز مفتاحية تمثل إحدى تعابير الوجه، وبالتالي تعبر عن المشاعر) كلغة للتعبير والتواصل.

"الأصدقاء" على التراسل الفوري IM

قبل ١٥ عامًا فقط، تواصل الناس بالهاتف أو بالرسائل المكتوبة. لم يسمع العديد من الأشخاص بالبريد الإلكتروني أو التراسل الفوري. اليوم، يرسل العديد من البالغين الرسائل الإلكترونية كوسيلتهم الرئيسة للاتصال التي تقدر ببلايين الرسائل الإلكترونية المرسلة يوميًا. يقضي الأطفال والمراهقين معظم وقتهم باستخدام التراسل الفوري للمحادثة في أوقات آنية مع أشخاص في المنطقة التي يقطنها أو حول العالم.

ومع وجود إمكانية الوصول إلى بلايين الأشخاص، تغير تعريف كلمة "صديق". يكون الأصدقاء على الشبكة الإلكترونية في العادة أشخاصًا لا يعرفهم طلابنا شخصيًا في واقع الحياة. قد يكونون اشخاصًا التقى بهم الطلاب على الشبكة الإلكترونية بطريقة عشوائية. وفي استطلاع الرأي الذي قمنا به في ٢٠٠٧ – ٢٠٠٨م حول سلوك الطالب على الشبكة الإلكترونية، وجدنا أن ٢٠% من جميع الطلاب في الصفوف من الرابع إلى الثاني عشر أفادوا أن لديهم "أصدقاء افتراضيين" على الشبكة الإلكترونية ممن لم يقابلونهم شخصيًا على الإطلاق.

قد يجد الطلاب أنه وبسبب نقص الاستثمار في الحياة الواقعية في الصداقة أو الافتقار إلى المعرفة بهؤلاء "الأصدقاء الافتراضيين،" يميل هؤلاء الغرباء للتصرف بوضاعة أو التحرش أو إحباطهم أو خذل الثقة التي بينهم.

المحتالون على التراسل الفوري

يتعرض معظم الطلاب لأوضاع لا يشعرون فيها بالراحة من محادثاتهم على التراسل الفوري أو قد يبدو بطريقة ما خاطئة. قد يحدث هذا الوضع إذا كانوا يتحادثون مع محتال أو أحد يدعي أنه صديقهم. يجب أن يتم إرشادهم للثقة بغرائزهم إذا كانت المحادثة على التراسل الفوري تبدو فظة وإنهاء الاتصال. يستطيعون بعدها التواصل عبر الهاتف. يمكن أن يطور الطلاب كذلك وسائل للتأكد من أنهم يتحادثون مع الشخص الصحيح. التمرين ٦–٥ – المحتالون على التراسل الفوري، يستخدم الحوارات على الشبكة الإلكترونية لإعداد حلول وقائية وممكنة للحوادث غير المريحة في الحياة الحقيقية. التمرين ٦–٦ – المحتالون في كل مكان يرفع مستوى الوعي لدى الطالب حول ما يعنيه أن يكون محتالاً على الشبكة الإلكترونية ويكشف عن العدد الهائل من المحتالين على الشبكة الإلكترونية.

توصيات لأولياء الأمور

قد يشعر أولياء الأمور الذين لا يستخدمون التراسل الفوري بأنفسهم بالضياع عنما يتعاملون مع استخدام اطفالهم لهذا الشكل الجديد نسبيًا من الاتصال. يمكن أن يقدم المعلمون الكثير من التوجيه والإرشاد لأولياء الأمور ممن لا يفهمون كافة المسائل المرتبطة بالتراسل الفوري من خلال التوصيات التالي:

- منع التراسل الفوري حتى الصف السادس.
- تعلم كيفية حماية أطفالكم بالأدوات المتاحة، مثل حجب التراسل الفوري أو تثبيت برنامج لمراقبة المحادثات والمساعدة على إعداد الحدود الزمنية.
- معرفة الأطفال في قائمة أصدقاء أطفالكم.
- التواصل مع أولياء أمور الأطفال في قائمة أصدقاء أطفالكم.
- تحديد الدخول في التراسل الفوري ووقته.

- إجراء محادثات مستمرة مع أطفالكم حول مسائل تتعلق بالتراسل الفوري.
- تعليم اطفالكم التواصل بمسؤولية.

بالإضافة إلى ما سبق، وبسبب وجود العزلة على أجهزة الحاسوب والإحساس بعدم وجود أي نوع من المسؤولية، سوف يختبر العديد من الأطفال عمليات تحرش على الشبكة الإلكترونية من محتالين وأشخاص يعرفونهم. التمرين ٦–٧ – التحرش على الشبكة الإلكترونية، يستخدم حالة على الشبكة الإلكترونية للكشف عن كيفية إمكانية استجابة الطلاب لتحرش مزعج على الشبكة الإلكترونية.

التراسل الفوري والخصوصية

قد لا يكون طلابك قد أخذوا مطلقا بعين الاعتبار إن كانت محادثات التراسل الفوري خاصة. اسأل الطلاب: هل كل شيء خاص بالفعل على الشبكة الإلكترونية؟ في الحسابات ذات كلمات المرور المحمية، هل تشعر بأن ما تكتبه أو تضعه خاص؟ التمرين ٦–٨ – ليس أمرًا خاصًا جدًّا بعد كل شيء والتمرين ٦–٩ – احتفظ به لنفسك، يبين للطلاب أن المحادثات على الشبكة الإلكترونية ليست خاصة وقد تعود بالمستقبل بأثر سلبي عليهم وعلى أندادهم. التمرين٦–١٠ – نصيحة التراسل الفوري يطلب من الطلاب استخدام معرفتهم وخبرتهم لإعداد نصيحة للمستخدمين الصغار على الشبكة الإلكترونية مثل الأشقاء الصغار على سبيل المثال.

التمارين

التمرين (٦-١):

محادثة تقليدية على التراسل الفوري

اطلب من طلابك كتابة عدة سطور من حوار عادي على التراسل الفوري بين صديقين من نفس المدرسة. أخبرهم بأن تكون حقيقية بقدر الإمكان كما لو كانت تحدث بالفعل. اطلب منهم مناقشة إجاباتهم. كيف تبدأ المحادثة العادية على التراسل الفوري؟ ما هي الميزات الفريدة للتراسل الفوري؟ اسألهم كم درجة يمنحون التراسل الفوري كأداة للمحادثة. لماذا؟ اطلب منهم الأخذ بعين الاعتبار إيجابيات وسلبيات التراسل الفوري.

التمرين (٦-٢):

الاتصال: التراسل الفوري بين شخصين

للأسف، بعض الأطفال والمراهقين يتفوهون بأمور وضيعة أو يضايقون الآخرين لدى استخدامهم التراسل الفوري. قد يكون هذا صحيحًا على الرغم من أنهم في العادة لا يتصرفون بهذه الطريقة في المدرسة. اسأل الطلاب لماذا يعتقدون أنه من الأسهل لبعض الطلبة التفوه بأمور وضيعة عندما يستخدمون التراسل الفوري بينما لا يتصرفون بتلك الطريقة على أرض الواقع. إذا واجه الطلاب صعوبة في الإجابة، اسألهم عن الأمر المفقود على الشبكة الإلكترونية وموجود في المقابلة الشخصية أو على الهاتف؟

قم بتحفيز ما يلي في إجاباتهم:

- لا يتوجب عليكم رؤية الشخص.
- تم إرسال الرسالة ومن ثم حذفت ومن ثم تم نسيانها.
- يبدو أنه لا توجد أية عواقب للسلوك السيء.
- البالغون غير متواجدون على الشبكة الإلكترونية لمراقبة كيفية التصرف.
- قد يكون التراسل الفوري مجهولاً. تستطيع التظاهر أنك شخص آخر والتخلص من ذنب التصرف بوضاعة.

يواجه الشباب صعوبة في التفكير بالمستقبل كعائق لأفعالهم. على الرغم من أنهم قد يتعرضون للمواجهة حول التراسل الفوري الخاص بهم، إن ذلك التوقع قد لا يوقف الاندفاع الفوري.

التمرين (٦-٣):
قيود التراسل الفوري

يمكن أن يكون التراسل الفوري طريقة مسلية للتحدث مع الأصدقاء. في بعض الأحيان، يمكنهم الإنخراط في عدة محادثات على التراسل الفوري مرة واحدة. ومع ذلك، هنالك أوقات يكون فيها التراسل الفوري ليس أفضل طريقة للتواصل.

١. اطلب من طلابك إعداد قائمة بالأوقات المفضلة لإجراء محادثات على الهاتف أو الالتقاء شخصيًّا بدلاً من التراسل الفوري.

يجب أن تركز القائمة على المحادثات التي يكون من الصعب إجرائها؛ على سبيل المثال، يجب أن تتضمن أمور يساء فهمها، ومحادثات حول الأحاسيس المؤلمة، أو محادثات الغضب.

بشكل عام، تتصاعد المشاعر في المحادثات بشكل أكثر عندما يتم تسليمها عبر التراسل الفوري. توفر المحادثات على الهاتف أو الشخصية فرصة أقل لإساءة فهم نية شخص ما. في هذه الأنماط من المحادثات، تعتبر نبرة الصوت وتعابير الوجه حساسة لفهم المحادثة. إن المختصرات واللغة المختصرة للتراسل الفوري تؤدي على الأرجح إلى إساءة فهم المحادثات بشكل أكثر.

٢. اسأل الطلاب: عندما ترغب في التعرف على أصدقاء، ما نوعية الأصدقاء أو الميزات المهمة لك؟

اطلب من طلابك إعداد قائمة سريعة بنوعيات وميزات التي تهمهم في أصدقائهم الجيدين. استدعي الطلاب لمشاركي القوائم الخاصة بهم، وبناء قائمة رئيسة على اللوح أو الشاشة بحيث يستطيع الجميع مشاهدة الاستعداد للجزء الثاني من السؤال.

سوف تتضمن القوائم على الأرجح كلمات أو عبارات كالآتي:

الثقة.
الولاء.
الاهتمام.
العاطفة.
شخص يصغي إليك.
شخص يجعل لك دائمًا أولوية.

٣. قم بسؤال الطلاب: إذا كنت ترغب في التعرف على صديق للمرة الأولى على التراسل الفوري، أي من الميزات من السؤال الثاني يسهل تعلمها عن التراسل الفوري؟ أي من هذه الميزات يصعب معرفتها عن التراسل الفوري؟ لماذا؟

إن الهدف للطلبة هو إدراك أن العديد من الميزات المهمة للصداقة لا يسهل تطويرها عبر التراسل الفوري. إن التراسل الفوري عبارة عن أداة ضعيفة للالتقاء بالأشخاص للمرة الأولى ومحاولة تنمية الصداقة. يكون من السهل كثيرًا تضليل الآخرين وإخفاء حقيقة من تكون وإخفاء ميزاتك أو نواياك الحقيقية. الثقة، على سبيل المثال، من السهل خيانتها عبر استخدام التراسل الفوري بمهارة كسلاح ولكن من الصعب جدًّا بنائها باستخدام التراسل الفوري كأداة. قم بتشجيع الطلاب ليعيدوا النظر في استخدامهم للتراسل الفوري إنشاء صداقات جديدة.

التمرين (٦-٤):
هناك طرق عديدة لتوصيل رسالة

كان مارك Mark وكلير Claire صديقين منذ ثلاثة شهور، ولكن هذه العلاقة وصلت إلى نهايتها. لقد تغيرت مشاعر مارك ويريد إنهاء العلاقة مع كلير. كان عصبيًا جدًّا حول ما سيقوله لها كيف سيقوله. اطلب من الطلاب النظر إلى الخيارات أدناه. أي من الخيارات يعتبر اختيارا ضعيفا إن استخدمه مارك وأي منها ستكون خيارات أفضلها؟

١. يتصل مارك بكلير بالهاتف ليوصل رسالته.
٢. يرسل مارك إلى كلير رسالة إلكترونية يقول لها فيه بأن علاقتهما انتهت.
٣. يتصل مارك بكلير بالهاتف ويسألها إن كان يمكنه لقائها بعد المدرسة للتحدث معها عن أمر ما. ويخبرها بأنهما عندما يلتقيان يرغب بإنهاء علاقتهما.
٤. يتراسل مارك مع كلير عبر التراسل الفوري ليخبرها بقراره بإنهاء علاقتهما.
٥. يكتب مارك ملاحظة إلى كلير ويضعها في خزانتها قبل استراحة الغداء مباشرة.
٦. يترك مارك ملاحظة لكلير على حسابها على الفيسبوك مفادها أن علاقتهما قد انتهت.

قم بسؤال الطلاب: أي من الخيارات الستة أعلاه:

١. تفضل بأن يحدث معك إن كان صديق أو صديقة يرغب بإنهاء علاقته معك؟ لماذا؟
٢. أي منها يظهر بأن مارك يرغب بأن يكون محترما مع كلير ؟
٣. أي منها تبدو أنها تقلل من احترام كلير ؟
٤. أي منها تظهر مارك بصورة الجبان؟

التمرين (٦-٥):
المحتالون على التراسل الفوري

قم بتقديم الحوار التالي لطلابك:

قصة شارلوت Charlotte

صديقة شارلوت Charlotte الحميمة هي مونيكا Monica، وهما تعرفان بعضهما البعض منذ سنوات. وفي إحدى الأمسيات، عندما كانت الفتاتان على التراسل الفوري، كتبت مونيكا فجأة عبارة " brb" "سأعود على الفور" . وتتفقد شارلوت بريدها الإلكتروني

لترى بعد دقيقة أن مونيكا قد عادت إلى التراسل الفوري. وتبدأ مونيكا بسؤال شارلوت إذا كانت قد عانقت أحدًا بحرارة. وجدت شارلوت الأمر غريبًا نوعًا مًا. تعرف مونيكا من الذي تعانقه شارلوت ، لذا أجابت شارلوت قائلة: أنت تعرفين. لكن واصلت مونيكا الضغط على شارلوت وتقول لها أنها لا تعرف. وتبدأ مونيكا بطرح أسئلة شخصية أخرى جعلت شارلوت تشعر بعدم الإرتياح. بدأت شارلوت تشعر بأن أمرًا ما ليس مألوفًا في محادثتهما.

قم بسؤال الطلاب ما يلي:

١. ما الذي يجب على شارلوت إن لم تشعر بالراحة تجاه المحادثة؟
٢. ما بعض التفسيرات المحتملة لسلوك مونيكا الفظ؟

إن هذا الحوار روتيني، وأي طالب يستخدم التراسل الفوري بانتظام تعرض له. إن التغير المفاجئ في المحادثة عندما عادت مونيكا إلى الحاسوب طبيعي لأنه في الواقع ليست مونيكا مَنْ تتحدث مع شارلوت الآن. إنه أحد إخوتها أو صديق كان ينظر من فوق كتف مونيكا وأكمل المحادثة بعد أن غادرت مونيكا. إن أفضل استجابة تعطيها شارلوت هي: "سأتصل بك هاتفيا،" ومن ثم مكالمتها هاتفيًا. قم بالتأكيد على الطلاب أنه يجب عليهم الثقة بغرائزهم إذا بدأ الشخص على التراسل الفوري بالتحدث بغرابة.

٣. ما الذي يمكن تفعله شارلوت ومونيكا للتأكد بألا يحدث هذا الأمر لهما مرة أخرى؟

سوف يحبذ الطلاب قول أنه يمكنهما عمل كلمة مرور تكون خاصة تماما. تقول أحدهما كلمة والأخرى تجيبها بالإجابة المناسبة.

٤. هل تعرف أحد ما حدث معه الأمر نفسه؟

قم بدعوة الطلبة لمشاركة هذه التجارب، ومن ثم استغل الفرصة لتعزيز الطريقة الملائمة للتعامل مع الوضع. إن النقطة الرئيسة هي التأكيد على أن الطلاب يجب أن يمتنعوا عن التراسل الفوري إذا شعروا بعدم الراحة ومهاتفة الشخص الآخر.

٥. بما أن شارلوت تشعر بعدم الراحة وتشتبه بالأمر، ما الأمر الذي إن عملته سيعتبر خطأ؟

يجب أن يميز الطلاب بأنه سيكون من الخطر البقاء في محادثة التراسل الفوري، سوف سكون من الخطا البدء بطرح أسئلة لمعرفة من الشخص الى آخر في المحادثة. إن البقاء في المحادثة يمنح المضايق فرصًا أكثر للتحرش بهم، ويوفر فرصة متزايدة للضحية للكشف عن معلومات شخصية او انهم يشعرون بالضيق أو الغضب أو الأذى. إن هدف المضايق هو تكبيد الضحية ألمًا عاطفيًا أو إحراجها. قم بالإصرار على الطلاب ألا يمنحوا المضايق ذلك الرضا.

التمرين (٦-٦):
المحتالون في كل مكان

اطلب من الطلاب النظر على البيان التالي ومن ثم تعبئة الفراغات الموجودة برقم.

حوالي..... % من المراهقين مارسوا خدعة على الشبكة الإلكترونية بالتظاهر بأنه شخص آخر على التراسل الفوري.

لقد طرحنا هذا السؤال على آلاف الطلاب في الصفوف من الرابع إلى الثاني عشر. أفاد معظم الطلاب بأن النسبة المئوية ستكون عالية جدًّا. في الواقع، لم يكن لدينا مطلقًا مجموعة من الطلاب تستجيب بنسبة مئوية اقل من ٥٠%. اطلب من الطلاب مشاركة إجاباتهم معك ومتابعة النقاش حول سبب ارتفاع النسبة المئوية. سوف يجيب الطلاب على الأرجح بأن لعب مثل هذه الخدعة لا يكون له عواقب في الغالب.

التمرين (٦-٧):
التحرش على الشبكة الإلكترونية

قم بتقديم الحوار التالي إلى طلابك:

قصة كارينا Karina

سجلت كارينا الدخول إلى التراسل الفوري مرة أخرى قبل الذهاب إلى النوم. رغبت بمعرفة من ما زال مستيقظا. شاهدت أن دارين موجود على الشبكة الإلكترونية. دارين طالب مضحك من المدرسة، على الرغم من أنها لم تكن تعرفه جيدا، وهو في العادة يضع نكتا في ملف التراسل الفوري الخاص به. كتبت "مفاجأة" لدارين وبسرعة تفقدت ملفه على أمل الحصول على ضحكة. وما وجدته على ملفه أجفلها وأزعجها. وضع دارين بعض التعليقات المزعجة عن الفتيات. شعرت كارينا بالاشمئزاز مما قرأته.

١. إسأل الطلاب كيف يجيب أن تجيب كارينا

يكتب المراهقون في العادة أمورًا في ملفات التراسل الفوري الخاصة بهم للتعبير عن أنفسهم. وفي بعض الأحيان، ما يضعونه هو لإحداث صدمة أو جذب الانتباه أو جذب انتباه سلبي. من المهم تذكير المراهقين أن لغة العديد من المراهقين هي بالفعل عبارة عن تحرش وأذى، ولا يجب أن يسمحوا بها. شجعهم على إجابات كالآتي:

- يجب أن تخبر كارينا دارين بأنها وجدت ملف التراسل الفوري الخاص به عدواني ومؤذي.
- يجب أن تسجل كارينا الخروج من التراسل الفوري وتحجب دارين من لائمة التراسل الفوري الخاصة بها.
- يجب أن تخبر كارينا شخصا بالغا بالأمر. سوف يكون ملف دارين مؤذيًا للآخرين أيضًا، والشخص البالغ هو أفضل شخص ليقول له إن لغته غير ملائمة ومؤذية. بكلمات أخرى، أحد الوالدين أو معلم يستطيع المساعدة على إعداد بعض القيود والحدود على الشبكة الإلكترونية لدارين.

٢. قم بسؤال الطلاب ما هي الطريقة الخطأ لتستجيب بها كارينا ؟ ما الذي يجب ألا تفعله؟

قم بتشجيع إجابات الطلاب كالتالية:

- لا يجب أن تخوض كارينا جدالاً مع دارين حول ما كتبه.
- لا يجب أن تنشر كارينا ما وجدته على زملائها وأصدقائها.
- والأمر الأهم، لا يجب أن تتجاهل الأمر: يجب أن تخبر شخصًا بالغًا.

٣. قم بسؤال الطلاب إن كانوا قد شاهدوا مسبقًا أمرًا مكتوبًا على التراسل الفوري أو على ملف أحد الزملاء في الصف يسيء إليهم. قم بتوجيه نقاش حول سبب كون هذه الأمور مؤذية وكيف يجب أن يستجيب الطلاب لها. شجع الطلاب ليدركوا أنه لا يتوجب عليهم قبول سلوك مؤذي من الآخرين. شجعهم بأن يمتلكوا الشجاعة لإخبار شخص بالغ حول بعض التعليقات المسيئة.

٤. اسأل الطلاب عن تعريفهم للتحرش. دع الطلاب يبحثون عن الكلمة التحرش على الشبكة الإلكترونية أو في قاموس. بناء على المعلومات المقدمة،، هل كان سلوك دارين تحرشًا؟ لماذا أو لماذا لا؟

٥. اسأل الطلاب إذا كانوا يستطيعون دائما القول على الفور إذا كان أحد يتصرف بوضاعة أو يتحرش على الشبكة الإلكترونية. هل من الممكن لأحد ما إخفاء نواياه في البداية، أي يبدو لطيفًا في البداية ومن ثم يصبح وضيعًا؟

٦. اسأل الطلاب عن كيفية التعامل مع الأمر إن أحدًا يعرفونه أو التقوا به على الشبكة الإلكترونية بدا لطيفًا ثم بدأ بالتحدث بأشياء لم تعجبهم. ماذا يجب عليهم عمله؟

قم بتشجيع إجابات مشابهة للسؤال رقم (١). قد يقول البعض: "سوف أكون وضيعًا تمامًا مثل الشخص الآخر." قم بالإشارة إلى أنه عندما يكون شخص ما وضيعًا، فإنه يقوم بذلك لرغبتهم بإيذاء أو إغضاب أو إخافة الشخص الآخر. إذا كان الطالب يستجيب بطريقة تظهر أنه متضرر أو غاضب أو خائف، فيكون قد تعرض للتلاعب من قبل المتسلط والمتحرش اللذان يكونان قد حصلا بالفعل على ما يرغبان فيه. من الأفضل تسجيل الخروج وعدم منح المتحرش أي نوع من الرضا.

التمرين (٦-٨):
المحادثات ليست أمرًا خاصًا جدًّا بعد كل شيء

إسأل الطلاب: كم عدد الطرق المختلفة التي يمكن أن تكون فيها محادثة على التراسل الفوري على الشبكة الإلكترونية تعتقد بأنها خاصة ويمكن عملها عامة؟

لا يوجد شيء خاص على الشبكة الإلكترونية. يجب تعزيز هذه النقطة مرات ومرات لدى الطلاب. يمكن جعل محادثة على التراسل الفوري عامة بعدد من الطرق الواضحة ولكنها ليست طرق واضحة جدًّا والتي سمعنا عنها كلها من العديد من الطلاب وأولياء الأمور والمعلمين:

- يمكن نسخ المحادثات على التراسل الفوري ولصقها في أي مكان مثل المواقع الإلكترونية أو الرسائل الإلكترونية.
- يمكن طباعة المحادثات على التراسل الفوري وتوزيعها على أي شخص أو تركها في أي مكان. أو رميها ومن ثم يتم إخراجها بسهولة من القمامة.
- يمكن التقاط المحادثات على التراسل الفوري أو تسجيلها من خلال برنامج تسجيل المفاتيح المثبت على الحاسوب.
- يمكن التقاط المحادثات على التراسل الفوري أو تسجيلها من خلال إداريي الشبكة ممن يراقبون المداخل المستخدمة بوساطة برنامج التراسل الفوري للاتصال عبر الإنترنت.
- يمكن حفظ المحادثات على التراسل الفوري واستعادتها من قبل إداريي خدمات البرنامج بأنفسهم.
- يمكن التقاط المحادثات على التراسل الفوري أو تسجيلها من خلال أحد برامج التجسس الخبيثة المثبتة على الحواسيب.
- يمكن مشاهدة المحادثات على التراسل الفوري من قبل أي شخص ينظر من وراء أحد المشاركين في المحادثة.
- يمكن التقاط المحادثات على التراسل الفوري من قبل برنامج المراقبة الأبوية على حواسيب المنزل.
- يمكن أن تلتقط صور الشاشة أجزاء من محادثات التراسل الفوري لدى حدوثها.

التمرين (٦-٩):
احتفظ به لنفسك

لا يوجد أي شيء خاص على الشبكة الإلكترونية. يمكن التقاط أي شيء ونسخه وأرشفته وطباعته وتمريره وحفظه وتخبئته والتلاعب به. وبسبب كون أي شيء غير خاص بشكل حقيقي على الشبكة الإلكترونية، إسأل الطلاب أي نوع من المعلومات يكون من الحكمة وضعها على ملفاتهم على الشبكة الإلكترونية.

تتضمن الإجابات كذلك الأسماء كاملة وتواريخ الميلاد والعناوين وأرقام هاتف المنزل والهاتف النقال والمعلومات حول المدارس وفرق المدرسة. إن هذا النوع من المعلومات تكشف العديد من المعلومات الشخصية التي يستطيع الآخرون استخدامها ضدهم. بالنسبة للطلاب الأكبر سنًّا والذين يجدون هذا الأمر أمرًا مزيفًا، اخبرهم انه في السنوات الأخيرة الماضية، كانت هنالك زيادة هائلة في سرقة الهوية على الشبكة الإلكترونية وانتحال الشخصية (تمت مناقشته بتفصيل أكثر في الفصل الثالث). كما أن المحتالين يستخدمون المعلومات الشخصية عن المراهقين بشكل متزايد في محاولة لخرق الحسابات المصرفية الخاصة بأولياء أمورهم وحسابات بطاقة الإئتمان. إن هذا ممكنا لأن العديد من أولياء الأمور يستخدمون أسماء أطفالهم وتواريخ الميلاد ككلمات المرور الخاصة بهم.

ما الأشياء التي يستطيع الطلاب وضعها بأمان في ملف على الشبكة الإلكترونية؟

تتضمن الإجابات أمورا مثل عدم الإفصاح عن تفاصيل شخصية مثل الإقتباسات المضحكة والقصائد والتعابير المفضلة.

التمرين (٦-١٠):
نصيحة في التراسل الفوري

إسأل الطلاب عن النصيحة التي يحبون تقديمها لأخيهم الصغير أو أختهم الصغيرة اللذين هما على وشك البدء باستخدام التراسل الفوري.

تأكد أنه بالإضافة إلى تعزيز النقاط الرئيسة من التمارين السابقة، يجب أن تتضمن الإجابات معرفة كيفية حجب أحدهم بوساطة أدوات التراسل الفوري ومعرفة كافة الأشخاص على لائحة الأصدقاء عن كثب. يقوم الأطفال والمراهقون في العادة بإضافة "صديق لصديق" إلى لائحتهم ووضع أنفسهم على المحك وعرضة لسلوك استغلالي ومؤذي من قبل الأشخاص الذين لا يعرفونهم بالفعل.

المصادر

الموقع الإلكتروني لـ Chiff.com: www.chiff.com/computer/internet/im.htm
يوفر هذا الموقع إرشادات لاستخدام وحل مشاكل برامج التراسل الفوري

Evers, J. (2005, December 7). *New IM worm chats with intended victims*.
متوفر في الموقع الإلكتروني لـ ZDNet: http://news.znet.com/2100-1009_22-145927

Gonsalves, A. (2005, July 20). *iTunes-disguised worm spreads via instant messaging.*
متوفر في الموقع الإلكتروني لـ ChannelWeb: www.crn.com/security/166401367

Instant messaging safety. (n.d.)
متوفر في الموقع الإلكتروني لـ
Wired Kids: www.wiredkids.org/kids/personal_information_safety/im_safety/

Instant messaging safety for teens/Children (AOL). (n.d.)
متوفر في الموقع الإلكتروني لـ Wired Kids: www.wiredteens.org/teensim.html

Krebs, B. (2007, September 11). *Skype users: Beware of instant message worm.*
متوفر في الموقع الإلكتروني لـ Washingtonpost.com:
http://blog.washingtonpost.com/securityfix/2007/09/skype_users_beware_of_instant_1.html

Online Safety/security FAQ. (n.d.)
متوفر في الموقع الإلكتروني لـ AIM.com:
www.aim.com/help_faq_/security/faq/adp

Sending and receiving instant messages. (n.d.).
متوفر في الموقع الإلكتروني لـ:
LOOKBOTHWAYS: http://look-both-ways.com/satyingsafe/IM.htm

10 Tips for safer instant messaging. (2008, January 31).
متوفر في الموقع الإلكتروني لـ Microsoft:
www.microsoft.com/protect/yourself/email/imsafety/mspx

الفصل السابع

التواصل الاجتماعي
Social Networking

على الشبكة الإلكترونية , لا توجد أية حدود.

التواصل الاجتماعي في كل مكان

إن انطلاقة الشبكات الاجتماعية على الشبكة الإلكترونية أحدثت ثورة في أنماط التواصل بين الشباب. يستخدم الأطفال والمراهقون مواقع التواصل الاجتماعي مثل: MySpace، Facebook، Xanga، Live Journal، Flickr، والعديد من مواقع الاستضافة لبناء التواصل وتطوير العلاقات على الشبكة الإلكترونية. لدى بعض المواقع مثل Classmates.com أو Graduates.com تركيز محدد على المدارس والطلاب. تجذب المواقع الاخرى المستخدمين من خلال اهتمامات محددة مثل الألعاب أو مشاركة الصور أو الرياضة أو الأفلام أو الهوايات أو الموسيقى. إن الإنتماء إلى مواقع مثل MySpace أو Facebook يمكن أن يشبه إلى حد كبير التسكع في المجمعات التجارية.

إن هجرة المراهقين والمراهقات الصغار إلى مواقع التواصل الاجتماعي أسهم في ثورة تسويقية ومكاسب مادية غير متوقعة لكل من المواقع والمعلنين فيها. في عام ٢٠٠٥م، اشترت شركة روبرت ماردوخ Rupert Murdoch المدعوة News Corporation موقع MySpace بما يعادل ٥٨٠ مليون دولار على الرغم من أن العمر التجاري لموقع MySpace لم يبلغ الثلاث سنوات! وأظهر تعداد في خريف عام ٢٠٠٧م أن (٩٦) من الشبكات الاجتماعية المتوافرة للعامة مختلفة الأحجام يتراوح عدد مستخدميها من عدة آلاف إلى (٢٠٠) مليون مستخدم. إن معظم هذه المواقع مخصصة للبالغين والمراهقين الأكبر عمرًا، ومع ذلك ينضم أطفال صغار يبلغ عمرهم (٩) سنوات تقريبًا إلى هذه المواقع. ولسوء الحظ، مع منح هؤلاء الأطفال والمراهقين فرصًا للانضمام إلى التواصل الاجتماعي، فإنهم مستهدفون من قبل عمليات نصب وتحرش تغريهم لإنفاق المال وتعريض أنفسهم للبرامج الضارة وما هو أسوأ من ذلك.

يظهر بحث تم إجراؤه مؤخرًا أن الشبكات الإجتماعية مثل Facebook و MySpace لا تساعد المستخدمين على بناء علاقات جديدة ووثيقة. كما أوضح البحث أن الاتصال وجهًا لوجه ما زال أمرًا ضروريًا لبناء علاقات شخصية وثيقة. (ScienceDaily, 2007)

وكبالغين، نبتكر حدودًا وبيئات تركيبية لأطفالنا للسماح لهم بالنمو بشكل صحي وآمن. ومن طبيعة الأطفال والمراهقين دفع القيود السابقة واختيار التركيبات التي يوجدها البالغين لهم. وعلى الشبكة الإلكترونية، لا توجد أية حدود. إن الحياة على الشبكات الاجتماعية بالنسبة للعديدين تشبه حياة رعاة البقر في الغرب الأمريكي. يميل الأطفال والمراهقون إلى الإحساس

بأن عالم التواصل الاجتماعي ملك لهم وأن البالغين غير مرحب بهم. ونجد بشكل روتيني الأطفال والمراهقين يختبرون الحدود بطرق تكون مؤذية أو تشوه السمعة أو مهينة أو غير ملائمة للعمر أو غير ملائمة من الناحية الجنسية.

تختلف المسائل المرتبطة بالشبكات الإجتماعية بالنسبة للأطفال والمراهقين الصغار، لذا سنقوم بتناولها بشكل منفصل.

التواصل الاجتماعي للمراهقين

بينما تطلب الشبكات الاجتماعية المألوفة مثل MySpace وFacebook من المستخدمين أن يكون عمرهم ١٤ عامًا على الأقل، فإننا نوصي بأن عمر ١٦ عامًا عمرًا أفضل للبدء في استخدام هذه المواقع. إن المراهقين الأصغر سنًّا ليسوا مستعدين من الناحية التنموية للتعامل مع العديد من المسائل التي تنشأ مع التواصل الاجتماعي. يضع بعض المستخدمين صورًا استفزازية أو يستخدمون لغة غير لائقة. على سبيل المثال، لم تستطع فتاة تبلغ من العمر ١٥ عامًا قمنا بالتحدث معها فهم المخاطر التي تقوم بها عندما تضع على صفحتها صورة استفزازية لنفسها بلباس السباحة، أو لماذا قد يتم اعتبار اختيارها كتقليل لقدر نفسها. إن وضع مثل هذا النوع من الصور يكون شائعًا أكثر مما يدركه معظم البالغين. استجابتها لاهتمامنا كانت "ماذا؟ مثلي، هنالك الملايين من مستخدمي MySpace". ما فرص أن يجدني أحد ما؟". إن المواقف مثل هذا الموقف تضع الشباب الصغار في خطر أكبر في جميع تفاعلاتهم على الشبكة الإلكترونية.

التمرين ٧–١ – أساسيات التواصل الاجتماعي يطلب من الطلاب تقييم نشاطاتهم واستخداماتهم لمواقع التواصل الاجتماعي، ويحددون العوامل الإيجابية والسلبية للموقع. كما أنه يوفر قائمة بقضايا التواصل الاجتماعي لأخذها بعين الاعتبار مثل نقص الثقة والخصوصية، والحيل التسويقية الخادعة، والتعرض للتحرش ونقص السيطرة على ما يضعه الآخرون. التمرين ٧–٢ – تقييم صفحات التواصل الاجتماعي يقدم للطلاب بعض الخطوات لتقييم مواقع التواصل الإجتماعي لمشاهدة إن كانت ملائمة لمشاركة الطالب.

الخداع والاحتيال على الشبكات الإجتماعية

جذبت مواقع الشبكات الاجتماعية مثل Facebook و MySpace عشرات الآلاف من المراهقين، وهي مبنية على الثقة والتنشئة الاجتماعية، فقد أصبحت أهدافًا رئيسة لكافة أنواع الأشخاص عديمي الضمير. يحتاج كل مستخدم للشبكة الاجتماعية سواء أكان ذكرا أم أنثى إلى رفع مستوى وعيه للعديد من الأنواع المتنوعة للإحتيال التي تستهدفهم. التمرين ٧–٣ – الاحتيال على الشبكات الاجتماعية يكشف بعض من الأسباب المعروفة جدًّا للاحتيال الذي يستهدف مستخدمي الشبكة الاجتماعية. يجب أن يساعد هذا التمرين على زيادة مستوى وعي الطالب وتشجيع الممارسات الأمنة أثناء التواجد على مواقع التواصل الاجتماعي.

هل هي فعلا خاصة؟

يبحث العديد من الأشخاص عن مواقع التواصل الاجتماعي. يتم البحث عن مواقع الشبكات الاجتماعية من قبل الشرطة، وموظفي القبول في الكلية، ومديري القبول في المدارس الثانوية الخاصة والموظفين ومديري البرامج المرحلية، ولجان البعثات، ومديري المخيم الصيفي، والجيش، والمؤسسات الرياضية، والبالغين الآخرين الذين يريدون تقييم أحد الأفراد. لسوء الحظ، كانت هنالك بعض العواقب الحقيقية والسلبية على الطلاب الذين وضعوا صورًا أو أي محتوى آخر يكشف عن النشاطات غير القانونية أو الإحراج أو سلوك غير ملائم. بعض الأمثلة التي تم الإبلاغ عنها:

اتحد مجلس الإعلانات The Ad Council والمركز القومي للأطفال المفقودين والمستغلين National Center for Missing & Exploted Children لإنتاج شريطين مصورين ممتازين يلفتان الإنتباه إلى إنعدام الخصوصية على الشبكة الإلكترونية والعواقب المحتملة. الرجاء زيارة Cybertipline.com :

فكر قبل أن تضع شيئا (http://tcs.cybertipline.com/psa/BulletinBoard_60.mov)

الجميع يعرف اسمك (http://tcs.cubertipline.com/psa/Everyone_60.mov)

- جامعة ديوك Duke University رفضت قبول أحد الطلبة استنادًا على المحتوى الذي تم العثور عليه في صفحته في المدرسة الثانوية على MySpace. (التواصل الشخصي).
- طالب في المدرسة الثانوية في أبوتسفورد Abbotsford High School في كندا تم فصله بسبب تهديده بضرب مدرس. ظهر ذلك عندما وضعه على صفحته على الفيسبوك، وادعى أنها كانت مجرد دعابة. (Luymes, 2007)
- كلية فيشر Fisher College في بوسطن فصلت طالبين لإعدادهما خططًا لاستهداف موظف في الكلية والتحرش به (Schwetzer, 2005).
- جامعة أكفسورد Oxford University، في إنجلترا، قامت بمحاكمة طالب على قيامه بسلوك مخل بالنظام بناء على دليل وجدته على حساب الطالب على الفيسبوك (Gosdon).
- جامعة ولاية فالدوستا Valdosta State University في جورجيا فصلت طالب لوضع محتوى على حسابه على الفيسبوك تم تفسيره كتهديد (Guess, 2008).
- جامعة ولاية لويزيانا Louisiana State University فصلت طالبين من فريق السباحة بعد وضعهما ملاحظات مهينة حول أحد مدربيهم (Camire, 2007).
- جامعة ساوثورن إلينوا Southern Illinois University، في إدواردز فيل Edwardsville، فرضت أحكامًا عقابية على طالب بسبب إنشائه صفحة على الفيسبوك مخصصة لإدعاءات زائفة بعلاقة حميمية مع طالبة (Savo, 2007).

- كلية أيوا ويسترن كوميونيتي Iowa Western Community College فصلت طالبًا قال على صفحته على MySpace بأنه يجب إطلاق النار على طلبة آخرين (Fichman, 2007).

الصفحات الخاصة ليست خاصة

على مدى سنوات، ابتكر المحتالون طرقًا متعددة لاختراق الصفحات الخاصة. لقد التقط المنتحلون الهويات وكلمات المرور بطريقة محترفة باستخدام الهواتف التي تحتوي على البريد الإلكتروني، قام المستخدمون الذين لا يشتبهون بالفعل بمنح معلومات تسجيل الدخول الخاصة بهم للمحتالين والنصابين من خلال برنامج يعتبر طرفًا ثالثًا قاموا بتجهيزه للتثبيت.

يعتبر العديد من المراهقين قيام البالغين بمشاهدة مواقع التواصل الاجتماعي الخاصة بهم انتهاكًا. في أغلب الأحيان، سيقومون بذكر حقوق الخصوصية في جدالات مع الآباء. في الحقيقة، كل شيء عام على الشبكة الإلكترونية، وما أن تتم زيارة موقع، يمكن نسخ كل شيء واستخدامه من قبل الزائر. في كل سنة، توجد أخبار عن تقارير حول شخص تعرض للإهانة علنًا عندما تم الإفصاح عن محتوى "خاص" في صفحات التواصل الاجتماعي الخاص بهم للعامة!

تقترح بيانات المسح والأبحاث غير الرسمية أن حوالي ٩٠% من الغرباء الذين ينقرون على الأبواب الخاصة لحسابات شبكة التواصل الاجتماعي يتمكنون من الدخول! هل يسمح طلابك للغرباء بالدخول إلى حساباتهم؟ اطلب منهم: هل من الممكن أن الأشخاص الذين تسمح لهم أنت والآخرين بالدخول إلى الشبكة الإجتماعية الخاصة بكم ليسوا كما يدعون؟

قام موظفو القبول والتسجيل في الكلية وأقسام الموارد البشرية باليحث بشكل محدد في الشبكات الاجتماعية عن معلومات تتعلق بمقدمي الطلبات للكلية والمرشحين للوظائف. لقد أنكر بعض الطلاب تسجيل الدخول في الكلية أو التقدم بطلب وظائف بسبب المحتوى الذي وضعوه على صفحاتهم الخاصة.

قم بإجراء مسح بدون ذكر الاسم. قم بتسليم ورقة صغيرة إلى طلابك ابتداء من الصف الثامن وما فوق. اخبرهم بأن هذا المسح لا يتم فيه ذكر الاسم بشكل كامل واطلب من متطوعين إحصاء النتائج. قم بسؤال طلابك السؤالين التاليين:

- هل سبق أن كان لديك أي حساب على شبكة للتواصل الإجتماعي؟
- هل قمت بمصادقة غريب أو سمحت لشخص غريب بمشاهدة صفحاتك الخاصة؟ قم بتذكيرهم بأن "صديق صديقك" هو أيضا شخص غريب!

اطلب من الطلاب جمع ومقارنة الإجابات. قد تشعر بالدهشة من عدد الطلاب الذي يقومون بانتظام بمصادقة شخص غريب تماما على الشبكة الإلكترونية.

وبقليل من الجهد، يستطيع الطلاب العثور على المزيد من المقالات التي توضح تفاصيل العواقب الوخيمة على كل من طلاب المدارس المتوسطة والثانوية بسبب وضع ما اعتقدوا أنه معلومات خاصة على الشبكات الإجتماعية. التمرين ٧–٤ – عليك أخذ العواقب بعين الاعتبار يطلب من الطلاب القيام ببحث في العواقب التي يواجهها الطلاب بسبب ما وضعوه على حساباتهم على الشبكة الاجتماعية. يمكنك أيضًا جعل الطلاب ينوعون في حلقة البحث بوساطة استبدال كلمة "فصل" بكلمات مثل اعتقال، ومحكوم، وعقوبة. إن الهدف الرئيس هو التأكيد على الطلاب بأن لا شيء خاص على الشبكة الإلكترونية، وحتى ليس كلمات المرور المحمية على صفحات الشبكة الاجتماعية.

يمكن العثور على العديد من الحوادث المماثلة في الأخبار في الجزء الخاص بالمصادر في نهاية هذا الفصل. في الوقت الذي تكون فيه معظم الأمثلة عن طلاب الجامعات، فإن هنالك عدة أمثلة عن العواقب التي يعانيها طلاب المدارس في المرحلة المتوسطة والثانوية. قم بقراءة المقالة المدرجة في USA Today والمعنونة، "ما الذي تقوله على الشبكة الإلكترونية يمكن أن يعود عليك بالضرر"، بقلم جانيت كورنبلام Janet Kornblum وماري بيث ماركلين Mary Beth Marklein (www.usatoday.com/tech/news/internetprivacy/2006-03-08).

يمكن أن يستخدم المراهقون مواقع التواصل الإجتماعي بأمان إذا اتبعوا الإرشادات الملائمة. التمرين ٧–٥ – إرشادات السلامة على مواقع التواصل الاجتماعي يساعد الطلاب على تحديد أفضل الطرق والسلوكيات لتقديم أنفسهم بشكل ملائم على مواقع التواصل والتواصل الاجتماعي.

التواصل الاجتماعي للطلبة الصغار

تغري المواقع الموجهة للأطفال مثل كليب بيونغيوين Club Penguin ويبكنز Webkinz الأطفال الصغار من عمر السادسة برسومات تفاعلية ممتعة، وألعاب، والقدرة على التواصل مع الأطفال الآخرين. يغدو الأطفال مفتونين في وقت مبكر متشوقين للتشبيك الاجتماعي والتواصل مع الأصدقاء على الشبكة الإلكترونية. وفي الوقت الذي توفر فيه هذه المواقع المخصصة للأطفال الصغار العديد من خيارات السلامة المتوافرة للآباء، إلا أن الأطفال الذين يزورون هذه المواقع ما زالوا يبلغون عن وجود لغة التحرش وتعرضهم لصور إباحية والتسلط بأنواعه. ومن الأمور المقلقة الأخرى هو أن هذه المواقع الموجهة للأطفال تعتبر بوابة متعددة الوسائط ينفتحون من خلالها على تجربة التواصل الاجتماعي في سن مبكرة جدًّا. يمكن أن يشجع هذا الانفتاح الأطفال في عمر التاسعة أو العاشرة على التهافت على MySpace والفيسبوك Facebook وغيرها من المواقع الموجهة للبالغين.

هل مواقع التواصل الاجتماعي آمنة للأطفال؟

رفع التسويق الذكي المصحوب بتأثير الأقران مستوى مواقع الكترونية مثل كليب بيونغيوين Club Penguin ويبكنز Webkinz إلى شعبية ملحوظة. بالإضافة إلى المواقع الإلكترونية القائمة منذ مدة طويلة مثل Runescape وNeopets، فإن هذه المواقع تجذب العديد من الطلاب في الصف الثامن وأقل. وعلى الرغم من أنهم لا يعترفون بذلك، فلقد بينت أبحاثنا أن عددًا ملحوظًا من طلاب المدارس المتوسطة يزورون مواقع التواصل الاجتماعي الموجهة للأطفال الصغار. لا يوجد دليل واضح على أن الطلاب الكبار يميلون أكثر للتحرش بالطلاب الصغار على هذه المواقع. ومع ذلك، فمن المهم أن يعرف الآباء والطلاب أن كون موقع إلكتروني مصمم ومسوق للأطفال الصغار، فإن ذلك لا يعني أن الأطفال الصغار هم فقط مَنْ يستخدمون الموقع الإلكتروني.

بينما تقدم بعض هذه المواقع مستويات متنوعة لضبط الآباء أو اعتدال البرنامج/ البشر، لقد سمعنا العديد من الأمثلة على الأطفال الذين وجدوا طرقًا للالتفاف على مثل هذه الضوابط والاعتدال. على سبيل المثال، لقد تعلم الأطفال منذ مدة طويلة أن الملاحظات البذيئة يتم ضبطها على الأرجح بوساطة "المراقب"الذي يراقب محادثاتهم. وعلى ذلك، تعلموا أن التعليقات المموهة والمختصرة يمكن أن تتجاوز هذه المرشحات. فإن معنى جُمل مثل "Ur a $tup!d j'rk" والتي كتابتها الصحيحة هي "You are a Stupid Jurk" والتي تعني "أنت وغد غبي" أو جملة "Im guna kyl u" والتي كتابتها الصحيحة "I am going to kill you" والتي تعني "سوف أقتلك"أو "U $ck" والتي كتابتها الصحيحة هي "You are suck"والتي تعني "أنت مقرف" أصبح واضحًا جدًّا، ولكن ليس لدرجة ليتم ملاحظته من قبل مرشح البرنامج.

التمرين ٧–٦– التواصل الاجتماعي بالنسبة للأطفال: القواعد والمخاطر يتمعن في مواقع التواصل الاجتماعي المصممة للأطفال الصغار ويطلب من الطلاب مناقشة المخاطر والقواعد والسلوك الملائم على الشبكة الإلكترونية.

أخبرنا الأطفال والآباء حول الاستغلال والتحرش والتسلط والمخادعة والتعرض للصور الإباحية والمحادثات الجنسية التي تظهر على هذه المواقع. في الحقيقة، قد يجادل البعض أن هذه المواقع مصممة للأطفال الصغار، فإنها قد تجتذب مشتهي الأطفال جنسيًّا. على الرغم من أن هذه المواقع تبذل جهودًا كبيرة وصادقة للمحافظة على سلامة الأطفال، إلا أنه لا توجد أية ضمانات. إن الأطفال الصغار هم المجموعة العمرية الأكثر عرضة للاستغلال لأنهم ساذجين ولا يمتلكون خبرة. إنهم على الأرجح عرضة للاستغلال وتنقصهم المهارات اللازمة للتعامل معه. على هذه المواقع، يستطيع الأطفال التفاعل مع الغرباء في الأماكن العامة، وفي بعض الأحيان في الأماكن الخاصة أيضًا. لقد تعرض الأطفال للخداع وقاموا بالإفصاح عن معلومات شخصية، مثل عناوين البريد الإلكتروني، وأرقام الهواتف، وحتى العناوين الخاصة الأخرى. التمرين ٧–٧ – ماذا يجب أن نفعل عندما... يطلب من الطلاب مشاركة قصصهم حول التجارب السلبية على الشبكة الإلكترونية، وكيفية تحديد أفضل الطرق للإستجابة كمجموعة. التمرين ٧–٨ – توفير السلامة على الإنترنت (إعلان الخدمة العامة) يطلب من الطلاب ابتكار إعلان الخدمة العامة الذي سوف يساعد على جذب الإنتباه إلى مشكلة التواصل الإجتماعي وتقديم كيفية الإستجابة المثلى للتجارب السلبية على الشبكة الإلكترونية.

هجرة المراهقين والبالغين إلى شبكات التواصل الاجتماعي

تظهر آلاف استطلاعات الرأي الخاصة بالطلاب وجود نزعة متنامية عند الأطفال للهجرة من شبكات التواصل الاجتماعية الموجهة للأطفال إلى شبكات التواصل الاجتماعي الحقيقية. يبدو أن هذه الهجرة بدأت بشكل جاد في الصف السابع والثامن، ولكن أخبرنا أطفال بعمر التاسعة أن لديهم حسابات على MySpace. إن هذا أمر مزعج جدًّا لأن شبكات

التواصل الاجتماعي الخاصة بالمراهقين والبالغين هي أماكن غير صحية أو آمنة للأطفال. إن الأطفال الذين يستخدمون شبكات التواصل الإجتماعي مثل MySpace والفيسبوك Facebook و Xanga عرضة لمخاطرة كبيرة كمشاهدة صور غير ملائمة ورسومات بلغة غير ملائمة واستغلال وخدع التسويق الإحتيالية.

نشر مكتب المدعي العام في مدينة إلينوا Illinois بيان صحفي في حزيران ٢٠٠٧م حول موضوع شبكات التواصل الاجتماعي الخاصة بالاطفال. وكان عنوانه المواقع الإلكترونية "نوافذ" تستهدف الاطفال الصغار للتواصل الاجتماعي والمحادثة على الشبكة الإلكترونية مع الغرباء "Gateway" Websites target Younger Children for Social Networking and Chatting Online with Strangers. إن هذا البيان جدير بالقراءة ومتوافر على: www.illinoisattorneygeneral.gov/pressroom/2007_07/20070731.html.

التمارين

التمرين (٧-١):
أساسيات التواصل الاجتماعي

قم بسؤال الطلاب الأسئلة التالية:

١. ما مواقع التواصل الاجتماعي الرئيسة التي تستخدمونها؟
٢. ما المواقع الأخرى التي سمعتم بها؟
٣. ما أكثر إيجابيات أو فوائد هذه المواقع؟
٤. ما القواعد التي تستخدمونها أنتم وعائلاتكم لهذه المواقع؟
٥. ما إعدادات الخصوصية المهمة لحسابكم؟
٦. ما المخاطر التي تأتي من استخدام هذه المواقع؟

عندما يتم السؤال عن مخاطر مواقع التواصل الاجتماعي، أشار المراهقون بشكل عام إلى المطاردة من قبل المستغلين والمخاطر المترتبة على وضع معلومات خاصة مثل الاسم أو مكان إقامتهم.

وفيما يلي أمثلة على مسائل إضافية قد لا يدركونها وهي أيضًا من مخاطر التواصل الاجتماعي:

- لا تعلم بمن تثق.
- لا يوجد شيء خاص على الشبكة الإلكترونية.
- كيف يمكن لتقديمك نفسك في صور ورسوم تعريضك للمخاطر بشكل أكبر.

على سبيل المثال، صورة لفتاة في الثالثة عشر من عمرها في وضع مغري قد يبدو مثيرا ويظهر دلعها، ولكنه يعرضها لخطر التعرض للتحرش الجنسي:

- إن عمليات الاحتيال التسويقية المضللة شائعة على هذه المواقع وتجذب المراهقين إلى صفحات إلكترونية مزيفة مصممة لاستخراج معلومات خاصة. بالإضافة إلى ذلك، توفر المواقع دخولا فوريًا إلى اللعب والقمار والفن الإباحي على الشبكة الإلكترونية.
- توجد هذه المواقع إحساسًا فوريا بالمجتمع، وهي سهلة نسبيًّا بالنسبة للغرباء فيما يتعلق بكسب ثقة المراهقين الساذجين والبريئين.
- قد يعرض المستخدمون أنفسهم للاستغلال والسخرية والتحرش بشكل عام، وخاصة فيما يتعلق بالمحتوى الذي وضعوه.
- من الصعب تمييز النوايا الحقيقية للآخرين على هذه المواقع.

- من المستحيل ضبط ما يضعه الآخرين عنك. قد يكون لصورة محرجة أو تعليق عواقب وخيمة على علاقاتك وعلى كيفية فهم الآخرين لك.

التمرين (٧-٢):
تقييم صفحات التواصل الاجتماعي

باستخدام المعايير التالية، قم باختيار بعض صفحات الفيسبوك Facebook أو MySpace التي قد تكون أمثلة جيدة لتقييم صفحات التواصل الإجتماعي. وضح لطلابك واجعلهم يقيمون الصفحات بناء على هذه المعايير:

١. هل كلمة المرور للصفحة محمية أو متاحة لجميع الزوار؟
٢. كم عدد المعلومات الشخصية المكشوفة على "البوابة الأمامية" للموقع؟
٣. هل تحتوي البوابة الأمامية أية صور لمالك الموقع؟ هل الصورة مغرية بأي شكل من الأشكال؟ هل تجتاز الصورة اختبار الآباء؟ بكلمات أخرى، هل سيوافق أغلبية الآباء على الصورة؟
٤. كم عدد المعلومات الشخصية المكشوفة داخل الموقع (الاسم الأول واسم العائلة، العنوان، المدرسة، المرتبة في الفرق/ الفريق أو رقم الدور/ الفريق، رقم الهاتف/ رقم الهاتف الخلوي، اسم المستخدم على التراسل الفوري..إلخ)؟
٥. هل يحتوي الموقع على صور إضافية لمالك الموقع؟ هل أي من الصور محرجة أو مغرية بأي طرق من الطرق؟ قم بتطبيق اختبار الآباء مرة أخرى.
٦. هل قام أي من الزوار بوضع تفاصيل واضحة عن مالك الموقع أو أي شيء آخر قد يكون محرجًا أو يشوه سمعته؟ هل قام مالك الموقع بوضع أية استطلاعات تشخصية للرأي؟ ما المعلومات التي يمكن العثور عليها في استطلاعات الرأي التي قد تكون شخصية جدًا أو مكشوفة جدًا للعامة؟
٧. هل يوجد أي محتوى على الموقع تعتقد بأن مالك الموقع لا يرغب في أن يراها أي من الاشخاص التاليين: الأم، الجدة، الاب، الجد، موظف التسجيل في الكلية، الشرطة، عميد الطلبة، مدير المدرسة الثانوية، المعلمون، موظف؟

التمرين (٧-٣):
الاحتيال على الشبكات الاجتماعية

تجذب مواقع التواصل الإجتماعي مثل الفيسبوك Facebook و MySpace عشرات الآلاف من المراهقين وهي مواقع قائمة على الثقة والتواصل الاجتماعي، ولذلك فإنهم أصبحوا أهدافًا رئيسة للأشخاص عديمي الضمير من كافة الأنواع. يحتاج كل مستخدم لموقع التواصل الإجتماعي لرفع وعيه حول العديد من الأنماط المختلفة للإحتيال التي

تستهدفهم. قم بالطلب من الطلاب قراءة العديد من المقالات من القائمة أدناه.اطلب من الطلاب كتابة ملخص من فقرة واحدة لمقالة ليقدموها إلى الصف.

١. False "Friends" Prey on Social Networking Sites
(Bob Keefe; Cox News Service; February 25, 2007)
www.coxwashington.com/hp/content/reporters/stories/2007/02/25/BC_SOCIAL_SPAM_ADV25_COX.html

٢. MySpace Phishing Scam Targets Music Fans
(John Leyden; The Register; October 14, 2006)
www.theregister.co.uk/2006/10/14/myspace_phishing_scam/

٣. Facebook "Ideal" for Phishing Attacks: Researcher
(CBC News; April 14, 2007)
www.cbc.ca/technology/story/2007/04/13/tech-facebookphishing-20070413.html

٤. Attack of the Facebook Snatchers
(Nick Sullivan; Symantee; April13, 2007)
https://forums.symantee.com/syment/blog/article?message.uid=306060

٥. MySpace Codes Bring Adware Payload
(Pete Cashmore; Mashable; July 10, 2006)
https://mashable.com/2006/07/10/myspace-codes-bring-adware-paload/

٦. Fake YouTube Scam Hits 1.400 MySpace Pages
(Pete Cashmore; Mashable; Novemeber 8, 2006)
http://mashable.com/2006/11/08/fake-youtube-scam-hits-1400-myspace-pages/

٧. FakeYourSpace: How Losers Become Popular
(Darnell Clayton; Blog Herald; November 30, 2006)
www.blogherald.com/2006/11/30/fakeyourspace-how-losers-become-popular

٨. Stalker Tracker Scam Targets MySpace
(Mary Landsman; About.com; March 26, 2007)
http://antivirus.about.com/b/a/257837.htm

٩. MySpace Accounts Compromised by Phishers
(Netcraft; October 27, 2006)
http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html

١٠. Phish-Hooked Thieves Find Easy Pickings on Social Sites
(Kim Hart; Washington Post; July, 2006)
www.washingtonpost.com/wp-dyn/content/article/2006/07/15/AR2006071500119.HTML

واجب القراءة المتقدمة

المقالة التالية ملائمة كواجب للمراهقين الأكبر سنًّا أو لصف لغة إنجليزية متقدم أو صف علم نفس. يمكن استخدام المحتوي لنقاش واسع النطاق حول "الصداقة" أو المسائل المتعلقة بالخصوصية.

A Friending Need
(Mark Vernon; The Guardian; October 5, 2006)
http://commentisfree.guardian.co.uk/mark_vernon/2006/10/friending_is_frightening.html

التمرين (٧-٤):
خذ العواقب بعين الاعتبار

ما الذي يمكن أن يتعلمه طلابك حول بعض العواقب الوخيمة التي يواجهها طلاب المدارس المتوسطة والثانوية بسبب ما وضعوه على حساباتهم على شبكات التواصل الاجتماعي؟ اطلب من طلابك إجراء بعض الأبحاث بالطريقة التالية:

١. قم بزيارة محرك بحث وأدخل بعض مجموعات الكلمات في حقل البحث. استخدم مجموعة الكلمات مثل "المدرسة الثانوية"، طرد، فيسبوك Facebook؛ أو "المدرسة الثانوية"، طرد، MySpace. (فائدة: حافظ على الاقتباسات حول "المدرسة الثانوية". تطلب الاقتباسات من محركات البحث بالعثور تمامًا على تلك المجموعات من الكلمات بنفس الترتيب بالضبط).

٢. حاول باستخدام نفس مجموعات الكلمات ولكن قم باستخدام "المدرسة المتوسطة" بدلا من "المدرسة الثانوية".

٣. قم باختيار مقالة واحدة أو اثنتين لقرائتها وكتابة تقرير عنها.

التمرين (٧-٥):
إرشادات السلامة على مواقع التواصل الاجتماعي

قم بتقديم ما يلي كواجب بعد تقسيم طلابك إلى مجموعات صغيرة:

لنفترض أنك كنت جزءًا من فريق قام بإنشاء شبكة تواصل اجتماعي جديدة وشائعة بشكل متزايد. تم منح فريقك مهمة ابتكار صفحة على الشبكة الإلكترونية للمستخدمين توصي بكيفية قيامهم بتوجيه أنفسهم بطريقة آمنة وملائمة. قم بكتابة إرشادات للتواصل الاجتماعي باستخدام عادات وممارسات آمنة.

التمرين (٧-٦):
التواصل الاجتماعي بالنسبة للأطفال:
القواعد والمخاطر

المواقع ClubPenguin، و Webkinz، و Runescape، و Neopets وغيرها من المواقع الإلكترونية المشابهة شائعة جدًّا. هل يستخدم أي من الطلاب في صفك هذه المواقع أو يعرف أحدًا يستخدمها؟ قم بإجراء استطلاع للرأي.

ما القواعد التي يضعها آباء طلابك لاستخدام هذه المواقع؟ قم بإنشاء قائمة بالقواعد. اطلب من الطلبة النظر على كل واحدة من هذه القواعد ووضع تقدير لها حسب الأهمية. قم بالنظر على أهم ثلاثة قواعد. لماذا يعتقد طلابك أنها مهمة جدا؟

والآن، قم بسؤال طلابك ما يلي: ما المخاطر التي تأتي من استخدام هذه المواقع؟

عند مناقشة المخاطر الموجودة على مواقع التواصل الاجتماعي، يقوم الأطفال بشكل عام بقبول التعرف على الغرباء، ويكشفون الكثير من المعلومات الشخصية، والتحرش أو التسلط. وتتضمن المخاطر الأخرى الأقل وضوحا والتي يجب مناقشتها ما يلي:

- التعرض للخداع للإفصاح عن كلمات المرور الخاصة بهم أو معلومات الحساب.
- الانقياد بعيدًا عن الموقع إلى مناطق أخرى على الشبكة الإلكترونية والتي قد لا تكون ملائمة أو آمنة.
- التعرض لصور أو نصوص مزعجة أو غير مريحة لهم.

التمرين (٧-٧):
ماذا يجب أن نفعل عندما...

يتحدث الأطفال في بعض الأحيان على Club Penguin و Webkinz، و Runescape، و Neopets وغيرها من المواقع الإلكترونية المشابهة أشياء وضيعة أو مؤذية للآخرين. يحاول المستخدمون في بعض الأحيان خداع الأطفال للإفصاح عن كلمات المرور الخاصة بهم أو معلومات تعريفية أخرى. قم بسؤال طلابك إذا سمعوا من قبل بأمور مؤذية تحصل مع آخرين على هذه المواقع الإلكترونية. شجعهم على مشاركة تجاربهم الخاصة في هذه الأحداث. قم بإعداد قائمة بالتجارب السلبية بناء على نوع التجربة. تتضمن الفئات على الأرجح ما يلي:

- لغة بذيئة.
- التحدث بأشياء وضيعة.
- التسلط.
- التعرض للسخرية.
- السرقة.
- الخداع.

أطلب من الطلاب التمعن في اللائحة التي ابتكروها. ثم قم بتقسيم الطلاب إلى مجموعات صغيرة وقم بتعيين تجربة واحدة أو أكثر لكل مجموعة. أخبر كل مجموعة بأن وظيفتهم التوصل إلى أفضل طريقة للإجابة عن التجربة المؤذية إذا حدثت لهم. سيكون هنالك في الأغلب مجموعة متنوعة وواسعة من الإجابات. وعلى ذلك، قم بتشجيع الأطفال على التركيز على ما يلي:

- عدم الاستجابة للشخص المتسلط أو الوضيع.
- قم بتسجيل الخروج إذا شعرت بعدم الراحة.
- قم بالإبلاغ عن المستخدم إلى الموقع الإلكتروني (يوجد في معظم الشبكات الاجتماعية وسائل للإبلاغ عن الإستغلال).
- قم بإخبار والديك! (قم بتذكير الطلاب بأهمية التحدث مع آبائهم حول الأمور التي تحدث معهم على الشبكة الإلكترونية).
- لا تقم ابدًا بالإفصاح عن المعلومات الشخصية وعدم مشاركة كلمات المرور الخاصة بحساباتهم مع أي أحد بما فيهم الأصدقاء.

التمرين (٧-٨):
إنشاء السلامة على الإنترنت
(إعلان الخدمة العامة)

إعلان السلامة العامة هو إعلان غير تجاري يستخدم في العادة لتثقيف العامة حول مسائل مهمة أو الإهتمامات الخاصة بالسلامة. قم بتقسيم طلابك إلى أزواج أو مجموعات صغيرة واطلب منهم ابتكار إعلان الخدمة العامة للسلامة على الإنترنت لموقع Club Penguin (www.clubpenguin.com) أو Webkinz (www.webkinz.com).

انظر إلى قائمة التجارب السلبية على الشبكة الإلكترونية التي أنشأئها الطلاب في التمرين ٧-٧، واختار إحدى مشاكل السلامة على الشبكة الإلكترونية التي تهم الطلاب الذين يستخدمون مثل هذه المواقع الإلكترونية مثل Club Penguin و Webkinz. اطلب من طلابك كتابة نص قصير يوضح المشكلة لدى حدوثها.

قم بتحذيرهم لتجنب استخدام اللغة غير الملائمة. يجب أن يتضمن النص راوي تكون مهمته لفت النظر إلى المشكلة والتحدث عن حل آمن وملائم. سيكون إشراف المعلم ضروريًا بينما يقوم الطلاب بإعداد النص. إن الهدف هنا هو جعل الطلاب يستوعبون إجابة آمنة وملائمة للأحداث السيئة التي قد تحدث معهم على الشبكة الإلكترونية.

المصادر

Ascione, L. (2006, June 12). *"Safe" social networking sites emerge: companies launch more secure, educational alternatives to MySpace and Friedster.*

متوفر في الموقع الإلكتروني لـ eSchool News:
www.eschoolnews.com/news/showstoryts.cfm?Articleid=6348

Camire, K. (2006, August 27*). Sex, drugs and Facebook.*

متوفر في الموقع الإلكتروني لـ The Sun Journal:
www.sunjournal.com/news/city/20060827102.php

Chalfant, D. (2005, August 27). *Facebook postings, photos incriminate dorm party-goers.*

متوفر في الموقع الإلكتروني لـ Northerner:
www.thenortherner.com/media/paper527/news/2005/11/02/News/Facebook.Postings.Photos.Incriminate.Dorm.PartyGoers-1042037.shtml

Dicton, B. (2006, April 11). *Gay student expelled from Baptist University*.

متوفر في الموقع الإلكتروني لـ Spero News:
www.speroforum.com/site/article/as?id=3248

Dorsy, M. (2007, October 4). *VSU expels student.*

متوفر في الموقع الإلكتروني لـ Valdosta Daily Times:
www.valdostadailytimes.com/local/local_story_277232726.html

Facebook connecting more than students. (2005, December 2).

متوفر في الموقع الإلكتروني لـ PhysOrg.com:
www.physorg.com/news8698.html

Facebook users: Trading privacy for friends? (2007, September 26). Agence France-Presse (AFP.com).

متوفر في الغوغل على الرابط التالي:
http://afp.google.com/article/ALeqM5jKnwxgE-aeuySPNnJwqL-ZPaoT3w

Fischman, J. (2007, May 4). *Threat on MySpace leads to expulsion.*

متوفر في الموقع الإلكتروني لـ The Chronicle of Higher Education:
http://chronicle.com/wiredcampus/article/2041/college-expels-student-after-threating-myspace-note

Gosden, E.(2007, July 17). *Student's trial by Facebook*.

متوفر في الموقع الإلكتروني لـ The Guardian:
www.guardian.co.uk/media/2007/jul/17/digitalmedia.highereducation/

Guess, A. (2008, January 11*). Maybe he shouldn't have spoken his mind.*
متوفر في الموقع الإلكتروني لـ Inside Higher Ed:
www.insidehighered.com/news/2008/01/11/Valdosta

How to help your kids use social networking websites more safely. (2006, Novemeber 9).
متوفر في الموقع الإلكتروني لـ Microsoft:
www.microsoft.com/protect/family/activities/social.mspx

Jadhav, A. & Graber, S. (2006, November 9).
متوفر في الموقع الإلكتروني لـ Valdosta State University's The Spectator:
www.vsuspectator.com/2006/10/02/students-sex-story-on-web-backfires/

Luymes, G. (2007, June 24). *Abbotsford teen expelled for online threat to kick teacher.*
متوفر في الموقع الإلكتروني لـ The Province:
www.canada.com/theprovince/news/story.html?id=3dd47e30-a00c-4b27-9ec3-6b73973231b1

National Association for College Admission Counseling.
www.nacacnet.org/MemberPortal/News/StepsNewsletter/myspace_students.html

Phishers can use social websites as bait to net victims. (2007, May 24).
متوفر في الموقع الإلكتروني لـ PhysOrg.com:
www.physorg.com/news99238473.html

Ruggles, R. (2007, May 3). *College "portrayed me as a monster," student says*.
متوفر في الموقع الإلكتروني لـ Omaha World-Herald:
www.omaha.com/index.php?u_page=2798&u_sid=2377278

Savo, K. (2007, September 26). *Facebook and the college student: How online presents affect college students across America.*
متوفر في الموقع الإلكتروني لـ The Waltonian [Eastern University (St. Davids, Pennsylvania) student newspaper]:
http://media.www.waltonian.com/media/storage/paper752/news/2007/09/26/News/Facebook.And.The.College.Student-2993429.shtml

Schwetzer, S. (2005, October 6). *Fisher College Expels student over website entries.*
متوفر في الموقع الإلكتروني لـ boston.com:
www.boston.com/news/local/articles/2005/10/06/fisher_college_expels_student_over_website_entries/

ScienceDaily (2007, September 14). *Is social networking changing the face of friendship?*
متوفر في: www.sciencedaily.com/releases/2007/09/070912161147.htm

Students should use common sense when posting to Facebook.com, say expert. (2007, July31).
متوفر في الموقع الإلكتروني لـ PhysOrg.com: www.physorg.com/news105120793.html

WiredSafety.org website:
www.wiredsafety.org/internet101/blogs.html
يوفر WiredSafety سلسلة واسعة ومتنوعة من المعلومات ويساعد على السلامة على الشبكة الإلكترونية.

Ybarra, M.L., Mitchell, K. J., Finkelhor, D., Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. Archives of Pediatrics & Adolescent Medicine 161(2), 138-145.
متوفر في: http://archpedi.ama-assn.org/cgi/content/full/161/2/138

الفصل الثامن

التواصل على شبكة الإنترنت
Communicating Online

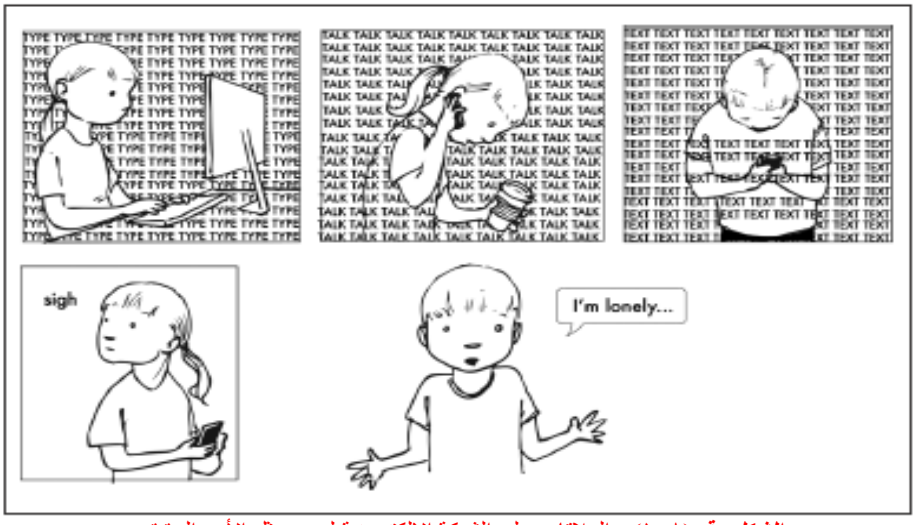
أكره المدرسة ¸ أكره والديَّ ¸ أكرهك.

POS (والدي موجود خلفي)، L8R (لاحقًا)، TTFN (باي باي الآن)، LOL (ضحك بصوت عالي)، ASL (العمر/ الجنس/ المكان): يميز معظم الطلاب اليوم هذه الاختصارات كلغة جديدة، أسلوب من المختصرات للتواصل مع الآخرين على الشبكة الإلكترونية. قد يرى العديد من البالغين هذه القائمة يتساءلون حول معنى هذه الاختصارات؛ إن غالبية الأطفال والمراهقين المعتادين على الشبكة الإلكترونية يعرفونها على الفور. ومع ذلك، يجب أن يعي طلابك الفروقات بين الحياة الحقيقية وأساليب التواصل على الشبكة الإلكترونية. التمرين ٨–١ – قاعدة الاختصارات، والذي يطلب من الطلاب إعداد قائمة بأكبر عدد ممكن من الإختصارات، يعد مقدمة جيدة لهذا الموضوع.

> إن العلاقة الملموسة مع أحد على الشبكة الإلكترونية تجعل الطلاب مندمجين بالمحادثة، حتى وإن كانت المحادثات وضيعة أو تحرشية، أو إذا كان الشخص الذي يتحدثون معه فقط لمجرد المعرفة، أو قد يكون غريبا تمامًا.

الرسائل الإلكترونية، والرسائل الفورية، والمدونات مملوءة بلغة وضيعة ومؤذية. وبسبب الاختصارات وأسلوب المحادثة على الشبكة الإلكترونية، فإن تعليقات التحرش ليست في العادة مغطاة بلغة لطيفة أو تمنح أي نوع من السياق. عوضا عن ذلك، تتواجد التعليقات الوضيعة لوحدها، ويمكن أن توجد أثرًا قويًا على القارئ. التمرين ٨–٢ – أنا أمزح فقط (؟) يطلب من الطلاب التمعن بنص رسالة على التراسل الفوري والتي تحتوي على رسالة ممزوجة. التمرين ٨–٣ – من السهل أن تكون وضيعًا يقدم للطلاب فرصة مناقشة السبب حول سهولة أن تكون وضيعًا ومؤذيًا على الشبكة الإلكترونية أكثر من التقابل وجها لوجه. التمرين ٨–٤ – وجه لوجه مقابل التواجد على المساحة السيبيرية (مساحة وهمية يستخدمها الشخص لدى التواجد عل الشبكة الإلكترونية) يطلب من الطلاب الأخذ بعين الاعتبار وتصنيف أنواع الأشياء التي قد يقولها الطلاب على التراسل الفوري والتي لا يقولونها لأحد بوجهه. ومن ثم يصنف الطلاب هذه الأنواع على النحو التالي: بناء علاقة، تدمير علاقة، أو ليس لها أي أثر على العلاقة.

يوجد العديد من الأسباب والدوافع لدى الطلاب ليفضلوا التواصل على الشبكة الإلكترونية، ومع ذلك فإن التواصل على الشبكة الإلكترونية ليس دائمًا أفضل أداة للتواصل.



الشكل رقم (٨–١) : العلاقات على الشبكة الإلكترونية ليست مثل الأمر الحقيقي

التمرين ٨–٥ – التراسل الفوري: علاج للخجل؟ يكشف سبب شعور الطلاب في حالات معينة بالراحة بشكل أكبر في التواصل على الشبكة الإلكترونية بدلاً من التعامل وجهاً لوجه. يتناول هذا التمرين إيجابيات وسلبيات اختيار التواصل على الشبكة الإلكترونية وكيف يمكن أن يحد من تطور أحدهم. التمرين ٨–٦ – ماذا تستطيع أن تصدق؟ يطلب من الطلاب تقييم محادثاتهم على الشبكة الإلكترونية وكم عدد المرات التي قد لا يقولون أو يستلمون تصريحات حقيقية. يجب أن تساعد هذه التمارين الطلاب على تأمل أنفسهم فيما يتعلق بمهارات التواصل والتنمية الشخصية والقدرة على بناء علاقات.

ابتسامة مزيفة؟

إن البشر عبارة عن حيوانات بصرية إلى حد كبير. يمكن ان تؤثر هذه الخاصية البشرية بشكل قوي على طريقة تواصلنا. إن نقص النماذج البصرية في غالبية الإتصالات على الشبكة الإلكترونية هو أحد أسباب سهولة خداع الآخرين على الشبكة الإلكترونية..

قام العالم النفسي بول إيكمان Paul Ekman بدراسة تعابير الوجه لمدة أربعين سنة وقام بفهرسة أكثر من ١٠،٠٠٠ حركة عضلية مختلفة للوجه (يحتوي الوجه البشري على ما يقارب ٨٠ عضلة) المشتخدمة في التعبير البشري، في كل من الوعي أو بشعور اللاوعي.

إلى أي درجة يستطيع طلابك تفسير تعابير الوجه؟ أنظر إذا كانوا يستطيعون تحديد الإبتسامة الحقيقية من الإبتسامة المزيفة. يمكن العثور على اختبار يدعى Spot the Fake Smile على علوم البي بي سي BBC Science (www.bbc.co.uk/science/humanbody/mind/surveys/smiles/)

هل وجدت هذا ممتعاً؟ لمزيد من المعلومات حول عمل الدكتور إيكمان Ekman، قم

بقراءة المقالة المعنونة بـ "العقل الأمريكي العلمي: نظرة تكشف كل شيء" "Scientific American Mind: A Look Tells All"، على:
www.sciam.com/article.cfm?articleID=0007F06E-B7AE-1522-B7AE83414B7F0182&sc=I100322

التمارين

التمرين (٨-١):
قاعدة الاختصارات

اطلب من طلابك ابتكار قائمة بأكبر عدد ممكن من الاختصارات التي يستخدمونها على الشبكة الإلكترونية. تأكد من أنهم يقدمون شرحا للمختصر. على سبيل المثال، POS تعني "والدي موجود خلفي". اطلب منهم عدم تضمين أي شيء يتعلق بلغة مؤذية. قم بإعداد قائمة بإجابات الطلبة.

وفيما يلي قائمة كعينة على هذه الإختصارات مع تفسيرها:

ASL	العمر/ الجنس/ المكان
BYKT	لكنك تعرف ذلك
CYL	أراك لاحقًا
FWIW	ماذا تساوي
IITYWYBMAB	إذا أخبرتك هل تشتري لي مشروبا
IMO	حسب رأيي
L8R	لاحقًا
LOL	أضحك بصوت عالي
OTOH	من ناحية أخرى
POS	والدي موجود خلفي
ROFL	أتدحرج على الأرض من الضحك
RTFM	إقرأ الكتيب الغبي
TTFN	باي باي الآن

التمرين (٨-٢):
أنا أمزح فقط (؟)

اطلب من طلابك قراءة الرسالة الفورية أدناه والإجابة عن الأسئلة التي تليها. أخبرهم بأن هذه رسالة مرسلة من صديق إلى آخر.

Hi h8 skl rents h8u
مرحبًا، أكره المدرسة، أكره والداي، أكرهك

١. ما الذي تقوله الرسالة؟ (مرحبًا، أكره المدرسة، أكره والديّ، أكرهك.)
٢. كيف سيشعر معظم الطلاب إذا استلموا هذه الرسالة؟
٣. إذا استلمت هذه الرسالة، هل ستعرف بشكل أكيد إن كانت حقيقية أم لا؟
٤. هل تغير إشارة الوجه المبتسم طبيعة الرسالة؟
٥. كيف تعرف أن أحد يمزح على الشبكة الإلكترونية؟ هل الحرف (jk) والتي تعني (just kidding) ومعناها (أنا أمزح فقط) أو الوجه المبتسم يوصل المعلومة دائما؟ لماذا ولماذا لا؟
٦. أيهما يحمل قوة أكثر، الكلمات أم الوجه المبتسم؟

قم بالتاكيد على الطلبة أن الكلمات تحمل قوة. إن كتابة "jk"والتي تعني (just kidding) ومعناها (أنا أمزح فقط) أو إضافة الوجه المبتسم ببساطة لا يلغي الأذى الذي يمكن أن تسببه تلك الكلمات. لسوء الحظ، يصبح العديد من المراهقين اليوم ضعيفي الإحساس بلغة التحرش وفي بعض الأحيان يحتاجون إلى تذكيرهم بأن لغة معينة هي بالتأكيد مؤذية ومهينة.

التمرين (٨-٣):
من السهل أن تكون وضيعًا

بعد اثني عشر عامًا من دراسة سلوك المراهقين على الشبكة الإلكترونية، وجدنا أن جميع المراهقين تقريبًا يتفقون أنه من الأسهل كثيرًا أن تكون وضيعًا ومؤذيًا على الشبكة الإلكترونية من التقابل وجهًا لوجهٍ. إسأل طلابك إعداد قائمة بخمسة أسباب لاتقادهم بأن هذا صحيحا.

يجب أن تتضمن قائمة الطلاب بعض مما يلي:

١. لا تستطيع رؤية تعابير الأشخاص على الشبكة الإلكترونية؟
٢. تستطيع حذف الرسالة حالما ترسلها ومن ثم تنسى كل شيء يتعلق بها.
٣. من الأسهل أن تكون مشاغبًا عندما لا يكون لديك تغذية راجعة فورية، مثل النماذج الاجتماعية عند مشاهدة أو سماع مشاعر شخص تعرض للأذى.
٤. لا يوجد أحد لإيقافك، لذلك لا يوجد إحساس بأنه سيتم الإمساك بك أو العثور عليك.
٥. الجميع يفعل ذلك.
٦. تستطيع إرسال رسالة بشكل مجهول باستخدام اسم مستخدم غير معروف وتعلم بأنه لن يتم اكتشافك.

التمرين (٨-٤):

وجه لوجه مقابل التواجد على المساحة السيبيرية
(مساحة وهمية يستخدمها الشخص لدى التواجد
على الشبكة الإلكترونية)

اطلب من طلابك النظر إلى التصريح التالي وأن يحاولوا معرفة النسبة المئوية المفقودة.

---% من المراهقين الذين شملهم الاستطلاع أفادوا أنهم كتبوا شيئًا أثناء التراسل الفوري لا يقولونه لأحد وجها لوجه.

والآن قم بإجراء استطلاع للرأي بدون كتابة الإسم. اطلب من الطلاب كتابة نعم أو لا على قصاصة ورق للإشارة إن كانوا كتبوا شيئا أثناء التراسل الفوري لا يقولونه لأحد وجها لوجه. قم بإحصاء النتائج. ما هي النسبة الحقيقية لصفك؟

في شهر يوليو/ تموز من عام ٢٠٠٥م، أفاد تقرير من Pew Internet and American Life Project بأن حوالي ٣١% من المراهقين أفادوا أنهم كتبوا شيئا أثناء التراسل الفوري لا يقولونه لأحد وجها لوجه (www.pewinternet.org/pdfs/PIP_Teens_July2005web.pdf). تقترح حواراتنا غير الرسمية مع آلاف الطلبة في الصفوف من ٤ – ١٢ خلال السنوات القليلة الماضية أن النسبة المئوية الآن هي على الأرجح أكثر من الثلثين.

اطلب من الطلبة تصنيف أنواع الأشياء التي قد يقولها المراهقون اثناء التراسل الفوري لا يقولونه لأحد وجها لوجه. ما الفئات التي ابتكروها. من المرجح أن تشتمل على ما يلي:

- أكاذيب.
- تهديدات.
- مجاملات.
- إحباطات.
- تصريحات محرجة.
- ملاحظات شخصية.
- تصريحات تحرش.

ثم، اطلب من الطلبة الإشارة إلى هذه الفئات كإحدى ما يلي:

١. بناء علاقة.
٢. تحطيم علاقة.
٣. ليس لها أثر على العلاقة.

التمرين (٨-٥):
التراسل الفوري: علاج للخجل؟

قم بتقديم القصة التالية إلى طلابك

قصة سكوت Scott

سكوت طالب في الصف السابع. وعلى مدار العديد من الشهور، شعر بالانجذاب نحو زميلته كريستينا. لسوء الحظ، كان سكوت خجولاً. ويقدر ما كان يحب ذلك، إلا أنه لم يستطيع أن يتحدث مع كريستينا وجها لوجه. وجد نفسه في بعض الأحيان يجلس بجانبها في الصف أو يقف خلفها في طابور الغداء لكنه ما زال متوترًا جدًّا للتحدث معها.

وفي يوم في الصف، سمعها سكوت تتحدث مع صديق. سألها صديقها عن اسم المستخدم الخاص بها على التراسل الفوري، وأجابته أنه ShoppinGurl13247. لم يستطيع سكوت تصديق ما سمعه! قام بكتابة الاسم بسرعة كبيرة وعد الساعات التي يستطيع فيها الدخول على التراسل الفوري.

ولاحقًا في ذلك المساء، أضاف سكوت كريستينا إلى قائمة أصدقائه وخلال ساعة وجد أنها موجودة على الشبكة الإلكترونية. أرسل إليها رسالة فورية يقول فيها "مرحبًا". ومما أثار دهشته كثيرا، أجابت كريستينا على الفور. تحدث سكوت مع كريستينا على التراسل الفوري لأكثر من عشرة دقائق قبل أن تخبره أن عليها الذهاب. شعر سكوت بالسعادة والشوق!

وفي الأمسيات التالية، كان سكوت ينتظر كريستينا لتسجل الدخول على الشبكة الإلكترونية بحيث يستطيع التحدث معها. وفي أغلب الأحيان، لم تستمر محادثاتهم على التراسل الفوري أكثر من عشرين دقيقة. ولأكثر من أسبوع، كان سكوت يتحدث مع كرسيتينا عبر التراسل الفوري ولكنه بقي خجولا جدا ليتحدث إليها شخصيًا.

قم بطرح الأسئلة التالية على طلابك:

١. إذا كنت صديق سكوت، هل تشجعه على التحدث مع كريستينا وجها لوجه؟
٢. هل تعتقد أن التراسل الفوري جيد لسكوت ، حيث أنه خجول؟ لماذا أو لماذا لا؟
٣. هل يساعد الحاسوب سكوت على التغلب على خجله، أو هل تعتقد أن سكوت يختبأ وراء الحاسوب للتحدث مع كريستينا ؟

التمرين (٨-٦):
ماذا تستطيع أن تصدق؟

" بينما يكذب المراهقين بسهولة وبشكل اعتيادي على بعضهم على الشبكة الإلكترونية، فإنهم في العادة يصدقون ما يقال لهم".

قم بكتابة التصريح أعلاه على اللوح. قم بطرح الأسئلة التالية على طلابك:

١. هل تعتقد أن التصريح أعلاه حقيقي أم غير حقيقي؟ لماذا؟
٢. لماذا تعتقد ان المراهقين يسعون لتصديق ما يقال لهم على الشبكة الإلكترونية؟
٣. كيف يمكن لهذه الميول تصديق ما يقوله الآخرين لك أن يؤثر في تجاربك على الشبكة الإلكترونية؟
٤. يقول خبراء السلامة على الشبكة الإلكترونية أن المراهقين يجب أن يرتابوا من كل شيء يقرأونه على الشبكة الإلكترونية. لماذا تعتقد أن الخبراء شكلوا هذا الرأي؟

الفصل التاسع

التعلم لفهم القراءة والكتابة الإعلامية
على الشبكة الإلكترونية
Learning to Be Media Online Savvy

يجب أن يفهم الطلاب بأنه بصرف النظر عما يفعلونه على الشبكة الإلكترونية, يحاول الآخرون التلاعب بتفكيرهم وسلوكهم.

كلما يصبح الطلاب مستخدمين بشكل أكبر لوسائط القراءة والكتابة الإعلامية، فإن ثقافة وسائط القراءة والكتابة الإعلامية لديهم تعتبر بشكل متزايد قيمة لتعليمهم. ليس المقصود من هذا الفصل أن يكون مساقًا كاملاً عن ثقافة وسائط القراءة والكتابة الإعلامية ولكن المقصود منه مقدمة للموضوع، وبخاصة في سياق الحياة على الشبكة الإلكترونية، ويبدأ بمساعدة الطلاب على التفكير بشكل دقيق حول وسائط القراءة والكتابة الإعلامية التي تهاجمهم بعنف.

يجب أن يتعلم كل طالب أن يصبح مفكرًا دقيقًا عندما يقرر الفاعلية والدافع لمصدر معلومات على الشبكة الإلكترونية. يجب أن يفهم الطلاب أنه بصرف النظر عمّا يفعلونه على الشبكة الإلكترونية، يحاول الآخرون التلاعب بتفكيرهم وسلوكهم.

قم بتذكير الطلاب أن:

- جميع وسائط الكتابة والقراءة الإعلامية، بما فيها محتوى الشبكة الإلكترونية، مبنية على أساس وجود تأثير محدد عليهم.
- يمكن أن تؤثر رسائل وسائط الكتابة والقراءة الإعلامية على المعتقدات والقيم والسوكيات.
- لدى مبتكرو وسائط الكتابة والقراءة الإعلامية هدف معين أو برنامج للرسائل التي يبتكرونها.

الإعلان والتأثير: تفكيك الإعلانات

قد لا يكون طلاب المدرسة الثانوية قد فكروا ابدًا بالأشخاص الذين تستهدفهم إعلانات ومعينة وما الذي تأمل أن تحققه هذه الإعلانات. وبشكل خاص في بيئة الشبكة الإلكترونية، فإن الوعي حول السبب والكيفية التي تحاول فيها الإعلانات التلاعب بهم غير قيمة.

التمرين ٩–١ – من المستهدف؟ يطلب من الطلاب تحليل الإعلانات على الشبكة الإلكترونية بينما يأخذون بعين الإعتبار الجمهور المستهدف وكيف يحاول الإعلان أن يسيطر على الجمهور. توجد تمارين مشابهة للتمرين ٩–١ عن تفكيك الإعلانات متوافرة على New

Mexico Media Literacy Project (www.nmmlp.org/media_literacy/deconstruction_gallery.html). يحتوي المشروع على معرض للإعلانات التلفزيونية، يدعى معرض التفكيك، بالإضافة إلى دليل للمعلمين والطلاب في تفكيك رسائل وسائط الكتابة والقراءة الإعلامية.

البنرات الإعلامية الشائعة

يتخم المعلنون في العادة المواقع الإلكترونية الشائعة بنفس النوع من البنرات الإعلانية لمدة من الزمن. إن أكثر أسلوبين شائعين جدا للاعلانات التي ظهرت على أعلى أو جوانب صفحة الشبكة الإلكترونية هما "Win the Race" و "Romance Quiz". التمرينات ٩–٢ و٩–٣ و ٩–٤ يطلب من الطلاب تحليل الإعلانات التي تستخدم لعبة مثل الجودة لجذب جمهورها. إن بعض الأمثلة تؤدي إلى الهدف المتنقل مثل ركوب لوح التزلج، أو تلبيس لعبة. التمرين ٩–٢ – الإعلانات التفاعلية على الشبكة الإلكترونية، الجزء الأول، يطلب من الطلاب الأخذ بعين الاعتبار إعلانًا يقدم المرادف على الشبكة الإلكترونية لتزيين لعبة، والذي يحاول بوضوح استمالة الفتيات تحت سن السادسة عشر. فمن غير المرجح أن العديد من الفتيات المراهقات الاكبر عمرًا سيبدين الكثير من الاهتمام في تزيين أو تجميل سوينكيZwinky. يأمل المعلنون بأنه بعد اللعب مع سوينكيZwinky وخزانتها، سوف ينقر الزائر على رابط الحصول على سوينكي "Get Zwinky!".

التمرين٩–٣ – الإعلانات التفاعلية على الشبكة الإلكترونية، الجزء الثاني، يطلب من الطلاب التمعن بنوع إعلانات "Win the Race"والتمرين ٩–٤ – الإعلانات التفاعلية على الشبكةالإلكترونية، الجزء الثالث، يطلب من الطلاب التمعن بنوع إعلانات " Take a Quiz"، سوف يميز الطلاب هذه الإعلانات، تأملوا بالجداول المخفية للإعلانات ومناقشة نجاح الآليات التسويقية على أنفسهم والآخرين.

قد يرغب المعلمون بمتابعة المناقشة من التمرين ٩–٤، السؤال ٤، بتعيينه واجب منزلي أو مشروع داخل الصف والذي يطلب من الطلاب جمع الإعلانات التي يعتقدون أنها ناجحة في جذب انتباههم.

الإعلان الذي يستهدف السلوك

يستهدف المسوقون والمعلنون المراهقين بشكل كبير والأطفال، في محاولة للتلاعب بهم والتأثير في اتخاذ قراراتهم الشرائية.

قدم موقع eMarketer.com تقريرًا عن مجموع الإنفاق للإعلان على الشبكة الإلكترونية الذي يستهدف السلوك في عام ٢٠٠٦م بما مجموعه ١.٢ بليون دولار أمريكي (eMarketer, 2006). بسبب قدراتهم التقنية، يمكن أن يستهدف المسوقين المستخدمين بشكل دقيق جدًّا من خلال المعلومات التي جمعوها، بما فيها:

- مزود خدمة الشبكة الإلكترونية الخاص بك.
- الوقت الذي تفضل فيه التواجد على الشبكة الإلكترونية خلال اليوم.

- المواقع الإلكترونية التي تحب زيارتها.
- الكلمات المفتاحية (صديق، شبكة، مدونة،..إلخ) التي تستخدمها على محركات البحث أو ضمن موجهات محددة لمواقع البحث (على سبيل المثال، فئة اللعب على الياهو Yahoo!'s gaming category).
- أية مجموعة مما ورد أعلاه.

ووفقا لكاري وودراف Carrie Woodruff، الشريك السابق والمدير الإعلامي في Fidelity Investments، يدمج المعلنون على الشبكة الإلكترونية رسائلهم في محتوى الشبكة الإلكترونية أو التكنولوجيا التي سيعتبرها المراهقين "رائعة" لأن المراهقين يستخدمون الشبكة الإلكترونية لكل من التسلية والفرصة لاستخدام أحدث التكنولوجيا. في كثير من الأوقات، ما يشبه محتوى الموقع الإلكتروني هو في الواقع نتيجة شراكة تسويق بين المعلن وما يجري على الموقع الإلكتروني، وصمموا شيئا مع بعضهم لجذب انتباهكم.

يقول وودرف Woodruff أن المعلنين لا يهتموا في العادة بنقر المستخدمين عبر المواقع الإلكترونية. إنهم يتطلعون لوعي تجاه العلامة التجارية والولاء وخاصة بين المراهقين.

مشروع أم لا؟ تقييم المعلومات على الشبكة الإلكترونية؟

يمكن لأي أحد أن ينشر أي شيء على الشبكة الإلكترونية. لا يوجد أية خبرة أو أوراق اعتماد. لا يوجد أي شيء صحيح. إذا، كيف يستطيع الطلاب الحكم على محتوى الشبكة الإلكترونية. كيف يستطيعون معرفة إن كان أحدهم لديه برنامج؟ بمن يستطيعون الثقة على الشبكة الإلكترونية؟ فيما يلي بعض النصائح والتمارين لمساعدتكم على تمييز الحقيقة من الكذب.

يمكن أن يبدأ الطلاب تقييمهم بوساطة النظر على مجال الموقع الإلكتروني. يتم تحديد موقع كل موقع الكتروني على الشبكة الإلكترونية بوساطة عنوانه على شبكة الإنترنت، والجزء الأخير من العنوان يعرف بأنه المستوى الأعلى للمجال. على سبيل المثال: .com، .edu، أو .gov. يمكن أن يقول المجال في بعض الاحيان أن شيئًا مهما حول مصدر المعلومات، مما يعني أنه يمكن استخدامها فقط من أجل الهدف التي أنشات لأجله. إنها .gov، و .edu، و .mil. التمرين ٩–٥ – ماذا يوجد في مجال؟ يطلب من الطلاب تحديد أكثر الاختصارات الشائعة ذات المستوى الأعلى (.edu، و .com، و .org..إلخ) ومناقشة ما أنواع المواقع الإلكترونية التي يسمح فيها استخدام هذه المجالات.

يمكن أن تتضمن أعلى مستوى للمجالات رمز الدولة وتتألف من حرفين.
على سبيل المثال:
. Canada
.cn China

.de German (Deutschland)
.es Spain (Español)

دعونا نفكك العنوان العام للمورد على الشبكة الإلكترونية URL:
www.cdc.gov/flu/avian/gen-info/facts.htm

إن مصدر المعلومات في هذا العنوان العام للموقع على الشبكة الإلكترونية URL هو وكالة حكومة الولايات المتحدة الأمريكية التي تدعى مركز التحكم بالأمراض (Centers for Disease Control CDC). إن المعلومات التي تلي المستوى الأعلى للمجال، وفي هذا المثال هو .gov، يعتبر الممر داخل مزود الخدمة للملف الذي ترغب بمشاهدته. إن الملف الذي يحضره العنوان العام للمورد على الشبكة الإلكترونية URL، وهو facts.htm، هو عبارة عن مزود الخدمة داخل مجلد يدعى gen-info، الموجود داخل مجلد آخر يدعى avian، والذي يوجد بداخله مجلد آخر يدعى flu، إن.gov تخبرك بأن جميع المعلومات تأتي من الموقع الإلكتروني لحكومة الولايات المتحدة الأمريكية.

ويمكن القيام بنقطة مشابهة لأية معلومات تأتي من العنوان العام للموقع على الشبكة الإلكترونية URL مع مجال.mil، والذي يتم استخدامه من قبل جيش الولايات المتحدة الأمريكية فقط. يدل المجال.edu على المؤسسات التعليمية؛ ومنذ العام ٢٠٠١م، قد تكون هذه المؤسسات عبارة عن الكليات والجامعات فقط. ومع ذلك، فإن المدارس الإبتدائية والثانوية التي سجلت(dot-edu) قبل عام ٢٠٠١ م سمح لها بالاحتفاظ بمجالاتها.

يجب أن يتذكر الطلاب أن المعلومات الحقيقة والمشروعة والقيمة يمكن العثور عليها على كل من (dot-coms)و (dot-orgs)و (dot-infos). ومع ذلك، فإنها في العادة تتطلب عينًا ثاقبة لتحديد إن كان يوجد ضرر مخفي أو برنامج على هذه المواقع الإلكترونية. إن المعلومات التي تاتي من.com أو.info أو org أو biz أو.net هي أساسيًا غير مقيدة مما يعني أنه يمكن لأي أحد أن يسجل موقع إلكتروني في أي من هذه المجالات. وبناء عليه، قد تخبرك هذه المجالات بحد ذاتها أي شيء حول الكيان الذي يشغل الموقع الإلكتروني وقد تكون مضللة.

التمرين ٩–٦ – المستويات الأعلى للمجالات والضرر يطلب من الطلاب التحقق أكثر حول الكيفية التي يمكن أن تساعدهم هذه المجالات على تقييم المعلومات على موقع إلكتروني. يطلب من الطلاب النظر إلى مختلف العناوين العامة للمواقع على الشبكة الإلكترونية URLs، وإصدار حكم أولي على مشروعية محتواها، ومن ثم تقييم المواقع الإلكترونية وتحديد إن كان المحتوى حقيقي أو ضار.

سوف يساعد تطوير مهارات التفكير الدقيقة الطلاب أيضا على صقل مهاراتهم في التحقق من المواقع الإلكترونية المضللة. التمرين ٩–٧ – الانطباعات الأولى يطلب من

الطلاب النظر على المواقع الإلكترونية وتحديد غن كانت مضللة. يوفر هذا التمرين نشاطًا إضافيًا للطلاب الأكبر عمرًا والذين يطلب منهم التحقق من المواقع الإلكترونية ببرامجها الأكثر قوة ومزعجة. يحتاج المعلمون مراجعة هذا التمرين قبل سؤال الطلاب مشاهدة المواقع الإلكترونية المقترحة.

ما هو DHMO؟

هل يجب أن تكون معنيا؟
اطلب من الطلاب زيارة Dihydrogen Monoxide Research Division (www.dhmo.org). إن هذا موقع مضلل، تم بناء العديد من المواقع الإلكترونية للمحاكاة الساخرة لمعالجة قضية او أمر عام. إن Dihydrogen Monoxide هو الاسم الكيميائي للماء. قم بسؤال الطلاب عن مدة الوقت الذي استغرقهم لاكتشاف الدعابة.

ومن الطرق الأخرى المفيدة في تقييم هدف ومصادقية الموقع الإلكتروني هي بالتحقق من مؤلف او مالك الموقع الإلكتروني. ومكان آخر جيد للبدء به هو الموقع الإلكتروني "من هو؟" الذي سيخبر الطلاب من الذي يملك موقع إلكتروني. التمرين ٩–٨ – مجال بحث "من هو؟" يطلب من الطلاب البحث في العديد من العناوين العامة للمواقع على الشبكة الإلكترونية URLs لمعرفة مالكيها.

بالإضافة إلى البحث عن كثب عن أسماء المجال واستخدام موجهات "من هو"، من المهم أن يسأل الطلاب أنفسهم الأسئلة التالية عن المواقع الإلكترونية:

١. من يقف وراء هذا الموقع؟ هل يدرج الموقع الإلكتروني المعلومات حول من يدير الموقع بشكل واضح مثل بيام المهمة ومعلومات الاتصال والعنوان؟
٢. ما الذي يجعل أولئك الذين يديرون الموقع الإلكتروني خبراء؟ ما المؤهلات التي يمكن التحقق منها والتي تثبت أنهم خبراء يمكن الوثوق بهم؟ هل توجد طرق لتقييم خبرتهم في الموضوع؟ هل تعتقد المجموعات الأخرى والمؤسسات أو الأفراد ممن تثق بهم أنهم خبراء؟
٣. هل هم متحيزون؟ إذا كان الموضوع جدليًا، هل يقدمون أكثر من جانب واحد للنقاش؟
٤. هل المعلومات مؤرخة؟ هل يمكنك معرفة عمرها؟ هل يشير الموقع الإلكتروني آخر مرة تم فيه تحديثها؟

تمتلك العديد من الكليات والجامعات مصادر مفصلة وممتازة لتقييم المعلومات الموجودة على الإنترنت. لمزيد من المعلومات الرجاء التفضل بزيارة :

- جامعة كاليفورنيا في بيركلي University of California ar Berkeley: تقييم الصفحات الإلكترونية: آليات للتطبيق & أسئلة يجب طرحها (www.lib.berkeley.edu/TeachingLib/Guides/Internet/Evaluate.html)
- مكتبة جامعة كورنيل Cornell University Library: خمسة معايير لتقييم الصفحات الإلكترونية (www.library.cornell.edu/olinuris/ref/research/webcrit.html)

الأساطير المدنية وخدع البريد الإلكتروني

يمكن أن تنتشر الأساطير المدنية والخدع مثل حريق مدمر. وبمجرد القيام بنقرة، من السهل على الطلاب تمرير قصة "حقيقية" مدهشة أو مرعبة لجميع أصدقائهم.

التمرين ٩–٩ – استيعاب الخدع يطرح أمثلة حول بعض أكثر خدع البريد الإلكتروني الشائعة ويعطي الطلاب أدوات لمساعدتهم على تحديد عمليات الغش والإحتيال على البريد الإلكتروني، بما فيها قائمة بالمواقع الإلكترونية الممتازة التي يمكن أن تساعد الطلاب على التمييز بين الحقيقي والمزيف. التمرين ٩–١٠ – هل كانت أسطورة مدنية؟ يجعل الطلاب يبحثون في الرسائل الإلكترونية والمواقع أو القصص التي تواجههم في تحديد مصداقيتها. إن كلاً من هذه التمارين يشجع الطلاب على تحديد إن كانت أمرًا حقيقيًا عبر اختيار عبارة أو جملة من التواصل المشبوه وإدخالها في محرك بحث موثوق. إذا كانت نتائج البحث الرئيسية تتضمن روابط لمواقع إلكترونية متخصصة في الأساطير المدنية والخدع – سوف يعرفون أنهم كانوا على حق بالاشتباه بها.

التمارين

التمرين (٩-١):
من المستهدف؟

اطلب من الطلاب العثور على إعلانات على الشبكة الإلكترونية التي تستهدف سكان محددين من خلال تمييز أنماط الحياة الجذابة (بيوت كبيرة، وملابس جميلة، وأدوات رائعة، وتأييدات المشاهير.. إلخ). قم باختيار مثالين واطلب من الطلاب محاولة تفكيكهما. اطلب منهم مناقشة الكيفية التي تحاول فيها هذه الإعلانات التأثير علينا، ومن هو "نحن" أو غير ذلك.

اطلب من الطلاب أخذ بضع دقائق للإجابة على الأسئلة التالية حول كل إعلان:

١. من تعتقد بالضبط أن الجمهور المستهدف لهذا الإعلان هو؟
٢. ما المجموعة من الأشخاص في المجتمع الذين يستهدفهم هذا الإعلان ولماذا؟
٣. ما القيم الشخصية التي يحاول هذا الإعلان التلاعب بها أو التأثير عليها؟

التمرين (٩-٢):
الإعلانات التفاعلية على الشبكة الإلكترونية
الجزء الأول

اطلب من الطلاب التفكير في إعلان النافذة المنبثقة التالي. إن هذا الإعلان على الشبكة الإلكترونية تفاعلي في كون المشاهد يستطيع أن يسحب ويوزع الملابس والإكسسوارات عن وإلى سوينكي Zwinky لابتكار مظاهر مختلفة.

إعلان نافذة منبثقة لسوينكي Zwinky

قم بطرح الأسئلة التالية على الطلاب:

١. من الجمهور المستهدف في هذا الإعلان؟
٢. كيف يجذب الإعلان انتباه الجمهور المستهدف؟
٣. ما الذي يأمل المعلنون من الجمهور المستهدف فعله بعد اللعب بهذا الإعلان؟

التمرين (٩-٣):
الإعلانات التفاعلية على الشبكة الإلكترونية
الجزء الثاني

إسأل الطلاب التفكير بالإعلان الموضح أدناه، أسلوب شائع جدا للافتة إعلان.

لافتة إعلان "Win the Race"

إن هذا النوع من الإعلانات على الشبكة الإلكترونية ويحاول جعل المشاهد النقر على زر يحرك أمرًا مثل قارب أو متزلج أو المتزلج على الجليد للفوز بسباق. وما أن يربح السباق، يتم تمرير المشاهد إلى الإعلان الحقيقي. إن هذا موقع لنغمات الهاتف "المجانية" الذي في الحقيقة غير مجاني لأنه يجب على المشاهد التسجيل في خدمة مدفوعة.

قم بطرح الأسئلة التالية على الطلاب:

١. ما الطرق التي تشبه فيها لافتة الإعلان لعبة ما؟
٢. ما الفئة العمرية التي تعتقد أنها ستهتم كثيرًا في محاولة الفوز بهذه اللعبة؟
٣. لماذا تفترض أن المعلنين يستخدمون الإعلانات التفاعلية لمنتجاتهم؟

التمرين (٩-٤):
الإعلانات التفاعلية على الشبكة الإلكترونية
الجزء الثالث

إن إعلانات "Take a Quiz" هو نمط آخر شائع من لافتة الإعلانات. إنها تدعو المشاهد للقيام باختبار من نوع واحد أو آخر. قم بسؤال الطلاب التفكير في " Romance quiz" الموضح أدناه، وهو نمط شائع جدا للافتة الإعلان.

لافتة إعلان "Take a Quiz"

قم بطرح الأسئلة التالية على الطلاب:

١. ما الفئة العمرية التي تعتقد أنها ستهتم كثيرًا في محاولة الفوز بهذه اللعبة؟
٢. من سيهتمون على الأرجح في إجراء الإختبار، الأولاد أو البنات؟ لماذا تعتقد ذلك؟
٣. ما الذي يجعل إعلانات كهذه فعالة؟ هل هي ناجحة على الأرجح في النجاح في التاثير في سلوك المشاهد أكثر من الإعلانات الساكنة؟ لماذا؟
٤. ما أنواع الإعلانات الأكثر نجاحا لتجعلك تنقر عليها؟

التمرين (٩-٥):

ماذا يوجد في المجال (الدومين)؟

قم بسؤال الطلبة عن اختصارات لاعلى مستوى من المجالات وعلى ماذا تدل ومن هم المخولين لاستخدامها.

.edu	.mil
.com	.net
.gov	.org
.info	.biz

ملاحظات المعلم

.edu تعليمي (المؤسسات التعليمية لما بعد المرحلة الثانوية)؛ قد تستخدم بعض المدارس الابتدائية والثانوية.edu لأنهم حصلوا على مجالهم قبل تغيير قواعد المجال في العام ٢٠٠١م.

.com تجاري (تستخدم عمليا لأي نوع من المواقع، سواء أكانت تجارية أم لا؛ إن استخدامها ليس مقصورا على التجارة)

.gov الحكومة (يتم استخدامها من قبل حكومة الولايات المتحدة الأمريكية فقط ويتم إدارته من قبل إدارة الخدمات العامة؛ لا تستخدم كافة الوكالات الحكومية.gov).

.info المعلومات (مخصصة لمواقع المعلومات، لكن.info غير محددة ويمكن لأي أحد استخدامها لأي هدف).

.mil الجيش (مقصور استخدامه على جيش الولايات المتحدة الأمريكية فقط)

.net الشبكة (وهي في الأصل مصممة للشركات الموجهة بشبكة، مثل مزودي خدمة الإنترنت؛ ويمكن لأي شخص الآن التسجيل كـ.net، على الرغم من أنها اليوم تحت سيطرة مزودي خدمة الشبكات)

.org منظمة (مصممة للمنظمات مثل المنظمات غير الربحية، ولكن اليوم يمكن لأي أحد أن يسجل كـ. org).

.biz الأعمال (تم ابتكارها من أجل الأعمال لتوفير فرص تسمية إضافية لأن العديد من أسماء.com تم استخدامها)

يوجد على الأقل عشرة مستويات رئيسية للمجالات الأخرى على الأقل قيد الاستخدام، وهنالك أخرى يتم التفكير بها.

التمرين (٩-٦):
المستويات العليا للمجالات

كيف يمكن أن يساعدنا المستوى الاعلى للمجالات لتقييم شرعية المعلومات؟ افترض أن طلابك كانوا يعملون تقريرًا عن حقائق حول التدخين. اطلب منهم النظر على عناوين الشبكة الإلكترونية أدناه وتصنيفها إلى فئتين، تلك التي يعتقدون أنه يمكنهم الثقة بها (بدون برنامج أو تحيز)، وأولئك الذين لديهم تحيز أو برنامج أو سبب لإقناع أحد بتوجه معين. ثم دعهم يزورون الصفحات الإلكترونية بأنفسهم ورؤية إن كانت غرائزهم الفطرية صحيحة.

dccps.nci.nih.gov/tcrb/Smoking_Facts/facts.html
www.forces.org/evidence/evid/therap.htm
www.rochester.edu/uhs/healthtopics/Tobacco
www.washingtonvotes.org/2005-SB-5114
www.heartland.org/Article.cfm?artId=18285

إن مصدر أول عنوان عام للمواقع على الشبكة الإلكترونية من معهد السرطان القومي للمعاهد القومية للصحة National Cancer Institute of the National Institutes of Health، بينما ثالث عنوان عام للمواقع على الشبكة الإلكترونية من الخدمات الصحية الجامعية لجامعة روشيستر University of Rochester University Health Services. إن كل من الروابط الأخرى لأية منظمة أو قد يكون أو لا يكون لها أي تحيز معين أو برنامج. يدعو مقال Heartland.org حول التدخين بطريقة غير مباشرة تقرير NIH المتعلق " ٤٠٠٠ سم ومسرطنات الموجود في علم التدخين الضار.

التمرين (٩-٧):
الانطباعات الأولى

يمكن لأي أحد نشر موقع إلكتروني. إن الخبرة والمصداقية لا تعتبر متطلبات. ليس كل شيء على الشبكة الإلكترونية هو كما يظهر. هل يستطيع طلابك تحديد أي من المواقع الإلكترونية التالية لا فائدة منها؟

www.ovaprima.org
www.improbable.com/airchives/classical/cat/cat.html
www.bigredhair.com/boilerplate
www.d-b.net/dti/
www.rythospital.com/nanodocs/

الإجابة: جميع المواقع لا فائدة منها. ومن الواضح، بمجرد قراءة عنوان عام لموقع على الشبكة الإلكترونية لا يخبرنا الكثير حول محتوى موقع. يمكن العثور على مواقع لا فائدة منها خلال الشبكة الإلكترونية. إنها الآن عبارة عن نموذج رقمي من المحاكاة الساخرة.

ومن الأمثلة الأخرى ما يلي:

- بنك ويرليد (www.whirledbank.org) Whirled Bank، مقابل البنك الدولي World Bank (www.worldbank.org)
- الإعداد للطوارئ Preparing for Emergencies – الموقع الضار Preparing for Emergencies (www.preparingforemergencies.co.uk)، مقابل الإعداد للطوارئ: الموقع الرسمي للحكومة (www.preparingforemergencies.gov.uk).

بالنسبة للطلاب الأكبر سنا: موقع ضار لظاهرة الحياة الثانية هو GetAFirstLife.com

تمرين للطلاب الأكبر سنا

طالما استخدمت المجموعات العنصرية وضد السامية الدعاية للتأثير على المواقف والسلوك. إن موقع MartinLutherKing.org هو موقع إلكتروني ضد النظام الملكي ممول من قبل Stormfront، مجموعة كراهية عنصرية. في النظرة الأولى، يبدو أن MartinLutherKing.org هو موقع مشروع إلا أن تبدأ بقراءة التفاصيل. إن هذا الموقع ليس للطلاب الصغار. يجب على المعلمين زيارة موقع MartinLutherKing.org قبل السماح للطلاب بزيارته. يجب عليك التأكد من إرشاد طلابك إلى الموقع الإلكتروني الرسمي (www.thekingcenter.org).

ومثال إضافي على الدعاية المضللة هو من معهد المراجعة التاريخية The Insitute for Historical review (www.ihr.org). يصرح أصحاب هذا الموقع أنهم منظمة "غير عقائدية، غير دينية، وغير ربحية"، ومع ذلك فإنهم يحاولون بوضوح القيام بمراجعة

تاريخية من خلال مقالات مثل "هل مات ست مليون شخص بالفعل" " Did Six Million Really Die?"، والتي من مراجعها محرقة الحرب العالمية الثانية WWII Holocaust. لمشاهدة هذه المقالة، الرجاء زيارة الرابط التالي: www.ihr.org/books/hardwood/dsmrd01.html.

التمرين (٩-٨):
مجال بحث "من هو؟"

كيف يستطيع طلابك تحديد لمن العنوان العام للموقع على الشبكة الإلكترونية مسجل؟ إنه سهل! يتطلب فقط زيارة مجلس إدارة الشبكة الإلكترونية "من هو". يوجد المئات منها على الشبكة الإلكترونية. ببساطة قم بالدخول إلى روابط "من هو" مثل Register.com، Whois.net، Whois.sc و Whois.domaintools.com.

استخدم الموقع الإلكتروني لمجموعة الكراهية من التمرين ٩-٧ كمثال. في حقل البحث، دع الطلاب يدخلون martinlutherking.org والنقر على Go. Who owns the domain martinlutherking.org?.

وعلى النقيض من ذلك، حاول البحث على العنوان العام لموقع على الشبكة الإلكتروني لـ thekingcenter.org. يمكن لمعرفة من يملك العنوان العام لموقع على الشبكة الإلكتروني أن يساعد الطلاب على اتخاذ قرارات حول قيمة المحتوى وأية تحيز أو ضرر محتمل.

والآن اطلب من طلابك زيارة الموقع الإلكتروني AntiPolygraph.org (www.antipolygraph.org). سوف تجد أن هذا الموقع الإلكتروني يحدث جدلا قويا بأن اختبار كشف الكذب هو عبارة عن وسيلة ضعيفة لتحديد إن كان شخصًا ما يكذب. لكن من ابتكر الموقع الإلكتروني ولماذا. قم بجعل الطلاب يستخدمون موجه "من هو" للبحث عن AntiPolygraph.org. لمن هذا المجال مسجل؟ اطلب منهم إدخال اسم الشخص مع وجود قوسين حوله في محرك البحث العام. هل يستطيعون العثور على أية معلومات تشرح سبب إنشاء هذا الشخص لموقع الكتروني يسمى AntiPolygraph.org؟

تمرين للطلاب الأكبر سنًّا

اطلب من الطلاب استخدام موجه "من هو؟" للبحث عن هذا العنوان العام لموقع على الشبكة الإلكتروني وهو: www.animal-rights.com. سوف يشاهدون أن أبحاث BLTC يمتلك المجال. ثم اطلب منهم إدخال "BLTC Research" محاطة بقوسين في محرك البحث العام ومشاهدة إن كانوا يستطيعون العثور على تصريح بمهمة هذه الشركة. سوف يجدون أن المهمة فريدة من نوعها نوعا ما، وبعضهم قد يقول أنها فريدة إلى أبعد الحدود. إن هذا لا يقترح أن BLTC Research جيد أم سيء ولكن لديهم برنامجا، وبناء عليه فإنهم متحيزون.

ملاحظات المعلم

إن موقع AntiPolygraph.org مسجل باسم جورج ماستشي George Maschke. كان ماستشي Maschke موظفاً في خزينة الجيش عندما تدمرت مسيرته المهنية من قبل آلة لكشف الكذب عندما تقدم بطلب وظيفة في مكتب التحقيقيات الفيدرالي FBI.

التمرين (٩-٩):
استيعاب الخدع

قم بعرض الرسالة الإلكترونية التالية على طلابك. هل هي حقيقية أم خدعة؟

الموضوع: اللوكيميا – الرجاء قراءته وتمريره للآخرين.

الرسالة: إذا قمت بحذف هذه الرسالة، فإنك بالتأكيد لا تمتلك قلبًا.

مرحبا،

أنا أب وأبلغ من العمر ٢٩ عامًا. لقد عشت أنا وزوجتي حياة رائعة. أنعم الله علينا بطفل أيضا.ابنتنا اسمها ريتشيل Rachel وعمرها عشر سنوات. ومنذ مدة بسيطة اكتشف الأطباء أن لديها سرطان في الدماغ وفي جسدها الصغير. توجد هنالك طريقة واحدة لإنقاذها... عملية. لسوء الحظ، لا نمتلك نقودا كافية لدفع تكلفة العملية.

لقد وافق كل من AOL و ZDNET على مساعدتنا. إن الطريقة الوحيدة التي يمكنهم مساعدتنا بها هي هذه الطريقة. أرسل إليك هذه الرسالة الإلكترونية وأنت ترسلها لأشخاص آخرين. سوف تقوم AOL بتعقب هذه الرسالة الإلكترونية عدد الأشخاص الذين سيستلمونها. إن كل شخص يفتح هذه الرسالة الإلكترونية ويرسلها إلى ثلاثة أشخاص على الأقل سوف يمنحنا ٣٢ سنتًا.

الرجاء مساعدتنا.

إن الخطوة لتحديد إن كان أمرًا ما صادقًا أم لا هو استخدام محرك بحث موثوق. قم بجعل الطلاب يجدون عبارة في الرسالة الإلكترونية أعلاه وإدخال العبارة بين قوسين في حقل البحث. هل ترى أية روابط بين الخمسة نتائج الرئيسة للبحث التي تؤدي بك إلى الاعتقاد أن البريد الإلكتروني أعلاه ليس صادقًا؟ قم بالتأكيد على أن هذه التقنية لا تثبت الحقيقة من الكذب، ولكن إذا كانت نتائج البحث تقود إلى مواقع إلكترونية المتخصصة في الأساطير المدنية وسلسة رسائل أو خدع فإن الرسالة الإلكترونية هي على الأرجح غير صادقة.

تعرف Princeton University's WordNet (http://wordnet.princeton.edu) الأسطورة المدنية بأنها " قصة تبدو غامضة وتنتشر عشوائيًا بنماذج مختلفة وهي في اغلب الأحيان مزيفة؛ وتحتوي على عناصر الدعابة أو الخوف ويعتقد بشكل عام أنها حقيقية؟"

ربما تكون قد سمعت بقصة تحدث لصديق صديقك. في الواقع، إن قصص صديق لصديق شائعة على الشبكة الإلكترونية ويعتقد في أغلب الأحيان بأنها حقيقية. وفي نهاية المطاف، يتضح أنها مجرد خدع، أو تكون بأفضل حالاتها عبارة عن قصص مبالغ فيها. لسوء الحظ، إن هذه الأساطير والخدع يمكن أن تضللنا، وتجعلنا نشعر بالخوف، وكما

يمكن أن تغير مواقفنا وسلوكنا. ادعت آخر الأساطير المدنية أن مستحضرات إزالة العرق تسبب السرطان وأن ارقام الهواتف الخلوية سوف يتم كشفها للمسوقين عبر الهاتف. لم يكن أي من الإشاعتين صحيح، ولكنها انتشرتا مثل الحريق الهائل على الشبكة الإلكترونية.

كيف تستطيع إذا معرفة الحيقية من الخيال. هنالك الكثير من المواقع الإلكترونية الممتازة التي تراقب وتتحقق وتؤرشف وتعد تقارير عن الأساطير المدنية والخدع. إنها:

- BreakTheChain.org (www.breakthechain.org)، والمتخصص في الرسائل الإلكترونية المتسلسلة.
- Snopes.com (www.snopes.com)
- ScamBuster.org's Urban Legends and Hoaxes Resource Center (www.scambusters.org/legends.html)
- Sophos -Hoaxes (www.sophos.com/security/hoaxes/)
- Hoax-Slayer (www.hoax-slayer.com)
- TruthOrFiction.com (www.truthorfiction.com)
- Symantec's Threat Explorer (www.symantee.com/avcenter/hoax.html) والمتخصص في فيروسات الخدع.
- Vmyths (www.vmyths.com) والمتخصص في فيروسات الخدع.
- McAfee's Virus Hoaxes (http://vil.mcafee.com/hoax.asp)، قائمة والمتخصص في فيروسات الخدع.

التمرين (٩-١٠):
هل كانت أسطورة مدنية؟

قم بتعيين واحد او أكثر من المواقع الإلكترونية من القائمة في التمرين ٩-٩ لطلابك. اطلب منهم زيارة موقع أو مواقع وحاول تحديد أسطورتيين حضارتين أو خدع شاهدوها على الشبكة الإلكترونية أو تم استلامها في رسالة إلكترونية. اطلب منهم كتابة تقرير عن نتائجهم إلى بقية الصف.

قم بإخبار طلابك بأنه في المرة القادمة التي يستلمون فيها رسالة إلكترونية أو يشاهدون شيئًا مريبًا على الشبكة الإلكترونية، يجب أن يختاروا عبارة أو جملة منها، قم بوضع أقواس حول ما قمت باختياره، وقم إدخالها في محرك البحث. قم بتذكيرهم بأنه يمكنهم أيضا زيارة واحد من المواقع المدرجة في التمرين ٩-٩ واستخدم حقل البحث في الموقع للتحقق إن كانت مدرجة كأسطورة مدنية أو خدع.

المصادر

الموقع الإلكتروني لـ AdBusters: http://adbustersorg
سوف يجد الزائرون مجموعة من الإعلانات الكاذبة من مبتكري "ثقافة – مضادة". تحذير: إن هذا الموقع الإلكتروني غير ملائم للطلاب الصغار. قد يكون بعض المحتوى مؤذ ويحتوي على مشاهد تعري أو مشاهد جنسية. ومع ذلك، يمكن أن تكون الإعلانات المؤذية نقطة بداية مثيرة للاهتمام للطلاب في الصفوف من التاسع إلى الثاني عشر للبدء بمناقشة رسائل ثقافة القراءة والكتابة الإعلامية.

الموقع الإلكتروني لـ Center for Media Literacy : www.medialit.org
إن مركز ثقافة القراءة والكتابة الإعلامية هي عبارة عن مؤسسة تعليمية تشجع ثقافة الوسائط الإعلامية في مجتمعنا.

Critically analyzing information sources. (n.d.).
متوفر في الموقع الإلكتروني لمكتبة جامعة كورنيل Cornell University Library:
www.library.cornell.edu/olinuris/ref/research/skill26.htm
تمت كتابة صفحة مكتبة جامعة كورنيل Cornell University Library من قبل جوان أورموندرويد Joan Ormondroyd، يوفر قائمة طويلة من الإقتراحات لتحليل مصدر المعلومات.

eMarketer. (2006, April). *Online ad targeting: Engaging the audience*. (Analyst report). New York: Author.

Haris, T. (n.d.) *How urban legends work.*
متوفر في الموقع الإلكتروني لـ HowStuffWorks:
www.howstuffworks.com/urban-legend.htm

الموقع الإلكتروني لـ Internet Detective website: www.vts.intute.ac.uk/detective/
يوفر The Intute Virtual Training Suite أدلة توجيهية تعليمية تركز على الشبكة الإلكترونية والبحث.

الموقع الإلكتروني: www.justthink.org
إن مهمة JustThink.org هو "تعليم الشباب لقيادة الحياة الصحية والمسؤولة ومستقلة في ثقافة متأثرة بشكل كبير بالإعلام."

Kaiser Family Foundation (2005, March). *Generation M: Media in the lives of 8-18 years olds.*
متوفر في: www.kff.org/entmedia/7251.cfm

الموقع الإلكتروني لـ Media Awareness Network: www.media-awareness.ca

إن شبكة الوعي الإعلامي The Media Awareness Network في كندا Canada مصدر مميز للمعلومات حول ثقافة القراءة والكتابة الإعلامية، مع المواد البحثية والتعليمية للطلاب والمعلمين. يمكن استخدام العديد من المقالات المكتوبة جيدا كواجبات قراءة للطلاب في المدارس المتوسطة والثانوية.

الموقع الإلكتروني لـ Media Education Foundation
تنتج The Media Education مصادر تعليمية بما فيها أفلام، "الإيحاء بالتفكير الدقيق على الأثر الإجتماعي والسياسي والثقافي لوسائل الإعلام الأمريكية."

الموقع الإلكتروني لـ New Mexico Media literacy Project: www.nmmlp.org
يعتبر هذا مصدرا ممتازا لثقافة القراءة والكتابة الإعلامية، يضع هذا الموقع في بعض الأحيان عينة من الإعلانات التلفزيونية مصحوبة بأسئلة بهدف تفكيك الإعلان ويوفر عينة للتفكيك. تتضمن الميزات الممتازة كل من ثقافة القراءة والكتابة الإعلامية Media Literacy 101، إعلان سيء لحدث Bad Ad Event، جوائز الشهرة والصيت Fame and Shame Awards، وغيرها الكثير. كما يتم تشجيع الزوار لدخول مسابقات وتقديم تفكيكات الإعلان الخاصة بهم.

الموقع الإلكتروني لـ Project Look Sharp: www.ithaca.edu/looksharp/resources_join.php
يصف The National Media Literacy List Serve نفسه بأنه " قائمة بريدية تحتوي عدة عناوين للبريد الإلكتروني للأشخاص المشتركين لثقافة القراءة والكتابة الإعلامية بدعم من مجلس جنوب نيو مكسيكو للوعي الإعلامي Southern New Mexico Media Awareness Council. إن بابه مفتوح للمعلمين والإداريين وعاملين في الإعلام المقروء والمكتوب والباحثين وغيرهم حيث يتفاعلون بشكل حيوي في مشاريع أو قضايا تتعلق بثقافة القراءة والكتابة الإعلامية. يوجد في القائمة مسجلين من كافة انحاء العالم والعديد منهم معروفون كخبراء في ثقافة القراءة والكتابة الإعلامية بالإضافة إلى باحثين ومعلمين."

Piper, P. (2000, September). *Better read that again: Web hoaxes and misinformation.*
متوفر في الموقع الإلكتروني لـ eContent: www.infotoday.com/searcher/sep00/piper.htm

Teacher helpers: Critical evaluation information. (n.d.).
متوفر في الموقع الإلكتروني لـ Discovery education:
http://school.discovery.com/schrockguide/eval.html

الفصل العاشر

التعرف على عمليات الغش والنصب وتجنبها
Recognizing and Avoiding Phishing and Other Scams

تأتي عمليات النصب على الشبكة الإلكترونية بجميع الأشكال والأحجام.

كتب ألبرت إينشتاين Albert Einstein ذات مـــــــــرة: "لقد أصبح من الواضح بشكل مرعب أن التكنولوجيا لدينا قد فاقت إنسانيتنا". يمكن ان يشير هذا الاقتباس بشكل واضح إلى وجود عمليات النصب على الشبكة الإلكترونية. يجد الأشخاص عديمو الضمير دائمًا طرقًا جديدة وأفضل لاستخدام أدوات الشبكة الإلكترونية لخداع الناس. ماذا ستفعل إن استلمت الرسالة الإلكترونية التالية؟

الموضوع: مرحبا

من: "Themba Lindani" <absathemba@gmail,com>

صديقي العزيز،

أنا السيد/ ثيمبا ليندايني Themba Lindani، مدقق مالي في قسم التحويلات الأجنبية في إدارة بنك أبسا Absa Bank Admin، وأطلب إذنك في إعادة تحويل أموال والتي نرغب في تحويلها إلى حساب أجنبي. إن المبلغ الكامل الذي سيتم تحويله هو (١٤.٧٠٠.٠٠٠ دولار). أنا أتواصل معك كأجنبي لأنه لا يمكن اعتماد هذا المبلغ إلى بنك محلي هنا في جنوب إفريقيا، والأموال بعملة الدولار الأمريكي. إن مالك هذا الحساب هو السيد/ موريس تومبسون Morris Thompson من أمريكا، وتوفي منذ عام ٢٠٠٠م في تحطم طائرة مع زوجته وابنته في ٢٠٠٠/٠١/٣١م على متن خطوط آلاسكا، رحلة رقم ٢٦١ مع مسافرين آخرين على متن الطـــــائرة. يمكنـــــك التأكـــــد مـــــن الأمـــــر علـــــى الـــــرابط التـــــالي: www.cnn.com/2000/US/02/01/alaska.airlines.list/

أنا أعرض عليك نسبة ٣٠% لقاء مساعدتك لنا بينما استلم أنا وزملائي ٦٠%، وتبقى نسبة ١٠% مخصصة للنفقات. هل أنت مهتم في هذه العملية، والتي أقدرها كثيرًا واتمنى أن تكون كذلك، الرجاء تزويدي بالمعلومات أدناه:

١) رقم هاتفك الشخصي،
٢) رقم الفاكس،
٣) اسمك الكامل،
٤) العمر،
٥) الشركة، إن وجد،

٦) عنوان الإقامة.

لا نرغب بأن تذهب هذه الأموال إلى حساب حكومي كفواتير غير مطالب بها، لذا أرغب أنا وبعض الموظفين بأن تقدم نفسك كأحد أقارب المتوفي، بحيث يتم تحويل الأموال إلى حسابك. وعند استلام موافقتك والمعلومات المطلوبة أعلاه، سوف يتم الإتصال بك لتزويدك بالخطوات الدقيقة التي يجب أن تقوم بها، لكي تمكننا من إنهاء هذه العملية بشكل عاجل وسري. الرجاء إجابتي على البريد الإلكتروني الخاص وهو themba,lindani@gmail.com

مع أطيب التحيات،

السيد/ ثيمبا ليندانى Themba Lindani

يبدو من الواضح أن هذه الرسالة الإلكترونية هي عبارة عن عملية نصب واضحة، ومع ذلك فإن مجموعة "Nigerian advanced-fee scam"، كما تطلق على نفسها، نجحت في إيقاع آلاف الأشخاص حول العالم والاحتيال عليهم بملايين الدولارات. وحتى الأشخاص ذوي الدرجات العلمية العالية تم خداعهم. إن تاريخ ونجاح عملية النصب المذكورة موضح بالتفاصيل على الموقع الإلكتروني لـ Les Henderson's Crimes of Persuasion (www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm). بدأت عمليات الاحتيال في أواخر التسعينيات، ومنذ ذلك الوقت، نشأت آلاف التغيرات في كافة أنحاء العالم. أصبح العديد منها معقدًا للغاية وبدأت مشروعة نوعًا ما.

قد يعتقد طلابك أن أي أحد يقع ضحية هذا النصب قد يكون غبيا. لكن اطلب منهم النظر على الأشكال ١٠-١ و ١٠-٢ واسألهم إن كانوا يعرفون أي أحد وقع ضحية عمليات النصب في هذه الأشكال.

Joe has added you as a friend on Facebook. We need you to confirm that you are, in fact, friends with Joe.

To confirm this friend request, follow the link below:
http://network.facebook.com/reqs.php

Thanks,
The Facebook Team

الشكل رقم (١٠-١): عملية نصب متعلقة بالفيسبوك

Customer Support Center - Account Maintenance

Case ID Number: AT-09GP98-10-D709

Amazon.com Inc. is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account Amazon.com Inc. some of the advanced security systems in the world and our anti-fraud teams regularly screen the Amazon.com Inc. system for unusual activity.
In accordance with Amazon.com Inc.'s User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason: we encourage you to log in and restore full access as soon as possible. Please follow the link and renew your account information:

https://www.amazon.com/gp/rsl/ref=UTF8&login_viewRSL=1&rslpage=1

Completing all items will automatically restore your account access.

Thanks for your patience as we work together to protect your account.

Regards,
Customer Support Center.

Copyright 1996-2007, Amazon.com, Inc. or its affiliates

الشكل رقم (١٠-٢): عملية نصب متعلقة بـ Amazon.com

استهدفت عمليتا النصب المذكورتين فيما سبق مستخدمي الفيسبوك Facebook و Amazon.com في ٢٠٠٧م، وقد لا تزال فاعلة اليوم بشكل أو بآخر. استهدفت عمليات نصب مشابهة بنجاح آلاف مستخدمي MySpace. تم خداع الأشخاص للإفصاح عن معلومات الحساب الشخصي، والتي في بعض الحالات تم استخدامها لغايات الكسب المادي من قبل المحتالين وفي حالات أخرى بهدف إحراج صاحب الحساب.

إن هذين المثالين هما من أنواع النصب المدعوة "عمليات الغش"، والتي سيتم تناولها لاحقًا في هذا الفصل. تخدع أنواع النصب الأخرى الأشخاص على تنزيل برنامج يعتقدون أنه لهدف معين عندما يكون في الحقيقة برنامج ضار.

عمليات النصب على الشبكة الإلكترونية

تأتي عمليات النصب على الشبكة الإلكترونية بجميع الأشكال والأحجام. تأتي إليك على الشبكة الإلكترونية، في إعلانات، من خلال إعلانات الشبكة الاجتماعية، عبر النوافذ المنبثقة، وفي الرسائل الإلكترونية، وفي التراسل الفوري، وكما تكون أيضًا مخفية داخل صور وملفات موسيقى يتم تنزيلها. كما أنها ظهرت في الرسائل النصية على الهواتف الخلوية. في العديد من الحالات، تؤثر على مستخدمي PC و Mac على حد سواء، لأن العديد من عمليات النصب لا تتعلق بالبرامج التي تم تنزيلها.

دعونا نستعرض عملية النصب على MySpace "متعقب الملف" كمثال عليه (الشكل رقم ١٠-٣). يتم إنتاج متعقب الملف من قبل StalkerTrack.com، شركة مملوكة من قبل Blue China Group في هونج كونج.

الشكل رقم (١٠-٣): هل هذا برنامج مفيد؟ الرجاء قراءة المادة المطبوعة.

تدعي شركة StalkerTrack أنها شركة مشروعة توفر برنامجًا قيمًا ومجانيًا يسمح لمستخدمي MySpace من تعقب كل من يزور صفحتهم الخاصة على MySpace. إذا ما الخطأ في ذلك؟ ما الخطأ، كما تعلم طلابك، هل تلك العروض "المجانية" على الشبكة الإلكترونية تأتي مع سعر مخفي. في المادة المطبوعة للبرنامج المثبت لـ StalkerTrack، يشير إلى أن المستخدم يعطي StalkTarack إذنًا لعمل أي شيء تقريبًا على حسابهم الخاص بـ MySpace. وفيما يلي اقتباس من شروطهم:

باستخدام نموذج الدعاية الخاص بنا، فإنك تفوض بموجبه Blue China Group Ltd بشكل كامل لإرسال رسائل تجارية من خلال النشرات والتعليقات بالنيابة عن طرف ثالث عبر المعلومات التي تزودنا بها. إن هذا ليس موقع نصب يحاول خداعك للكشف عن معلومات شخصية. إن كل شيء نقوم به بمعلوماتك الشخصية سري هنا. إذا كنت تحت سن الثامنة عشرة، **يجب** عليك الحصول على إذن من والدك أو الوصي عليك قبل ملء هذا الأنموذج.

إن هذه الصفحة غير تابعة أو مدارة من قبل MySpace (tm). أية مسؤولية، بما في ذلك وليس على سبيل الحصر أية مسؤولية عن الأضرار التي تسبب بها أو يزعم أنها ناتجة عن أي فشل في الأداء أو خطأ أو حذف أو تفسير أو عطل أو تأخير في التشغيل أو نقل أو فشل خط الاتصالات، سوف يكون محددًا بشكل مقيد على المبلغ المدفوع من قبل أو بالنيابة عن المسجل لهذه الخدمة.

اطلب من طلابك إعادة قراءة الفقرة لأخيرة. إذا قام الطلاب بتنزيل هذا البرنامج وقام بإلحاق الضرر بحواسيبهم أو يضع محتوي غير ملائم على صفحاتهم على MySpace، ما مسؤولية هذه الشركة؟ الجواب هو:لا شيء! لا يدفع المستخدمون أي شيء لهذا البرنامج، وفي حال حدوث أضرار على حواسيبهم أو على سمعتهم على الشبكة الإلكترونية فإنه لا يتوجب عليها أي شي بالمقابل. ويوافق المستخدمون على هذا بالنقر على "موافق" عندما يثبتون البرنامج. القسم التالي للشروط يتضمن تفاصيل حول ما يمكن عمله على حساب مستخدم MySpace إذا تم تثبيت هذا البرنامج.

قد نقوم بعمل دمج لما يلي بناء على اهتمامات صديقك.

١. الدخول مؤقتا إلى حساب MySpace للهدف التالي (الأهداف التالية).
٢. قم بوضع منشورات "معلومات المتعقب" في القسم المناسب.

٣. تعليق أصدقائك حول هذا المتعقب.
٤. تقديم مواقع ترفيه جديدة.

إن هذه الخدمة مجانية. لن يطلب منك أن تدفع في أي وقت. لن يتم تسجيلك لأي شيء يطلب دفع. إن هذه الخدمة ممكنة للعديد من الساعات للجهود البشرية.

تحتفظ Blue China Group, Ltd بحقها في تغيير شروط الاستخدام/ بوليصة الخصوصية في أي وقت بدون إشعار. لمشاهدة أحدث نسخة لبوليصة التأمين هذه، قم ببساطة بالتأشير على هذه الصفحة كمرجع مستقبلي.

إن تفهم أن هذه الإتفاقية تسود في حال وجود خلاف بين الإتفاقية وشروط الاستخدام التي قبلت بها عندما اشتركت في MySpaces. كما أنك تفهم أنه بالدخول بشكل مؤقت إلى حسابك على MySpace، لا توافق Blue China Group, Ltd على شروط استخدام MySpace وبالتالي لا تلتزم بها.

ويتم تفسير هذه الإتفاقية وتخضع لقانون الإقليم الإداري الخاص لهونج كونج. فإنك توافق بوضوح على المكان الحصري والإختصاص الشخصي للمحاكم الواقعة في الإقليم الإداري الخاص في هونج كونج لأية أفعال ناشئة عن أو متعلقة بهذه الإتفاقية.

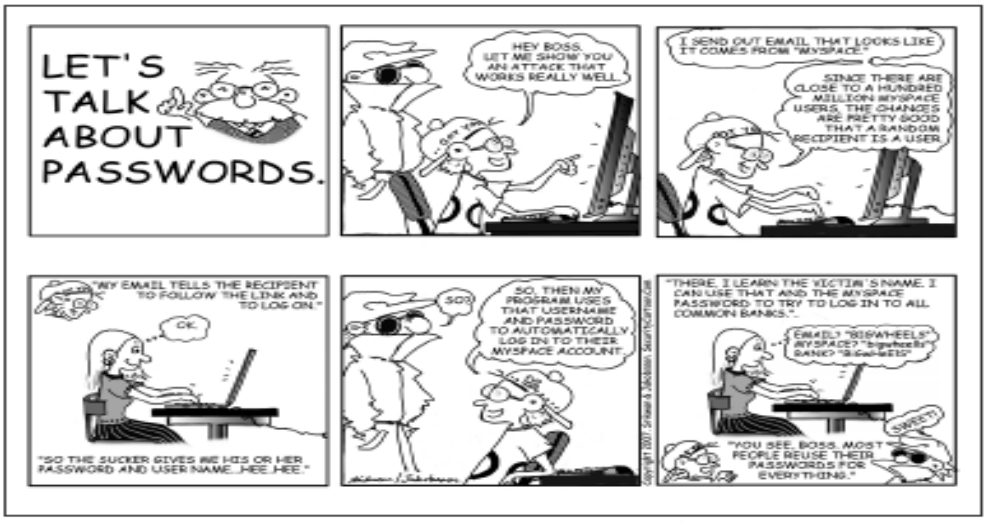
تم نسخها من StalkerTrack.com: http://stalkertrack.com/promo.html

إن مستخدمي MySpace الذين يثبتون هذا البرنامج يوافقون على الإفصاح عن هوية تسجيل الدخول الخاصة بهم وكلمة المرور لمالكي StalkerTrack، الذين يستخدمونها لأي شيء يرغبون فيه بدون استشارة المستخدم! إن ذلك يتضمن أصدقاء مستخدمي المراسلات الدخيلة ويضعون إعلانات على صفحات مستخدمي MySpace، وانتحال شخصية المستخدمين بينما يتواصلون مع أصدقاء لتشجيع برامج StalkerTrack ومنتجاتهم. لماذا يستطيعون عمل كل هذا؟ لأن المستخدم منحهم موافقته عندما نقر على زر "Accept" في برنامج التثبيت. إن "مجاني" لديها سعر زهيد جدا!

تراقب برامج التعقب الأخرى من يزورون صفحات شبكات التواصل الاجتماعي، حيث يتواجد هؤلاء الأشخاص، وما الذي ينقرون عليه وما يفعلونه أثناء تواجدهم على مواقع الشبكات الاجتماعية. إن جميع هذه المعلومات يتم تخزينها وتحليلها واستخدامها على الحواسيب المركزية للشركة؟ كيف سيتم استخدام هذه المعلومات لجني الأموال؟ هل سيبيعون المعلومات الشخصية عن حسابات مستخدميهم؟

وكما شاهدنا، إن مستخدمي شبكات التواصل الاجتماعي الذين يثبتون برامج التعقب يفصحون عن كثير من الخصوصية وإدارة حساباتهم الشخصية ونشاطهم على الشبكة الإلكترونية. والأسوأ من ذلك، إن العديد من برامج الإعلانات على شبكات التواصل الاجتماعي تخفي برامج إضافة مخفية. يأتي جزء من الأجزاء المبلغ عنها بشكل جيد من برامج الإعلانات من شركة تدعى زانغو Zango، والتي تنتج برامج إضافة مخفية في إضافات

متعـــددة موجـــودة فـــي مواقـــع مثـــل EverythingMyspace، MyspaceGlitters، وLoserAlliance وVideocodelab. كما أنهم ينتجون أيضًا مشغل فيديو YouTubeمزيف. يتم تقديم المستخدمين مع ما يبدو صورة YouTube.



الشكل رقم (١٠-٤): يريد المحتالون كلمة المرور الخاصة بك.

(تم إعادة طباعتها بعد الحصول على تصريح. للحصول على المزيد من المواد، الرجاء زيارة www.SecurityCartoon.com)

جامع الأصدقاء الهائل

هل فكرت يومًا كيف أن صفحة شخص ما على شبكة التواصل الاجتماعي قد تحتوي على ٤٠ أو ٥٠ أو ١٠٠ صديق أو أكثر؟ هل الشخص مشهور فعلا لتلك الدرجة؟ هنالك العديد من البرامج، والمعروفة ببرامج "جامع الأصدقاء الهائل"، التي سوف تضيف العديد من الأشخاص إلى صفحة شبكة التواصل الإجتماعي الخاصة بأي شخص. إلا أن تم إغلاقها بنجاح، كانت FakeYourSpace.com خدمة تضيف صورًا لرجال ونساء رائعين على صفحات MySpace أو Facebook. مقابل رسوم شهرية، يمكن أن يجعلها المستخدمين تبدو كأنه لديهم الكثير من الأصدقاء الجيدين يعلقون على الجدار الخاص بهم.

عند النقر عليها، يطلب منهم السماح لمشغل الفيديو لتنزيل وتثبيته بحيث يمكنهم مشاهدة الفيديو. يقوم البرنامج بتثبيت الكثير من برامج الإعلانات من Zango. التمرين ١٠–١ – برامج الإعلانات والخصوصية يتوجب عليه رفع وعي الطلاب حول مخاطر برامج الإعلانات وانتهاكها للخصوصية.

يلاقي النصابون نجاحًا كبيرًا في استهداف مواقع شبكات التواصل الإجتماعي. ولمعرفة السبب، يمكن للطلاب زيارة الرابط التالي لـ Washington Post لقراءة مقال رائع

بعنوان "Phish-Hooked Thieves Find Easy Pickings on Social Sites"، بقلم كيم هارت Kim Hart، كاتب ضمن فريق العمل في واشنطن بوست Washington Post، في حزيران/يوليو ٢٠٠٦م (www.washingtonpost.com/wp-dyn/content/article/2006/07/15/AR2006071500119.html).

إن شبكات التواصل الاجتماعي، مثل غيرها من المواقع الإلكترونية المشروعة، لا يمكن لومها على عمليات الإحتيال التي تستهدف مستخدمي الشبكات. إن هذه العمليات هي تماما خارج سيطرتهم في العادة، وعندما يعرفون عنها، فإنهم يبذلون كل ما بوسعهم لإيقافها. لكن تستمر عمليات الاحتيال والنصب في جميع الأوقات وتتخذ كل شكل يمكن تخيله. يحتاج طلابك إلى إدراك الأشكال التي تتخذها عمليات النصب بحيث لا يتم خداعهم. التمرين ١٠–٢ – تحقيقات يجعل الطلاب يلقون نظرة ثاقبة على شبكات التواصل الإجتماعي على الشبكة الإلكترونية وبعض من المخاطر مثل برامج التجسس الخبيثة والبرامج الضارة التي يتم نقلها عبر هذه الشبكة.

يدعو المراهقون إلى دائرة "أصدقائهم" حوالي ٨٧% من الغرباء الذين يطرقون الباب الأمامي لمواقع شبكات التواصل الاجتماعي الخاصة بهم (McCarthy, 2007).

عمليات النصب والإحتيال

من السهل جدًّا على كل واحد، وحتى البالغين، الوقوع في عمليات النصب والاحتيال. يجب أن تتم توعية الطلاب بعمليات النصب والإحتيال في سن مبكرة.

يحتوي الموقع الإلكتروني Stop-Phishing.com (www.indian.edu/~phishing/) مصادر ممتازة، بما في ذلك رسوم كرتونية تتعلق بالعديد من المواضيع في هذا الكتاب. قم باتباع رابط Protect Your Family إلى صفحة Reducing Risk of Phishing Page، والتي تعلمك كيفية تمييز محاولات النصب. إن اختبار معدل الذكاء للنصب في SonicWALL (www.sonicwall.com/phishing/) بناء جدًّا. ننصح بأن تقوم بخوض الاختبار بنفسك قبل أن يقوم به الطلاب ومراجعة الإجابات غير الصحيحة لفهم كيفية تمييز مواقع النصب والاحتيال. إن عينات الرسائل الإلكترونية الخاصة بعمليات النصب والصفحات الإلكترونية بناءة جدًّا. التمرين ١٠–٣– مقدمة على عمليات النصب يجعل الطلاب يتعودون على المصطلح واختبار قدراتهم لتحديد مواقع النصب والإحتيال.

بالإضافة إلى اختبار SonicWALL، يحتوي PhishTank (www.phishtank.com) على قاعدة بيانات لمحاولات النصب المشتبه بها. يمكنك نسخ العناوين العامة للموقع على الشبكة الإلكترونية وزيارة أحدث مواقع النصب والاحتيال المشتبه بها، بالإضافة إلى مشاهدة لقطات شاشة للمواقع المؤرشفة. كما يمتلك Consumer Direct، وهو موقع حكومي في المملكة المتحدة لديه ذاكرة ألعاب لاختبار قدراتكم على اكتشاف الرسائل غير المرغوبة

وعمليات النصب والاحتيال، وكذلك قائمة بالموارد لاكتشاف عمليات الاحتيال. الرجاء زيارة:

- www.consumerdirect.gov.uk/watch_out/scams/dont-get-trapped/
- www.consumerdirect.gov.uk/watch_out/games/

الشكل رقم (١٠-٥): الاحتيال والنصب

ضمن الجهود لاستباق تطبيق القانون، إن متوسط عمر مواقع النصب والإحتيال هو يومين فقط. وهي تظهر في العادة لعدة ساعات إلى عدة أيام قبل أن ينقلها ويضع مواقع جديدة في موقع آخر.

قامت FraudWatch International (www.fraudwatchinternational.com) مؤخرًا بإقرار مواقع للنصب والاحتيال وأوصاف لطرق النصب والاحتيال وكيفية تجنبها. الرجاء النقر على Fraud Info على شريط البحث. التمرين ١٠ – ٤ – مراجعة الوسائط الإعلامية المقروءة والمكتوبة يسمح للطلاب ببحث عمليات النصب والاحتيال الحالية ومشاركة نتائجهم مع نظرائهم.

تتيح بعض الأعمال الهجومية للنصب والاحتيال على شبكات التواصل الإجتماعي للمحتالين خداع المراهقين لتثبيت برنامج على حاسوب العائلة، عبارة عن حصان طروادة Trojan horses الذي يحتوي على مسجل المفاتيح. سوف يسجل مسجل البيانات هويات تسجيل الدخول وكلمات المرور وإرسالها إلى المحتالين. كما يبحث المحتالون عن أسماء وتواريخ ميلاد المراهقين لأنها مستخدمة بشكل شائع ككلمات مرور من قبل آبائهم. التمرين

١٠ – ٥ –حصان طروادة Trojan Horses يساعد الطلاب تحديد شروط واستخدام حصان طروادة Trojan horses.

وهنالك نوع من آخر شائع من الخدع يتعلق برسائل إلكترونية معينة، ملصقات المدونة، والملصقات على مواقع شبكات التواصل الاجتماعية التي توصي بمنتج أو موقع إلكتروني. يبدو أن هذه الملصقات تأتي من أصدقاء الطالب. حاول موقع احتيال توجيه المراهقين لشراء موسيقى من موقع إلكتروني الذي يقوم ببساطة بجمع معلومات بطاقات الائتمان الخاصة بوالديهم وبالمقابل لا يبيعونهم أية موسيقى على الإطلاق. قم بإخبار طلابك أنه إذا بدا أن صديقًا يوصي بمنتج أو موقع إلكتروني، الشراء على مسؤولية المشتري وتحذير المشتري بفحص السلعة – دع المشتري يتوخى الحذر!

الشكل رقم (٦-١٠): المزيد عن كلمات المرور

في شهر كانون الثاني/ يناير ٢٠٠٧م، حددت MessageLabs (www.messagelabs.com)، الشركة الرائدة في مجال السلامة على الشبكة الإلكترونية، أن عدد الرسائل الإلكترونية للاحتيال والنصب أكثر من عدد الرسائل الإلكترونية للفيروسات. وبالمتوسط، خلال الستة شهور الأولى لعام ٢٠٠٧م، واحد من كل ٢٢٨ رسالة الكترونية كانت عبارة عن اعتداء احتيال. إن كل من Paypal.com و Ebay.com هما أكثر المواقع الإلكترونية المستهدفة.

محادثة مع محتال

ما يلي هو عبارة عن مقتطف من ملصق يتضمن مقابلة بين روبرت هانسين Robert Hansen، المدير التنفيذي لـ SecTheory، شركة للسلامة على الإنترنت، وليثيوم Lithium شاب ومخادع ناجح. وافق ليثيوم على إجراء المقابلة بشرط أن تبقى هويته غير

مكشوفة. تم إجراء هذه المقابلة على الشبكة الإلكترونية في بداية شهر مايو/ أيار من عام ٢٠٠٧م وتم وضعها على الموقع الإلكتروني ha.ckers.org (http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/).

روبرت هانسين : حسنًا، لقد استمتعت كثيرًا بهذا الملصق. لا توجد أخبار جديدة هنا، ولكنني تمكنت من التحدث مع أحد كان يرغب في الجلوس وكتابة بعض الأفكار من منظور مخادع. يستخدم المخادع اسم ليثيوم Lithium ووافق على الإجابة عن عدد من الأسئلة التي كانت تدور في ذهني لمدة من الزمن. أشكره شكرًا جزيلاً، اعتقد أن الكثير من هذه المعلومات هي معلومات قيمة للمجتمع بشكل كبير. وهي كلماته الخاصة – بدون أي تغيير:

روبرت هانسين : كيف تصف نفسك؟ العمر؟ هل تذهب للمدرسة؟ ما اهتماماتك؟

ليثيوم: مصمِّم هي أفضل كلمة لوصف نفسي. أبلغ من العمر ١٨ عامًا. نعم، ذهبت إلى المدرسة. تركت الدراسة بعد المدرسة الثانوية. هواياتي هي فنون الدفاع عن النفس المتنوعة؛ اللياقة البدنية وأخيرًا... الشبكة الإلكترونية.

روبرت هانسين : كيف بدأت في عمليات الاحتيال؟ كيف بدأت اهتمامك فيها؟

ليثيوم: إن بريد الاحتيال التقليدي الذي استمرت عائلتي بتلقيه في صندوق الوارد. كانت رسائل ذات تركيبة ضعيفة جدًّا! ومع ذلك كانوا يعملون بشكل عام. لذا علمت تلقائيًّا أنه يمكنني ابتكار طرق أكثر فاعلية وأحصل على مردود أكبر.

روبرت هانسين: كم المدة الزمنية التي ما زلت تمارس عمليات الاحتيال فيها؟

ليثيوم أنا أمارس عمليات الاحتيال منذ عمر الرابعة عشرة. أي منذ حوالي خمس سنوات.

روبرت هانسين: هل لديك أية فكرة عن عدد الأشخاص الذين سرقن هويتهم حتى الآن؟

ليثيوم: ما يفوق ٢٠ مليون شخص. إن دودة شبكات التواصل الاجتماعي أثرت على أعمالي بالفعل! مازال لدي عدة مئات من آلاف الحسابات على العديد من المواقع الإلكترونية التي لم أحظ بفرصة إلى الآن للنظر خلالها.

روبرت هانسين: هل احتجت إلى تزوير أية علاقات معينة مع أشخاص آخرين ومجموعات للبدء.

ليثيوم : لا، عندما بدأت كنت وحدي. جاء الكثير من المجموعات لتسألني إن كنت أرغب، رفضت.

روبرت هانسين: ما أنواع المواقع التي تعد أفضل مواقع للنصب والإحتيال.

ليثيوم: مواقع شبكات التواصل الاجتماعي، إن أي موقع يتعلق بالمراهقين تبدأ من عمر ١٤ عامًا وأكثر.

روبرت هانسين: كم عدد الأشخاص الذين احتلت عليهم في كل موقع أعلنت فيه؟

ليثيوم: إن ذلك يعتمد على حجم الموقع الإلكتروني (حجم المستخدمين). في العادة، احتال على ٣٠ طفلاً في اليوم.

روبرت هانسين : كيف تقوم بتحويل المال من الهويات وكم من المال يوفر لك؟

ليثيوم: أقوم بتحصيل من مواقع التواصل الإجتماعي ٥٠٠ دولار أمريكي من خلال صفقات الإعلانات المدعوة CPA والتي تعني (نقرة واحدة لكل إعلان).

وتنجح بمعدل خمس مرات من كل عشرة مرات يقوم فيها الشخص باستخدام نفس كلمة المرور لحساب البريد الإلكتروني الخاص به. والآن يعتمد الأمر على ما يحتويه صندوق الوارد في البريد الإلكتروني حيث يحدد مبلغ الربح الذي أحصل عليه. إذا كان حساب البريد الإلكتروني يحتوي على حسابات لكل من ebay/ rapidshare/ egold/ paypal، وحتى حساب البريد الإلكتروني بحد ذاته، أقوم ببيعها إلى المحتالين. أقوم بتحصيل من ٣ إلى ٤ آلاف في اليوم. لا أقوم بممارسة الاحتيال إلا ٣ – ٤ أيام في الأسبوع. يعتمد الأمر على مقدار الوقت الذي استثمره في ذلك، كلما استثمرت وقتا أطول، كلما زادت العائدات.

روبرت هانسين: هل هنالك أية ضوابط لمكافحة عمليات الاحتيال (أدوات أو تقنيات) والتي تجعل الحياة كمحتال على الشبكة الإلكترونية أصعب.

ليثيوم: نعم بالطبع، هنالك العديد من الأمور التي تجعل الاحتيال أصعب. لكن منذ أن قام كل من متصفح الإنترنت Internet Explorer ٧ وفايرفوكس Firefox بتطبيق الحماية ضد الإحتيال، فإنهما السببان الرئيسيان الأكثر إزعاجا.

الحد من مخاطر تعرض طلبتك لعملية نصب

كيف يستطيع طلابك تقليل مخاطرهم في التعرض لعملية نصب على الشبكة الإلكترونية؟

فيما يلي بعض النصائح المفيدة.

يجب أن يشتري الطلاب من مواقع موثوقة.

يجب أن يشتري الطلاب منتجات الشبكة الإلكترونية من مواقع موثوقة ومعروفة، أو مواقع لديها أيضًا واجهات تجارية ملموسة "تجارة تقليدية". وعندما يشكون بالأمر، يجب أن يسأل الطلاب الأسئلة التالية:

١. هل يضع الموقع عنوان بريدي كامل؟
٢. هل البحث الموجه عن "من هو" (انظر: التمرين ٩-٨) في الفصل التاسع) يطابق اسم الموقع أو الملكية المعلنة؟
٣. ما الروابط التي تظهر في محرك البحث عندما تقوم بإدخال اسم الموقع أو العمل؟ هل تشير أي من الروابط إلى عمليات نصب أو شكاوي حالية من عميل مستاء؟

يجب أن يتفقد الطلاب بروتوكول نقل النصوص المترابطة

هل لاحظت يوما أن شريط العنوان في متصفح الشبكة الإلكترونية يبدأ في العادة بعنوان الكتروني بـ "http://"؟. إن المختصر http يرجع إلى بروتوكول نقل النصوص المترابطة ويسر إلى مجموعة من القواعد (البروتوكولات) بين أجهزة الحاسوب عبر

الشبكة الإلكترونية لنقل المعلومات. إن أية معلومات منقولة عبر الشبكة الإلكترونية عبر http مرئي بشكل كامل إلى كل جهاز يعبر من خلالها. يمكن اقتباس المعلومات بسهولة ونسخها ومشاهدتها من قبل الآخرين.

إذا كنت ترغب في إرسال المعلومات بشكل خاص من خلال موقع إلكتروني، إن استخدامhttp فيه مخاطرة كبيرة. قم بإخبار طلابك أنه من السياسة الجديدة عدم إرسال معلومات خاصة – كلمات مرور، معلومات البطاقة الائتمانية، أرقام الضمان الاجتماعي.. إلخ – من خلال موقع يبدأ عنوانه الإلكتروني بـ http. أخبرهم أنه في أي وقت يرغبون فيه في إرسال معلومات خاصة غير موقع إلكتروني، يجب أن يتأكدوا أن شريط العنوان لمتصفح الشبكة الإلكترونية الخاص بهم يبدأ بـ https://. إن الحرف "s" في https يستخدم بروتوكول الأمن كلا من التشفير والتصديق لمنع أي شخص من مشاهدة المعلومات الخاصة بينما تتنقل بين المستخدم أو العميل أو وجهته.

في بعض الأحيان إن https مضمنة في الصفحة الإلكترونية وهي ليست واضحة على الفور. اطلب من الطلاب النظر إلى الشكل رقم (١٠-٧):

يبدو أنه يطلب من المستخدم تسجيل الدخول من وصلة http. ومع ذلك، إذا نقر أحد على زر تسجيل الدخول بدون إدخال أية معلومات، يتغير العنوان على الفور إلى https (انظر الشكل رقم ١٠-٨)، والذي يوضح أن تسجيل الدخول الفعلي يكون عبر https.

الشكل رقم (١٠-٧)

الشكل رقم (١٠-٨)

الشكل رقم (١٠-٩)

الشكل رقم (١٠-١٠)

علاوة على ذلك، متى أراد الطلاب القيام بعملية آمنة أو اتصال على الشبكة الإلكترونية عبر https، سوف يبين متصفح الشبكة الإلكترونية رمز القفل في الزاوية اليمنى السفلية للنافذة. يحاول بعض المحتالين خداع الزوار من خلال وضع رمز الإغلاق على الصفحة الإلكترونية الفعلية بدلا من زاوية متصفح الشبكة الإلكترونية. إن قفل الفيسبوك موضح في الشكل رقم (١٠-٩)، وقفل Amazon.com موضح في الشكل رقم (١٠-١٠).

يجب ألا يقوم الطلاب ابدًا بتسجيل الدخول إلى، أو الشراء من موقع إلكتروني إن لم يشاهدوا بروتوكول http في شريط العنوان ورمز القفل في الزاوية اليمنى السفلية لمتصفح الشبكة الإلكترونية.

يجب أن يستخدم الطلاب قوة ملاحظتهم

إن PayPal هو مصرف على الشبكة الإلكترونية وخدمة الدفع. تم خداع العديد من مستخدمي PayPal للإفصاح عن معلومات تسجيل الدخول إلى حسابهم وكلمات المرور بعد استلام رسالة الكترونية للاحتيال والتي تبدو أنها قادمة من PayPal. إن الرابط المخفي يوجههم لتسجيل الدخول إلى صفحة إلكترونية تشبهها تماما تقع على الموقع الإلكتروني www.paypai.com. كان الرابط لموقع إلكتروني استبدل حرف l بـ i في PayPal. يجب أن

يمعن الطلاب النظر ليتاكدوا من أنهم متواجدون على الموقع الإلكتروني الذي يعتقدون أنهم عليه، وبخاصة إذا كانوا يتبعون رابط من بريد إلكتروني .

يجب ألا يسجل الطلاب الدخول ابدًا على مواقع إلكترونية بعد النقر على روابط تظهر في الرسائل الإلكترونية أو الرسائل الفورية.

من السهل إخفاء أو تمويه الروابط الموجودة في الرسائل الإلكترونية. إن العنوان العام للموقع على الشبكة الإلكترونية الذي يظهر في الرابط ضمن الرسالة الإلكترونية لا يجب أن يطابق العنوان العام للموقع على الشبكة الإلكترونية الذي يتم الوصول إليه عند النقر على الرابط. قم بتعليم طلابك ألا يتبعوا الروابط في الرسائل الإلكترونية والرسائل الفورية. بدلاً عن ذلك، قم بإرشادهم للتأشير على العناوين الموثوق بها لحساباتهم، أو طباعة العناوين يدويًا.

يجب أن يتحقق الطلاب قبل تثبيت برنامج "مجاني"

هل يرغب طلابك بتثبيت لعبة رائعة، أو إضافة أو أداة؟ هل هي "مجانية"؟ اطلب منهم استخدام محرك البحث لمعرفة اسم اللعبة أو الإضافة. اطلب منهم أيضًا البحث عن الاسم مصحوبًا بكلمات مثل إضافة برنامج أو برنامج ضار. هل ذلك البرنامج الذي على وشك أن يقوم الطلاب بتثبيته في الواقع برنامج إضافة أو برنامج تجسس أو برنامج ضار؟

يجب أن يفكر طلابك بعناية شديدة قبل إدخال المعلومات الشخصية في أي مكان على الشبكة الإلكترونية

إن المعلومات الشخصية قيمة جدًّا لأولئك الذين يستطيعون استخدامها لسرقة هوية الطلاب أو التلاعب بهم. يجب أن يحمي الطلاب معلوماتهم الشخصية بعناية!

قم بتعليم طلابك الحكمة التالية " إذا كان يبدو جيدًا جدًّا ليكون حقيقيًا، فهو على الأرجح احتيال!"

يجب أن يتعلم الطلاب أن يكونوا على حذر جدًّا على الشبكة الإلكترونية. إن معظم المحتالين ناجحين جدًّا لأنهم يكتسبون بسهولة ثقة ضحاياهم.

يجب أن يقوم الطلاب دائما بحذف الرسائل الإلكترونية التي تصلهم من غرباء ويجب ألا ينقروا أبدا على مرفقات الرسالة الإلكترونية أو الرسالة الفورية.

إذا لم يتعرف طلابك على مرسل الرسالة الإلكترونية، قم بتعليمهم حذفها بدون فتحها؛ ومن ثم يجب أن يحظروا المرسل إن كان على التراسل الفوري. إن الوقت الوحيد الذي يعد النقر مرفقًا على رسالة إلكترونية أو على التراسل الفوري آمنا إذا كانوا يعرفون المرسل ويتوقعون أن يرسل شيئًا.

يجب ألا يسمح الطلاب ابدًا للغرباء الاتصال بهم على الشبكة الإلكترونية.

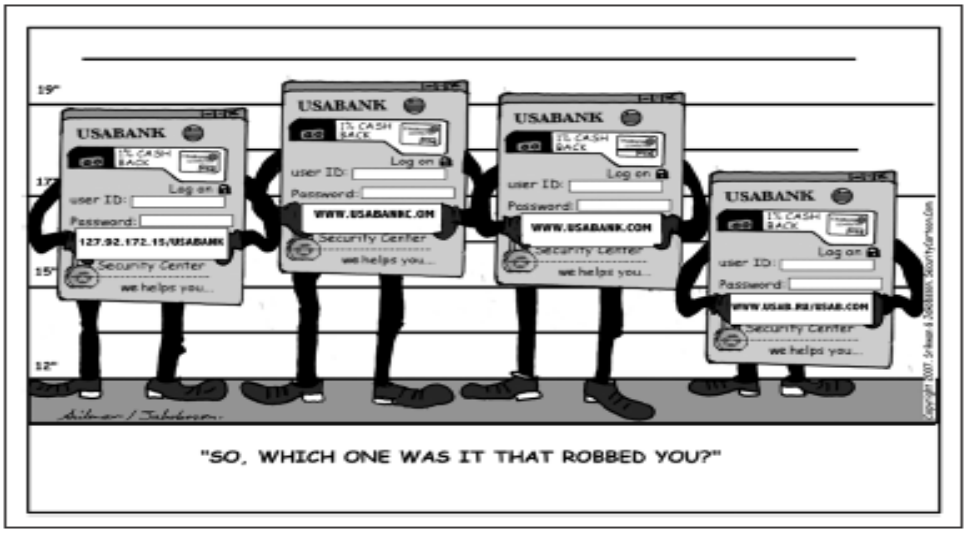
يستطيع أي أحد إخبارك بأي شيء يريده على الشبكة الإلكترونية، ولكن ذلك لا يجعله صحيحًا. يجب أن يجعلها الطلاب قاعدة شخصية ألا يصبحوا أصدقاء مع أشخاص

لا يعرفونهم. وأخبر طلابك أيضًا ألا يثقوا بحكم أصدقائهم. قد لا يعرف أصدقائهم الشخص أيضًا.

يجب أن يتعلم الطلاب تثبيت برنامج موثوق ويمكن الإعتماد عليه في مكافحة الفيروسات ومكافحة التجسس وجدار ناري للحماية.

إن يقوم كل شخص يمتلك جهاز حاسوب يشغل نظام تشغيل ويندوز Windows أن يثبت برنامج لمكافحة الفيروسات ومكافحة التجسس وجدار ناري للحماية، والمحافظة على تحديثها كلها. على الرغم من أن الفيروسات التي تؤثر في الحواسيب الشخصية لا تجتاح مستخدمي ماكنتوش Mac، يمكن أن يمرر مستخدمو أجهزة ماكنتوش فيروسات إلى مالكي الحاسوب الشخصي وبناءً عليه يجب عليهم التفكير في تثبيت برنامج مكافحة الفيروسات على حواسيبهم.

يقدم الموقع الإلكتروني PCWorld.com العديد من الإستعراضات حول برامج مكافحة التجسس أو مكافحة الفيروسات والأمن (www.pcworld.com/tc/spyware/).



الشكل رقم (١٠-١): صف هجوم المحتال

إن موقع Spywarewarrior.com مصدر رائع لاستخدامه للتعلم عن أفضل أدوات مكافحة التجسس. يوجد ثلاثة جدران نارية معروفة جدا لأجهزة الحاسوب الشخصية وهي كومودو فيروول برو Comodo Firewall Pro، وزون ألارم Zone Alarm، ونورتون بيرسونال فيروول Norton's Personal Firewall. إذا جاء الحاسوب الشخصي الخاص بكم بجدار ناري مثبت فيه عند التصنيع، فعليك التأكد من أنه فعال. يوفر الموقع الإلكتروني OnGuardOnline.gov مقاطع فيديوتوضح كيفية تفعيل جدار ناري مثبت عند التصنيع في كل من أجهزة ماكنتوش Macs وأجهزة ويندوز اكس بي XP (SP2) Windows

(http://onguardonline.gov/tutorials/). وما أن تدخل على الموقع الإلكتروني، انقر على الرابط المناسب للأمن/ الأدوات.

يجب أن يحافظ الطلاب على برامجهم ونظام التشغيل لديهم محدث بشكل دائم

يكتشف مطورو البرامج بشكل مستمر مشاكل جديدة في الأمن، ويقومون بشكل منتظم بإصدار التحديثات، ورقعات، وإصلاحات. يجب أن يتفقد الطلاب بشكل دائم التحديثات لنظام التشغيل وبرامج حاسوبهم.

يجب أن يتعلم الطلاب كيفية زيادة إعدادات الأمن لمتصفح الشبكة الإلكترونية الخاص بهم

يجب أن تدرس طلابك كيفية تحديد إعدادات الأمن في متصفحهم. لا تقدم كافة متصفحات الشبكة الإلكترونية نفس إجراءات الأمن. إن كشاف الشبكة الإلكترونية هو في الوقت الحالي أكثر متصفح مستهدف من قبل المتسللين إلى أجهزة الحاسوب.

يعتبر موزيللا فيرفوكس Mozilla's Firefox من أكثرها أمانًا، ولكن لا يعد أي منها نموذجيًّا. يجب أن يتحقق الطلاب من أكثر نسخة محدثة لمتصفح الشبكة الإلكترونية.

إن كان لأي من طلابك شبكة الكترونية لاسلكية في المنزل، أخبرهم بتفعيل مميزات الأمن للجهاز اللاسلكي، وبخاصة حماية كلمة المرور. سوف يستخدم الآخرين ويستغلون الشبكة الإلكترونية اللاسلكية غير المحمية.

هل أنت ضحية محتال؟

غذاء لأفكار الطلاب

بقلم: ماركوس جاكوبسون Markus Jakobsson وسوكامول سريكوان Sukamol Srikwan

يفترض العديد من الأشخاص أن أي موقع إلكتروني يشبه موقع البنك الخاص بهم و eBay و PayPal.. إلخ، هو بالفعل كما يبدو. ليست هذه هي القضية. إنها عبارة عن أدوات تلقائية، مثل: "WebWhacker"، تلك مواقع إلكترونية مستنسخة. يستخدم المحتالون أدوات كهذه لابتكار نسخ مثيلة لمواقع معروفة جدًّا. عندما تزور موقع، ما الذي يجب أن تبحث عنه لتتأكد أنها حقيقية؟

- هل تتأكد من أن جميع الإشعارات والرموز تبدو صحيحة؟ إن هذه ليست طريقة آمنة. من السهل جدًّا نسخ الشعارات والرموز.
- هل تتحقق من عدم وجود أخطاء في التهجئة؟ فأنت قد تكون بمأمن من المحتالين الذين لا يستطيعون التهجئة، لكن الكثير من المحتالين يعرفون كيفية التهجئة أو لديهم برامج للتحقق من التهجئة!
- هل تبحث عن قفل للتأكد من أن الموقع محمي؟ تذكر، ليس من الصعب أن تتضمن صورة لقفل صفحة إلكترونية أكثر من أي صورة أخرى! يجب أن يكون القفل في المكان الصحيح ليتم أخذه بعين الاعتبار، ويعتمد مكان وجوده على أي نوع من المتصفح لديك.

إذا كان العنوان الإلكتروني (URL) يبدو حقيقيا، هل ذلك يعني أنه حقيقي؟ هل www.citibank-high-security.com ينتمي لسيتي بنك CitiBank؟ هل www.ebay.account-protector.com ينتمي إلى eBay؟ إن الحقيقة هي أن أي أحد على معرفة بتقنية كيفية تسجيل عنوان إلكتروني مثل ذلك، لذا كن حذرًا. عندما ترى عنوان إلكتروني، كيف تتأكد من أنه حقيقي؟ إحدى الطرق الجيدة هي زيارة www.whois.net وإدخال

العنوان الإلكتروني حول ذلك. تستطيع معرفة من يمتلك العنوان العام للموقع الإلكتروني،وإن ذلك في العادة مفيد جدا لتمييز إن كان حقيقي أم لا.

هل تعمل ما بوسعك لتعلم كيفية البقاء آمنا أو هل تعتبرها وظيفة شخص آخر؟ هل تعتقد أن "بنكي سوف يحميني،"أو "سوف يحجب مزود خدمة الشبكة الإلكترونية الخاص بي المواقع السيئة،"أو "سوف تتعقب الحكومة المحتالين وسجنهم"؟ إن البنوك لدينا والحكومة تبذل أقصى ما بوسعها لحمايتنا، ولكن يجب أن نتحمل كامل المسؤولية عن أماننا الخاص، أيضًا.

التمارين

التمرين (١٠-١):
برامج الإعلانات والخصوصية

إن الهدف من هذا التمرين هو توليد نقاش حول فكرة الحق في الخصوصية أو ماذا يعني اجتياح الخصوصية. يجب أن يركز النقاش أيضًا على حقيقة أن برنامج الإضافة يتلاعب بمصادر حاسوب المستخدم لاستهداف المستخدم بالإعلانات. تم تخريب جهاز حاسوبه لمساعدة مرسل الرسائل غير المرغوبة، وفي العادة بدون معرفة المستخدم أو إذنه.

ما برنامج الإعلانات بالضبط؟ قم بالطلب من الطلاب ما يلي:

١. قم بزيارة محرك البحث Google وأكتب فيه مايلي: تعريف برامج الإعلانات.
٢. قم بقراءة التعريفات العشرة الرئيسة؟
٣. قم بإعداد قائمة، بناء على هذه التعريفات، بالأشياءالتي يفعلها برنامج الإعلانات والتي لا يحبونها أو لا يرغبون في حدوثها لهم؛
٤. قم بمقارنة قائمتهم بقوائم الأشخاص الأخرى لترى إن كانوا يتشاركون في اهتمامات مشاركة؛ و
٥. تحديد سبب عدم محبتهم لبعض الأشياء التي يمكن أن يفعلها برنامج الإعلانات.

التمرين (١٠-٢):
تحقيقات

هل يستطيع أي موقع للتواصل الاجتماعي حماية طلابك من عمليات الاحتيال والنصب على الشبكة الإلكترونية؟ يجب أن تكون الإجابة واضحة: لا، وحتى الفيسبوك لا يستطيع والذي كان يعتقد ولمدة طويلة أنه أكثر موقع للتواصل الاجتماعي أمانًا، والذي يستطيع حماية المستخدمين بشكل كامل. في يوليو/ تموز عام ٢٠٠٧م، سمح الفيسبوك لمعلن بوضع إعلانات لخدمة مواعدة. سبب النقر تحذيرًا ليظهر أنه تم اكتشاف برنامج تجسس على حاسوب المستخدم. كما تم إبلاغ المستخدم أيضًا أنه يستطيع تنزيل برنامج ما لإزالة برنامج التجسس. ما الخطأ في هذا الحوار؟ اطلب من الطلاب القيام بما يلي:

١. الذهاب إلى محرك البحث، بين قوسين، وثم قم بإدخال الكلمات "البرمجيات الخبيثة"؛
٢. النظر عبر الروابط واختيار واحد أو اثنين للتحقق منهما؛ قد لا تكون جميع الروابط متعلقة بهذا البرنامج، لذا عليكم الإختيار بعناية (انظروا : ملاحظات المعلم أدناه)؛ و
٣. تحديد ما هو عملية الاحتيال بإنذار البرمجية الخبيثة.

ملاحظات المعلم

قد لا تكون جميع الروابط متعلقة ببرنامج الاحتيال المعروف بإنذار البرمجية الخبيثة، لذا قد تحتاج إلى مساعدة طلابك على تحديد أفضل الروابط. ومن أفضل الروابط الرابطين التاليين:

- The Register– الفيسبوك يقدم إعلانات لبرنامج أمن احتيالي (www.theregister.co.uk/2007/07/11/facebook_serves_crudware_ads/)
- Spacequad AntiSpam Services_ماسح ضوئي لبرنامج التجسس إنذار البرمجية الخبيثة (www.spacequad.com/article.php/MalwareAlarm)

التمرين (١٠-٣):
مقدمة إلى عمليات النصب

قم بالذهاب إلى www.Stop-Phishing.com (مجموعة مكافحة عمليات النصب The Anti-Phishing Group في جامعة إنديانا Indiana University).

هل يعتقد طلابك أنهم أذكياء لدرجة كافية لتمييز الموقع المرخص من موقع الإحتيال؟ اطلب منهم القيام باختبار مستوى الذكاء للإحتيال من سونيك وول SonicWALL Phishing IQ Test (www.sonicwall.com/phishing/).

ما معدل نجاحهم؟ هل أبلى طلابك بلاءً حسنًا؟

قم بتشجيعهم على جعل والديهم القيام باختبار الاحتيال لمشاهدة كيف يبلون فيه!

التمرين (١٠-٤):

مراجعة الوسائط الإعلامية المقروءة والمكتوبة

قم بتحديد المقالات أدناه إلى مجموعات من الطلاب لنقاشها، واطلب منهم تقديم ملخص لها لبقية الصف.

- "False 'Friends' Prey on Social Networking Sites,"
بقلم بوب كوفي Bob Kofee
(Cox News Service; February 25, 2007)
www.coxwashington.com/hp/content/reporters/stories/2007/02/25/BC_SOCIAL_SPAM_ADV25_COX.html

- "MySpace Phishing Scam targets Music Fans,"
بقلم جون لايدن john Leyden
(The Register, October 14, 2006)
www.theregister.co.uk/2006/10/14/myspace_phishing_scam/

- "Facebook 'Ideal for Phishing attacks: Researcher"
(CBC News, April 14, 2007)
www.cbc.ca/technology/story/2007/04/13/tech-facebookphishing-20070413.html

- "Attack of the Facebook Snatchers,"
بقلم نيك سوليفان Nick Sullivan
(Symantec.com; April 13, 2007)
https://forums.symantec.com/syment/blog/article?message.uid=306060

التمرين (١٠-٥):
أحصنة طروادة Trojan Horses

قم بالطلب من طلابك ما يلي:

١. زيارة Google.com؛
٢. إدخال تعريف: Trojan Horses في حقل البحث .
٣. قراءة بعض التعريفات الأولى.

قم بسؤال طلابك عن سبب تسمية البرنامج Trojan horse.

اطلب منهم تذكر مادة التاريخ الإغريقي.

المصادر

Cashmore, P. (2006, July 10). *MySpace codes bring adware payload.*
متوفر في الموقع الإلكتروني لـ Mashable:
http://mashable.com/2006/07/10/myspace-codes-bring-adware-payload/

Cashmore, P. (2006, November 8). *Fake YouTube scam hits 1,400 MySpace pages.*
متوفر في الموقع الإلكتروني لـ Mashable:
http://mashable.com/2006/11/08/fake-youtube-scam-hits-1400-myspace-pages/

Clayton, D. (2006, November 30). *FakeYourSpace: How losers become popular*.
متوفر في الموقع الإلكتروني لـ Blog Herald:
www.blogherald.com/2006/11/30/fakeyourspace-how-losers-become-popular/

landesman, M. (2007, March 26). *Stalker tracker scam targets MySpace.*
متوفر في الموقع الإلكتروني لـ About.com
http://antivirus.about.com/b/a/257837.htm

McCarthy, C. (2007). *Facebook users pretty willing to add strangers as 'friends.'*
متوفر في الموقع الإلكتروني لـ CNET:
http://news.cnet.com/8301-10784_3-9759401-7.html

Mutton, P. (2006, October 27). *MySpace accounts compromised by phishers.*
متوفر في الموقع الإلكتروني لـ Netcraft:
http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html

الموقع الإلكتروني OnGuard Online: http://onguardonline.gov
إن هذا الموقع " يوفر نصائح عملية من الحكومة الإتحادية وصناعة التكنولوجيا لمساعدتك لتكون محمي ضد التزوير على الشبكة الإلكترونية، وتأمين حاسوبك، وحماية معلوماتك الشخصية." كما يضع هذا الموقع الحكومي عدة اختبارات على مواضيع مثل سرقة الهوية، والإحتيال وعمليات النصب على الشبكة الإلكترونية على http://onguardonlin.gov/quiz/

Scams. (n.d.)
متوفر في الموقع الإلكتروني لـ Office of Fair Trading:
www.oft.gov.uk/oft_at_work/consumer_initiatives/scams/
يعطي هذا الموقع الخط الرسمي حول ما يجب فعله إن أصبحت ضحية لتزوير الإنترنت ويوفر نصيحة جيدة حول كيفية اكتشاف عمليات النصب والتزوير.
كما أنه يقدم ألعابا فلاشية سريعة عن التحقق من الرسائل غير المرغوبة وعمليات النصب والخداع، على www.oft.gov.uk/oft_at_work/consumer_initiatives/scams/scam-flash

الموقع الإلكتروني لـ Stop-Phishing.com:

www.indiana.edu/~phishing

إن مجموعة البحث ضد الإحتيال Anti-phishing research group في جامعة إنديانا Indiana University تصف هدفها بأنه " المكافحة لفهم التزوير على الشبكة الإلكترونية والتحقق منه وتجنبه، وبشكل خاص، تقليل قابلية البقاء الإقتصادي لهجومات الإحتيال والنصب."

الفصل الحادي عشر

وضع قواعد منزلية لسلامة الإنترنت
Establishing Home Rules for Internet Safety

شجع الأطفال والآباء على إجراء حوار حول الحياة على الشبكة الإلكترونية.

مسألة تسوية A Matter of Compromise

إذا سألت أي من الآباء حول استخدام أطفالهم للشبكة الإلكترونية، فإنهم على الأرجح سيخبروك أن لديهم اهتمامات حول الدخول لمواد غير ملائمة. كما من المحتمل أن يقولوا أنهم قلقون من التحرش والتسلط.

في الواقع، وفقا لدراسة Pew Internet و American Life Project نشرت في ٢٠٠٥، ٦٢% من الآباء و٣٣% من المراهقين أفادوا أن أولياء أمورهم يتفقدون مراهقيهم بعد دخولهم على الشبكة الإلكترونية (Lenhart, Madden & Hiltin, 2005). ويتابع التقرير بالإفادة أن ٨١% من الآباء و٧١% من المراهقين يتفقون على أن الأطفال غير حذرين للدرجة الكافية فيما يتعلق بالمعلومات التي يعطونها على الشبكة الإلكترونية، وأن ٦٢% من الآباء و٦٢% من المراهقين يتفقون على أن الأطفال يفعلون أمورًا على الشبكة الإلكترونية لا يرغبون في أن يعلم بها آبائهم.

كلما امتلك عدد أكبر من الأطفال هواتفا خلوية بمميزات مثل الرسائل النصية، وخدمة الشبكة الإلكترونية، والكاميرات، فإن الآباء يصبحوا قلقين حول الاستخدام غير الملائم لاستخدام الهاتف الخلوي تماما مثل السلوك غير الملائم على الشبكة الإلكترونية. وفقا لدراسة Ace*Comm Corporation في أغسطس/ آب لعام ٢٠٠٦ م على ١٠٠٠ من الآباء، فإن ٦٦% منهم قلقين من الاستخدام المفرط لأطفالهم للرسائل النصية وميزات الهاتف الخلوي الأخرى بدلاً من التركيز على المدرسة أو الواجبات المنزلية. (Sullivan, 2006)

ومع ذلك، وبشكل إجمالي، يعتقد معظم الآباء أن الشبكة الإلكترونية مصدر إيجابي لأطفالهم لكنهم يعتقدون أن أطفالهم يحتاجون لمعرفة كيفية استخدام الشبكة الإلكترونية (Turow & Nir, 2000).

ما توجده هذه المشاعر لمعظم الآباء هو الكثير من الخلافات حول استخدام أطفالهم للشبكة الإلكترونية. ومن أجل التخفيف من اهتماماتهم، يضع معظم الآباء قواعد في المنزل لاستخدام الشبكة الإلكترونية.

التمرين ١١ – ١ – الشبكة الإلكترونية في المنزل يسأل الطلاب عن سلوكياتهم على الشبكة الإلكترونية والقواعد في منازلهم. يمكن أن يوفر هذا التمرين حجر الأساس

لمناقشة السلامة على الشبكة الإلكترونية والسلوك المناسب ويوفر مقدمة لمحادثة يمكن الاعتماد عليها في التمرين ١١ – ٢ و التمرين ١١ – ٣.

يخبرنا المراهقون ان أكثر أمر يعجبهم في استخدام الشبكة الإلكترونية هو البقاء على اتصال مع أصدقائهم واللعب والوصول إلى جميع أنواع المعلومات سواء كانت جدية أو سخيفة. يحبون حرية اكتشاف كل شيء، من الرياضة إلى الموسيقى والنكت والتسوق.

لذا، قد يكون من الصعب على بعض المراهقين قبول أنه يجب أن تكون هنالك قواعد في المنزل حول ما يتعلق باستخدام الشبكة الإلكترونية. وما يحبط المراهقين أكثر هو على الأرجح أن العديد منهم يشعرون أنهم يعرفون أكثر بكثير من آبائهم فيما يتعلق باستخدام الشبكة الإلكترونية وكيفية تمييز وتجنب المزالق. إذا، كيف يستطيع الأطفال والمراهقون التوصل إلى اتفاق مع آبائهم حول استخدام الشبكة الإلكترونية؟ يوجد أمران مهمان جدًّا يمكن للطلاب القيام بهما لمناقشة الدخول على الشبكة الإلكترونية مع آبائهم بشكل أفضل:

١. التواصل بشكل أفضل مع الآباء

إن معظم مخاوف الآباء هي لسببين، الأول هو لعدم معرفتهم بما يفعله أطفالهم على الشبكة الإلكترونية. والسبب الثاني هو أنهم يقلقون أيضًا حول كيفية تعامل أطفالهم مع المصائد والصعوبات التي يجدونها على الشبكة الإلكترونية، وبخاصة أنهم لا يعرفون ماهية هذه الصعوبات بحد ذاتها. قم بإخبار طلابك بأن التواصل مع آبائهم حول ما يفعلونه على الشبكة الإلكترونية يمكن أن يقطع شوطا طويلا نحو تخفيف مخاوف آبائهم.

٢. إنشاء حدود مقبولة على الشبكة الإلكترونية

ما أن يتم تأسيس التواصل مع الآباء حول النشاطات على الشبكة الإلكترونية، تأتي الخطوة التالية وهي الإتفاق على مجموعة من القواعد، أو الحدود التي ستحكم نشاطات الطلاب على الشبكة الإلكترونية.

التمرين ١١ – ٢ – مسح للآباء يطلب من الطلاب أن يقدموا لآبائهم سلسلة من الأسئلة حول اهتماماتهم بسلامة الطلاب على الشبكة الإلكترونية. قد يساعد هذا التمرين على فتح حوار بين الآباء والأطفال وتطوير فهم مشترك واتفاق حول السلوك على الشبكة الإلكترونية. من المهم أيضًا للطلاب رؤية أن معظم الآباء سوف يكونون أكثر ميولاً للسماح لهم باستخدام الشبكة الإلكترونية إذا كان هنالك المزيد من التواصل معهم حول ما يفعلونه على الشبكة الإلكترونية ويمكنهم توضيح الكفاءات الضرورية لحماية أنفسهم ضد الاستغلال والتزوير.

التمرين ١١ – ٣ – عقد مع الآباء يقدم قصة خلافية بين طالبة في الصف السابع ووالديها الصارمين، والذين يمتلكون آراءً مختلفة حول استخدام الطالبة للشبكة الإلكترونية. يجب أن يساعد هذا التمرين الطلاب على تطوير آليات لحل الخلاف ومهارات التفاوض للوصول إلى عقد حول استخدام الإنترنت يكون مقبولاً أكثر من قبل كل من الوالدين والطالب.

وفي نهاية المطاف، أكثر شيء يريده الآباء لأولادهم المراهقين هو السلامة من الأذى. قم بسؤال الطلاب إن لم يكن ذلك بالضبط ما يريدونه لأنفسهم وأطفالهم المحتملين في المستقبل.

تنقية الشبكة الإلكترونية Web Filtering

إن إحدى أكثر الأدوات القيمة للمساعدة في حماية الطلاب على الشبكة الإلكترونية هو منقي الشبكة الإلكترونية. إن العديد من منتجات تنقية الشبكة الإلكترونية متوافرة على الإنترنت؛ قد تكون مدرستك تستخدم إحداها. وفيما يلي بعض من المنتجات الموصى بها:

لمستخدمي حواسيب أبل ماكنتوش Apple Mac

- Content Barrier, by Intego (www.intego.com)
- Bumper Car, by Freeverse (http://freeverse.com)
- OS X Leopard، والتي تأتي مع العديد من ضوابط الوالدين القائمة ضمن برنامج التشغيل. وقد تم وصفها في هذه المقالة في MacWorld:
  www.macworld.com/article/61132/2007/11/tco_parentcontrols.html?t=101

لمستخدمي حواسيب ويندوز PC Windows

- Net Nanny (www.netnanny.com)
- Safe Eyes, by InternetSafety.com (www.internetsafety.com)
- CYBERsitter, by Solid Oak Software (http://cybersitter.com/cybdefault.htm)

التمرين ١١ – ٤ – إعدادات الخصوصية في الفيسبوك تكشف مجموعة التواصل الاجتماعي الشائعة واهتمامات الخصوصية التي تؤثر في كافة المستخدمين. يستطيع أن يستخدم المعلمون هذا التمرين لشرح الأمور المتعلقة بالسلامة وأيضًا ليبينوا للطلاب كيفية زيادة إعدادات الخصوصية الشخصية ضمن جهود ابتكار تجربة تواصل اجتماعي أكثر أمانًا.

التمرين ١١ – ٥ – مشروع إعلانات الخدمة العامة PSA Project يتعلق بالسلامة على الإنترنت. يمكن بعد ذلك إلهام الطلبة لابتكار إعلان الخدمة العامة الخاص بهم PSA والذي يمكن استخدامه لتعليم زملائهم في المدرسة.

التمارين

التمرين (١١-١):
الشبكة الإلكترونية في المنزل

قم بسؤال طلابك إن كان لديهم قواعد في البيت لاستخدام الشبكة الإلكترونية. قم بسؤال أولئك الذين لديهم قواعد لإعداد قائمة تلك القواعد ومشاركتها مع باقي الصف. ثم قم بإعداد قائمة رئيسة، وتصنيف القواعد وفقا لنوعها. على سبيل المثال، قد تكون القواعد على الأرجح كما يلي:

- كمية الوقت المستهلك على الشبكة الإلكترونية.
- الوقت من اليوم الذي يسمح فيه للطالب بالتواجد على الشبكة الإلكترونية أو أمام الوسائل الإعلامية المقروءة والمكتوبة.
- استخدام مواقع إلكترونية معينة.
- استخدام التراسل الفوري.
- قائمة الأصدقاء على التراسل الفوري.
- المعلومات الشخصية التي يمكن وضعها.
- استخدام مواقع التواصل الاجتماعي.
- أنواع الألعاب التي يمكن لعبها (لا يوجد العاب مصنفة "للبالغين" على سبيل المثال).
- مكان الحاسوب مع قدرات الشبكة الإلكترونية (على سبيل المثال، يجب أن يكون في مكان عام).
- تثبيت برنامج التنقية على الشبكة الإلكترونية – متوفرة على الحاسوب.
- اللعب على ألعاب الشبكة الإلكترونية بعد إكمال الواجبات المنزلية
- تنزيل برنامج من الشبكة الإلكترونية.

التمرين (١١-٢):
مسح للآباء

قم بالطلب من الطلاب، كل من أولئك الذين لديهم بالفعل قواعد في المنزل تتعلق باستخدام الشبكة الإلكترونية وأولئك الذين ليس لديهم، توجيه الأسئلة التالية إلى آبائهم. قم بتوجيههم لإحضار الإجابات إلى المدرسة للحصة القادمة:

١. هل أنتم مهتمون بأي شكل من الأشكال باستخدامي للشبكة الإلكترونية؟
٢. هل ستكونون أكثر ارتياحًا أو أقل ارتياحا حول استخدامي للشبكة الإلكترونية إذا قمت بمشاركتكم بشكل يومي بتجاربي على الشبكة الإلكترونية؟
٣. هل ستكونون أكثر ارتياحًا او اقل ارتياحًا حول استخدامي للشبكة الإلكترونية إذا قمت بمناقشتكم بشكل يومي بالمشاكل التي أواجهها لدى التواجد على الشبكة الإلكترونية؟
٤. هل ستكونون أكثر ثقة أو أقل ثقة في قدرتي على الاعتناء بنفسي على الشبكة الإلكترونية إذا أخبرتكم بشكل يومي بما أفعله للبقاء بأمان على الشبكة الإلكترونية؟
٥. هل ستفضلون أكثر أو أقل بالسماح لي باستخدام الشبكة الإلكترونية إن لم يكن هنالك قواعد حول استخدامي للشبكة الإلكترونية؟
٦. هل ستفضلون أكثر أو أقل بالسماح لي باستخدام الشبكة الإلكترونية إذا كان الدخول على الشبكة الإلكترونية على حاسوبنا يحتوي على برنامج تنقية يساعد على حمايتي؟

قد يتردد بعض المراهقين في طرح هذه الأسئلة على والديهم؟ ومن الطرق المقترحة للتمكن من ذلك هي: ١) تقديم استطلاع الرأي للآباء في أمسية مفتوحة للآباء في مدرستك، ٢) وضع استطلاع الرأي على الشبكة الإلكترونية وإعطاء الطلاب رسالة إلى المنزل لآبائهم تحتوي على الرابط، ٣) الطلب من الصف القيام باستطلاع للرأي لمجموعة من الآباء. إن الأمر المهم لطلابك هو رؤية أن أكثر الآباء المنطقيين سوف يكونون أكثر ميولا للسماح لهم باستخدام الشبكة الإلكترونية إذا كان هنالك المزيد من التواصل معهم حول ما يفعلونه على الشبكة الإلكترونية ويمكنهم توضيح الكفاءات الضرورية لحماية أنفسهم ضد الإستغلال والتزوير.

قم بجمع الإجابات عن أسئلة استطلاع الرأي وقدم النتائج المحصلة إلى الطلاب لمناقشتها. من المرجح أن تدعم النتائج الفرضية التي مفادها بان التواصل بين الطفل والوالدين يقلل من مخاوف الآباء إلى أدنى حد. إن الهدف الرئيس لهذا التمرين هو تشجيع الأطفال والآباء هو وجود حوار حول الحياة على الشبكة الإلكترونية.

التمرين (١١-٣):
عقد مع الآباء

قم بتقديم القصة التالية إلى طلابك:

قصة كاسي Cassie

إن والدي كاسي ، الطالبة في الصف السابع، صارمان جدًّا ويبدو أنهما لا يسمحان لها ابدًا بفعل ما يفعله أصدقاؤها . على سبيل المثال، يستخدم العديد من أصدقائها التراسل الفوري ولكن هي غير مسموح لها . تشعر بأنها الوحيدة في مدرستها التي لا تستطيع استخدام التراسل الفوري. وكلما سألت والديها إن كان بإمكانها استخدامه، يكون الجواب السريع هو "لا" .

قم بالطلب من طلابك ما يلي:

١. كتابة الاسباب الرئيسية التي يعتقدون أنها وراء عدم السماح لوالدي كاسي لها باستخدام التراسل الفوري.
٢. كتابة عقد ينبغي أن تقدمه كاسي لوالديها للسماح لها باستخدام التراسل الفوري. أخبرهم أن يتذكروا أن هذا العقد يجب أن يكون عبارة عن مجموعة من القواعد ستقوم باتباعها عند استخدام التراسل الفوري. أخبرهم أن ينظروا إلى الاسباب التي كتبوها في إجابة السؤال رقم(١) لمساعدتهم على استنتاج القواعد التي يمكن أن تقلل مما يقلق والديها.
٣. انتقاد عقود بعضهم البعض. كصف واحد، عليكم اختيار أفضل القواعد وكتابة عقد نهائي مع بعضهم البعض.

التمرين (١١-٤):
إعدادات الخصوصية في الفيسبوك

إن هذا تمرين قيما لاهتمامات طلاب المدرسة الثانوية في إعدادات الخصوصية لشبكات التواصل الإجتماعي مثل الفيسبوك. إذا توفرت لديك خدمة الإنترنت وجهاز عرض لعرض الشاشة، قم بزيارة الفيسبوك (www.facebook.com). حاول إعداد حساب كعينة مع طلابك. سوف يتم منحك العديد من الاختيارات لاختيار إعدادات الخصوصية لحسابك.

تحدث مع طلابك حول محاسن ومساوئ كل من إعدادات الخصوصية. اطلب من طلابك مناقشة فوائد تعلم إعدادات أكثر خصوصية بدلاً من الإعدادات الأقل خصوصية. وبعض القيام بهذا التمرين، اقترح على طلابك التفكير بإعدادات الخصوصية الخاصة بحساباتهم على الفيسبوك.

التمرين (١١-٥):

مشروع إعلانات الخدمة العامة PSA Project

إن إعلان الخدمة العامة (PSA) هو إعلان غير تجاري مستخدم لتعليم العامة حول مسائل مهمة أو أمور السلامة. فيما يلي بعض الأمثلة لإعلان الخدمة العامة:

- مثال مصور فيديو على إعلان الخدمة العامة للسلامة على الإنترنت والمتواجد على YouTube.com : www.youtube.com/watch?v=LCrlZom3Ro
- تضع شبكة الوعي الإعلامي The Media Awareness Network في كندا بضع إعلانات للخدمة العامة PSA's حول السلامة على الإنترنت:
www.reseau-medias.ca/english/corporate/media_kit/pass.cfm
- يوجد إعلان للخدمة العامة PSA على عناوين يوتيوب YouTube حول التحرش الجنسي على الشبكة الإلكترونية (غير مناسب للطلبة الصغار):
www.youtube.com/watch?v=BoisfcfMA1Ql

إن لم يوجد في مدرستك برنامج لتسجيل الصوت والتحرير من أجل إنشاء وتحرير الملفات الصوتية، يمكنك استخدام Audacity (http://audacity.sourceforge.net)، محرر صوتي مجاني متوفر لكل من ماكنتوش Macs والحاسوب الشخصي PC. إنه برنامج سهل الإستخدام يسمح للطلاب بتسجيل العديد من الأصوات وتحرير الملفات الصوتية. بالنسبة للمدرسين الذين لديهم برنامج مع آلة تصوير فيديو وتحرير الفيديو مثل iMovie– وبالمزيد من الوقت يمكن إنشاء فيديو لإعلان الخدمة العامة PSAs.

قم بتقسيم الطلاب إلى مجموعتين لابتكار إعلان الخدمة العامة للسلامة على الإنترنت على الراديو. قم بتعيين مواضيع أو اطلب من الطلاب اختيار مواضيعهم الخاصة. يجب أن تكتب كل مجموعة في البداية لقطة على الراديو، والتي سيتم مراجعتها من قبل المعلم قبل التسجيل. قد ترغب بإعطائهم أدنى وأعلى حد للمقتطف على الراديو. وبمجرد الحصول على موافقتك على نص موضوع السلامة على الإنترنت الخاص بهم، دع الطلاب يسجلون إعلانات الخدمة العامة الخاص بهم.

المصادر

Age-based guidelines for kid's internet use. (2007, April 16).
متوفر من الموقع الإلكتروني لمايكروسوفت Microsoft:
www.microsoft.com/protect/family/age/stages.mspx

Lenhart, A., Madden, M., & Hitlin, P. (2005, July 27). *Teens and technology Youth are leading transition to a fully wired and mobile nation*.
متوفر من الموقع الإلكتروني لـ Pew Internet:
www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005Web.pdf

Turow, J., & Lilach, N. (2000, May). *The internet and the family 2000: The view from parents, the view from kids*. (Report Series No.33). Philadelphia: Pennsylvania University, Annenberg Public Policy Center. (ERIC Document Reproduction Service No. ED448874). Available from http://eric.ed.gov/ERICWebPortal/custom/portalets/record-Details/detailmini.jsp?= nfpb=true& &ERICxtSearch_SearchValue_0=ED448874&ERICExtSearch_SearchType_0=no&accno=ED448874

Using family contracts to help protect your kids online. (2006, October 21). متوفر من الموقع الإلكتروني لمايكروسوفت Microsoft:
www.microsoft.com/protect/family/guidelines/contract.mspx

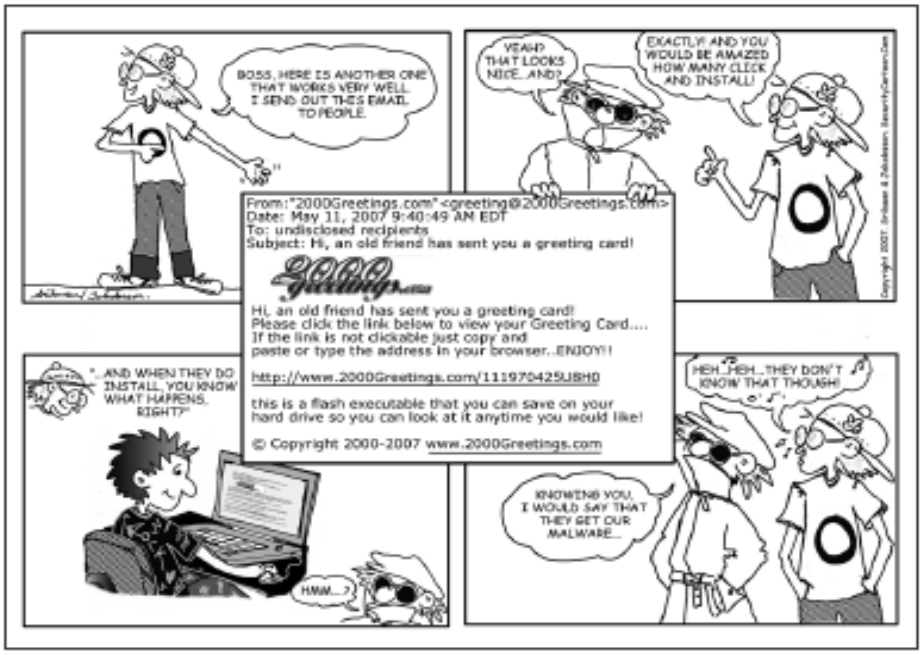
الفصل الثاني عشر

حماية معلوماتك الشخصية
Safeguarding Your Personal Information

قد يتم التقاط معلومات الشخصية أو حصرها أو نسخها أو سرقتها أو الاستيلاء عليها من قبل "آليات خاصة" وبيعها أو تخريبها أو إعلانها على الملأ بالاف الطرق المختلفة.

تصبح حماية خصوصيتنا على الشبكة الإلكترونية أصعب وأصعب بشكل متزايد. قد يتم التقاط معلوماتك الشخصية أو حصرها أو نسخها أو سرقتها أو الاستيلاء عليها من قبل "آليات خاصة" وبيعها أو تخريبها أو إعلانها على الملأ بآلاف الطرق المختلفة. قد يعتقد بعض الطلاب بأن خصوصيتهم لا تهم بالفعل. نأمل بأن يساعدك هذا الكتاب على إقناعهم بأن خصوصيتهم ومعلوماتهم الشخصية قيمة بالفعل.

لذا، ما مدى خصوصية المعلومات الشخصية لطلابك وعائلاتهم؟ اطلب من طلابك إكمال كل من التمارين في هذا الفصل وقم بتتبع نتائجهم. اطلب منهم التوضيح لوالديهم ما مدى ما يعرفونه عبر مشاركة هذه النتائج معهم. اطلب من طلابك تعليم والديهم أهمية المحافظة على خصوصيتهم على الشبكة الإلكترونية. نضمن أن يفوز الطلاب بنقاط في المنزل!



الشكل رقم (١٢-١): عملية احتيال تقليدية على الشبكة الإلكترونية

يمكن أن تسرق ديدان الحاسوب وبرامج القرصنة معلومات حساسة تبقى في متصفح الشبكة الإلكترونية. التمرين١٢ –١– ماذا يمكن أن يكشف متصفح الشبكة الإلكترونية الخاص بك عنك؟ يقدم موقع إلكتروني الذي يوفر نصًا يكشف المعلومات الشخصية الحساسة مثل: الاسم والعنوان ورقم الهاتف ورقم البطاقة الإئتمانية وكلمة المرور التي يتم تخزينها في متصفح الشبكة الإلكترونية.

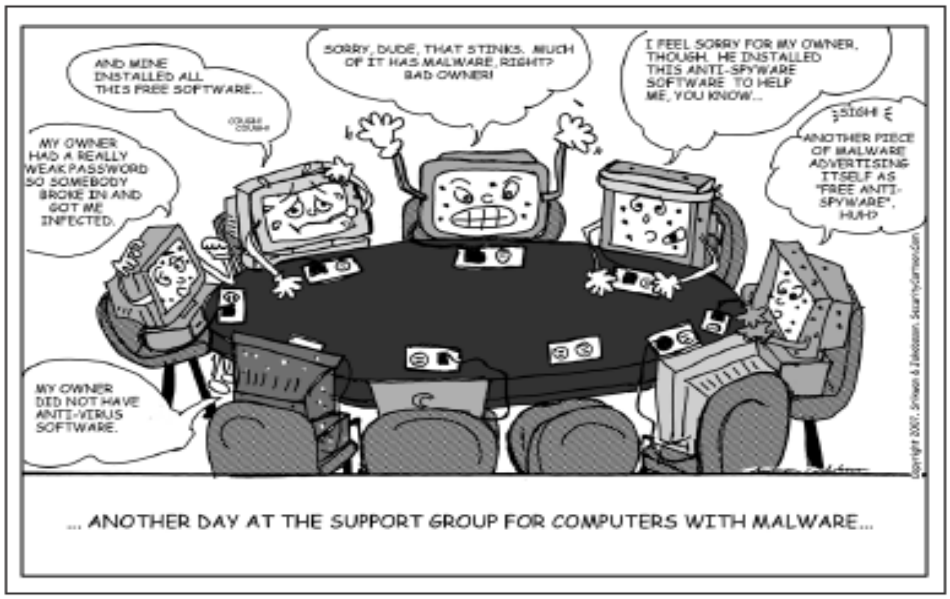
كما يمكن الحصول على المزيد من المعلومات الشخصية من خلال البحث في رقم الهاتف ودليل الهاتف. التمرين ١٢–٢ – هل يمكن العثور عليك من خلال رقم هاتفك؟ يطلب من الطلاب البحث عن المعلومات المتوفرة عبر الغوغل وإرشادهم إلى كيفية إزالة معلوماتهم. التمرين ١٢–٣ – عمليات البحث في دليل الهاتف، يسأل الطلاب القيام بعمليتي بحث في دليل الهاتف عن أنفسهم وأفراد عائلتهم.كما أنه يوفر إرشادات حول الكيفية التي يستطيع فيها الطلاب إزالة معلوماتهم الشخصية من قواعد البيانات. التمرين ١٢–٤ – ما الذي يستطيع أن يجده الآخرين عن منزلكم؟ يكشف عن الكمية الهائلة من المعلومات الشخصية المتوفرة على الشبكة الإلكترونية، مثل القيمة المقدرة لمنازلهم ومخطط منازلهم.

P2P والبرامج الضارة Malware

هل يستخدم طلابك برنامج P2P (خدمة التواصل ونقل الملفات بين الأجهزة مباشرة بدون جهاز حاسوب رئيس)؟ يسمح برنامج P2P لمستخدمية بمشاركة الملفات مع بعضهم البعض عبر الشبكة الإلكترونية. تتضمن البرامج الشائعة Limewire و Kazaa و Shareaza و Morpheus. لسوء الحظ، وجد أن بعض هذه البرامج تثبت برامج للتجسس والإعلانات. مؤلف Spyware Warrior، إيريك هويز Eric Howes، وجد أن Kazaa يثبت ٣٥ جزءا مختلفا من برامج التجسس مع Kazaa. بين إيديلمان Ben Edelman، باحث معروف في برامج التجسس والإعلانات، وجد أيضا أن Kazaa 3.0 يثبت برنامج إعلانات بالإضافة إلى تطبيق Kazaa.

هل ترغب في معرفة إن كان برنامج P2P الخاص بك يثبت برنامج تجسس. قم بالإطلاع على بحث بين إيديلمان Edelman Ben عن التجسس وP2P : www.benedelman.org/spyware/p2p/

إن العديد من الملفات المتداولة على شبكات P2P تم اكتشاف أنها تحتوي أيضا على حصان طروادة Trojan horses، وديدان worms وفيروسات viruses. ومع ذلك، إن لم يثبت برنامج P2P أي برنامج للتجسس، وبشكل اعتيادي، قد يشارك برنامج P2P كامل محتويات حاسوب أحد الطلبة مع مستخدمي P2P الآخرين. هل لدى طلابك أي من هذه البرامج مثبتة على حاسوبهم؟ إن كان كذلك، أخبرهم بتفقد التطبيقات المفضلة لمشاهدة ما يتم مشاركته فقط. إن توصيتنا هي عدم مشاركة أي شيء! قم بإطفاء المشاركة. قد يكون الطلاب يسمحون للآخرين للوصول إلى الملفات الموجودة على حواسيبهم.



الشكل رقم (١٢-٢): مجموعة دعم للحواسيب المصابة

منارات الشبكة الإلكترونية Web Beacons

يتم استخدام منارات الشبكة الإلكترونية Web Beacons، والتي تسمى أيضًا جواسيس الشبكة الإلكترونية Web Bugs و ملف صورة GIF، لمراقبة نشاط الأشخاص على الشبكة الإلكترونية. تتكون منارة الشبكة الإلكترونية في العادة من صورة شفافة (صغيرة جدًّا، يكون مقاسها في العادة ١ بيكسيل × ١ بيكسيل) يتم وضعها على موقع إليكتروني أو في رسالة إلكترونية. تسمح منارة الشبكة الإلكترونية للموقع بتسجيل أحداث معينة للمستخدم الذي يفتح الصفحة أو البريد الإلكتروني الذي يحتوي على هذه المنارة. إن هذه عبارة عن طريقة يمكن للمحتالين من خلالها تحديد إن كان المستلم قد فتح الرسالة الإلكترونية. كما يستخدم المعلنون على الشبكة الإلكترونية منارات الشبكة الإلكترونية. لسوء الحظ، لا يوجد أي شيء يستطيع متلقي الرسالة الإلكترونية فعله لتجنب منارة الشبكة الإلكترونية من الإبلاغ عن الأمر. وما يؤديه القيام بفتح رسالة إلكترونية تحتوي على منارة الشبكة الإلكترونية هو إبلاغ المرسل بذلك.

ملفات تعريف إرتباط الإعلانAdvertising Cookies

إن ملفات تعريف الارتباط مجهزة على مشغل الأقراص الصلبة ويراقب سلوككم في التصفح. ليست جميع ملفات تعريف الارتباط سيئة وليست جميع ملفات الارتباط هي عبارة عن منقبات للبيانات تحاول تعقب نشاطاتكم على الشبكة الإلكترونية. على سبيل المثال، قد تخزن بعض ملفات تعريف الارتباط تفضيلات مختارة للزائر في استخدام موقع إلكتروني معين. بالنسبة لأولئك الطلبة الذين يرغبون في الحصول على نظرة عن كثب على ملفات تعريف الإرتباط التي يتم تثبيتها على حاسوبهم ومن ثم إدارته. توجد العديد من البرنامج المتوفرة. يستطيع الطلاب زيارة Download.com (www.download.com) وإدخال مصطلح البحث "cookie". تبين تقديرات المستخدم ما الذي يوصي به الآخرين. التمرين ١٢–٥ –ملفات تعريف إرتباط الإعلان يبين للطلاب كيفية تحديد ملفات تعريف إرتباط الإعلان على حواسيبهم والتي تتعقب متصفحهم على الشبكة الإلكترونية وتجمع وتشارك المعلومات الشخصية.

التمارين

التمرين (١٢-١):
ماذا يمكن أن يكشف متصفح الشبكة الإلكترونية الخاص بكم عنكم؟

اطلب من الطلاب زيارة صفحة إلكترونية تم ابتكارها من قبل أستاذ مشارك في كلية المعلوماتية في جامعة إنديانا

Indiana University School of Informatics
(http://homer.informatics.indiana.edu/cgi-bin/riddle/riddle.cgi/)

والنقر على زر الإجابة. هل كان البرنامج المتوافر على الشبكة الإلكترونية قادر على الكشف عن أي شيء عنهم؟

حتى إن لم تكشف أي شيء على الإطلاق، لا يجب أن يشعر الطلاب بأنهم في أمان. يمكن أن تسرق العديد من ديدان الحاسوب وبرامج القرصنة المعلومات الموجودة في مكان التعبئة في متصفح الشبكة الإلكترونية. بما في ذلك كلمات المرور. يجب أن يفتح الطلاب تفضيلات متصفحات الشبكة الإلكترونية لمنزلهم والتحقق لمشاهدة المعلومات الشخصية المخزنة هناك. اطلب منهم توصية آبائهم بأن تلك المعلومات قد تم شطبها.

التمرين (١٢-٢):

هل يمكن العثور عليك من خلال رقم هاتفك؟

١. اطلب من الطلاب زيارة (www.google.com)
٢. اطلب منهم إدخال رقم هاتف منزلهم في حقل البحث، باستخدام رمز المنطقة والفواصل (على سبيل المثال، 555-555-5555) ثم انقر على بحث.

هل يوجد على الغوغل ملف لأي أحد من الطلاب؟ هل توجد روابط لخرائط وإرشادات لمنازلهم؟ إذا نقروا على اختيار نتائج دليل الهاتف، يجب أن يجدوا رابطًا يعمل على إزالة معلوماتهم، إذا رغبوا بذلك. يمكنك أيضًا الطلب من الطلاب إدخال أرقام هواتف أصدقائهم وأفراد العائلة الآخرين.

التمرين (١٢-٣):
عمليات البحث في دليل الهاتف

ما كمية المعلومات التي يمكن أن يوفرها بحث بسيط في دليل الهاتف على الشبكة الإلكترونية عن الطلاب وعائلاتهم. اطلب من الطلاب زيارة كل من المواقع الإلكترونية أدناه والبحث عن أسمائهم ومن ثم أسماء والديهم أو الأوصياء عليهم.

- Switchboard (http://switchboard.intelius.com)
لطلب إزالة تلك المعلومات من قاعدة بيانات Switchboard، يستطيع الطلاب النقر على رابط الخصوصية على زر الصفحة الرئيسة ومن ثم اتباع رابط الإزالة Opt-Out.
- AnyWho (www.anywho.com)
لطلب إزالة تلك المعلومات من قاعدة بيانات AnyWho، يستطيع الطلاب النقر على رابط المساعدة Help على زر الصفحة الرئيسة ومن ثم اتباع رابط "كيفية إزالة القائمة السكنية الخاصة بكم".

التمرين (١٢-٤):
ما الذي يستطيع أن يجده الآخرون عن منزلكم؟

هل يستطيع الآخرون معرفة عدد غرف النوم أو عدد دورات المياه الموجودة في منازل الطلاب؟ هل يمكنهم معرفة ثمن منازلهم؟ اطلب من الطلاب زيارة Zillow.com (www.zillow.com) وإدخال عنوان الشارع والمدينة والولاية ورمز المنطقة.

التمرين (١٢-٥):
إعلان ملفات تعريف الارتباط

يمكن أن يشاهد الطلاب عينة من ملفات تعريف إرتباط الإعلان الموجودة في حواسيبهم ومراقبة سلوك متصفحهم على الشبكة الإلكترونية. اطلب من الطلاب زيارة مبادرة شبكة الإعلان على الشبكة الإلكترونية Network Advertising Initiative online (www.networkadvertising.org) والنقر على أداة المستهلك للإزالة Consumer Opt-Out للمستهلكين للعثور على قائمة بملفات تعريف ارتباط متصفح الشبكة الإلكترونية التي تراقب نشاطهم على الشبكة الإلكترونية. سوف تتحقق هذه الأداة فقط من نسبة مئوية صغيرة لملفات تعريف الارتباط المحتملة التي قد تكون تراقب نشاطكم على الشبكة الإلكترونية. على الرغم من أن الطلاب لديهم اختيار حذف ملفات تعريف ارتباط الإعلان، قد يكون هنالك العديد من ملفات تعريف الإرتباط الأخرى الموجودة على حواسيبهم والتي لا يمكن إزالتها. من الأفضل إعداد متصفح الشبكة الإلكترونية لعدم قبول طرف ثالث من ملفات تعريف الارتباط. إن الطرف الثالث من ملفات تعريف الارتباط هي تلك التي تأتي من موقع إلكتروني غير الذي تمت زيارته.

المصادر

P2P file sharing (2008, February).

متوفر من الموقع الإلكتروني لـ OnGuard Online: www.onguardonline.gov/p2p.html
إن هذه الصفحة تدرج مخاطر برنامج P2P. ويتضمن الموقع لعبة لاختبار لفحص معرفتكم عن مخاطر برنامج P2P بالإضافة إلى شريط مصور من iSafe حول بعض المسائل المتعلقة ببرنامج P2P.

Online data vendors: How consumers can opt out of directory assistance and non-public information. (2007, June).

متوفر في الموقع الإلكتروني لـ Privacy Rights Clearing-house:
www.privacyrights.org/ar/infobrokers.htm
إن هذه عبارة عن قائمة شاملة لبيانات البائعين الذين يقدمون بوليصة "إزالة opt-out" وأولئك الذين لا يقدمونها.

World Wide Web Consortium (W3C) - Platform for Privacy Preferences (P3P) Project : www.w3.org/P3P/
على هذا الموقع، يمكنكم العثور على المزيد من التوصيات عن W3C ومبادرات لبناء أدوات الخصوصية في متصفحات الشبكة الإلكترونية.

World privacy forum's top ten outs. (2008, January 28).

متوفر في الموقع الإلكتروني لـ World Privacy forum:
www.worldprivacyforum.org/toptenoptout.html
قام منتدى الخصوصية العالمي World Privacy Forum بوضع أهم عشرة أمور يجب إزالتها والتي يوصي بها للمستهلكين. يجب أن يوضح الطلاب هذا المصدر لآبائهم أو الأوصياء والإشادة عليهم بالاستفادة من هذه الخدمة.

الملحق (أ)

المصادر على الشبكة الإلكترونية

إن المصادر المتوفرة هنا تتراوح من نصيحة عامة ممتازة إلى نصيحة فنية لأولئك الذين يمتلكون مهارات أكثر تعقيدًا على الحاسوب. إن القائمة لا نهائية، والهدف منها اقتراح أماكن للبدء بالبحث عن معلومات إضافية متعلقة بالمواضيع في النص واستكمال المصادر الموجودة في كل فصل.

إن الشبكة الإلكترونية بحر متغير باستمرار من المعلومات. وحتما سوف تصبح بعض الروابط أدناه قديمة أو تغيرت إلى مواقع جديدة على الشبكة الإلكترونية. إذا وجدت رابطًا لا يعمل أو حاولت إزالة جزء من الرابط بعد خط مائل (/) لرؤية ما هو متاح في الموجه السابق على الحاسوب. أو قم بالذهاب إلى أعلى مستوى للمجال وابحث عن رابط جديد للعنصر الذي تريده.

وقد تم إنشاء منطقة محمية بكلمة مرور لموقعنا الإلكتروني (www.ChildrenOnline.org) يحتوي على عناوين عامة لمواقع إلكترونية متضمنة في هذا الكتاب. إن كلمة المرور هي 7xStG!972H. سوف نبذل أفضل ما في وسعنا لاستبدال الروابط المنتهية بمجرد الإبلاغ عنها أو إضافة مصادر إضافية.

Apple.com
www.apple.com/macosx/features/security
معلومات من حاسوب أبل Apple Computer حول مميزات الأمن لحواسيب أبل Apple ونقص الفيروسات والتلاعبات والبرامج الضارة التي تؤثر على أجهزة ماكنتوش.

Benjamin Edelman - Media Coverage
www.benedelman.org/media
السيد/ إيديلمان هو أستاذ مساعد في كلية الأعمال بجامعة هارفارد ويقوم بإجراء أبحاث على وسائل وآثار برامج التجسس والإعلانات. يدرج موقعه الإلكتروني العديد من المقالات الإلكترونية ذات الصلة.

ChildrenOnline.org
إن هذا موقع مساندة لمؤلفي هذا الكتاب. تم وضع المصادر والمقالات مصحوبة بقائمة للتواريخ القادمة لعروضنا.

Cyberangels.org
من أجل إجراء مناقشة صريحة لـ "cyber street smarts" للشباب، قم بزيارة الموقع الإلكتروني لـ CyberAngels (www.cyberangels.org).تقدم دروسه التعليمية "Internet 101" نصائح ذات مغزى حول مجموعة متنوعة من المواضيع المتعلقة بالمراهقين بما في خدمات المواعدة والتحرش على الشبكة العنكبوتية وخصوصية البريد الإلكتروني ومخاطر مشاركة الملفات.

CyberTipLine.com
تم إنتاج CyberTipLine.com من قبل المركز القومي للمفقودين والأطفال المستغلين National Center for Missing and Exploited Children. يوفر عدد من المصادر بما في ذلك فيديوهات للخدمة العامة حول المتهجمين على الشبكة الإلكترونية. يتضمن هذا موقعًا مفيدًا جدًّا للمراهقين يدعى "لا تصدق النوع" "Don't believe the type".

متصفح الشبكة الإلكترونية لفايرفوكس Firefox Internet
تمتلك فايرفوكس Firefox العديد من "الإضافات" التي تسمح لميزات جديدة مثل القدرة على تنقية محتوى الشبكة الإلكترونية وجعل تصفح الشبكة الإلكترونية أكثر أمانا. قم بزيارة الإضافات المتوفرة لـ "تصفح الخصوصية والامن" عبر الذهاب إلى:
https://addons.mozilla.org/en-US/firefox/browse/type:1/cat:12

تتضمن بعض الامثلة المحددة ما يلي:

- FozFilter (لأجهزة الحاسوب الشخصية فقط): https://addons.mozilla.org/en-US/firefox/addon/4351
- ProCon Latte (لجميع المنصات): https://addons.mozilla.org/en-US/firefox/addon/1803
- LeeBlock (لجميع المنصات): https://addons.mozilla.org/en-US/firefox/addon/4476

GetNetWise.org
إن GetNetWise.org مصدر ممتاز للمعلمين والطلاب والآباء حول العديد من المواضيع المتعلقة بالسلامة على الشبكة الإلكترونية وحماية خصوصية الفرد على الشبكة الإلكترونية. إنه مشروع لمؤسسة تعليم الإنترنت Internet Education Foundation (http://neted.org).

GetSafeOnline.org
إن GetSafeOnline.org ممول من قبل الحكومة البريطانية والأعمال البريطانية. يحتوي الموقع على العديد من المصادر القيمة التي تتضمن اختبار من عشرة أسئلة لاختبار معرفتهم حول السلامة على الشبكة الإلكترونية. إنه مصدر ممتاز للنصائح والإرشادات.

Microsoft.com/protect/
مجموعة متنوعة من الصفحات الإلكترونية مع مصادر تركز على الحاسوب والسلامة على الشبكة الإلكترونية بالإضافة إلى حماية خصوصية الفرد على الشبكة الإلكترونية.

مميزات Vista OS features
www.microsoft.com/windows/products/windowsvista/features/safer.mspx

المساعدة للوقاية من فيروسات الحاسوب Help To Prevent Computer Viruses
www.microsoft.com/protect/computer/viruses/prevent.mspx

خطوات لحماية حاسوبك Steps to Protect Your Computer
www.microsoft.com/protect/computer

المحافظة على معلوماتك أكثر أمانا Keep Your Information More Secure
www.microsoft.com/protect/yourself/

الإشراف الأبوي والإرشاد القائم على العمر Parental Supervision and Age-Based Guidance
www.microsoft.com/protect/family

فيديوهات على الشبكة الإلكترونية التي تدعم السلامة على الشبكة الإلكترونية والسلوك الصحي على الشبكة الإلكترونية Online videos supporting Internet safety and healthy online behavior
www.microsoft.com/protect/videos

OnGuardOnline.gov
http://onguardonline.gov/isafevideo.html
يوفر هذا الموقع مجموعة متنوعة من الفيديوهات على الشبكة الإلكترونية المنتجة من قبل iSafe.org. يرافق كل فيديو خطة درس ومرشد مصادر للمعلمين. تغطي الفيديوهات مواضيع مثل برامج التجسس والإحتيال ومشاركة الملفات وسرقة الهوية.

OpenDNS.com
يوفر تجربة تصفح أسرع وأكثر أمانًا على الشبكة الإلكترونية من خلال البحث في نظام اسم المجال DNS (Domain Name System Lookups)بينما تضع ملايين المواقع الإلكترونية لمحتوى البالغين على القائمة السوداء.إنه مجاني، لا يتطلب أي شيء للتنزيل ويفيد لجميع أنواع الحواسيب/ المنصات/ أنظمة التشغيل.

PCTools.com
www.pctools.com/guides/security/

يوفر PCTools دليل للأمن على الشبكة الإلكترونية لجميع النسخ من ويندوز Windows ومكتشف الشبكة الإلكترونية Internet Explorer.

Provoxy

www.privoxy.org

يصف Provoxy نفسه بأنه "وسيط للشبكة الإلكترونية مع قدرات تنقية متقدمة لحماية الخصوصية، وتغير بيانات الصفحة الإلكترونية، وإدارة ملفات تعريف الارتباط والتحكم بالدخول وإزالة الإعلانات واللافتات والنوافذ المنبثقة وغيرها من البرمجيات المؤذية على الشبكة الإلكترونية". تتوفر لماكنتوش Macs وأجهزة الحاسوب الشخصي PCs بالإضافة إلى أنظمة التشغيل الأخرى.

Safeteens.com and Safekids.com

يقوم كاتب عامود في صحيفة لاري ماجيد Larry Magid مصادر ومقالات للأطفال والمراهقين ووالديهم والتي تتضمن العديد من مقالاته عن سلامة الطفل والمراهق على شبكة الإنترنت.

شركة الأمن **Sophos.com**

www.sophos.com/security/top-10

يتم الإبلاغ عن أكثر عشرة برامج ضارة لسوفوس Sophos خلال أي شهر.

ملاحظة: تحتوي بعض البرامج الضارة المدرجة في Sophos.com الكثير من الأسماء الصريحة العدائية والجنسية.

قائمة الاحتيال على سوفوس Sophos: www.sophos.com/security/hoaxes/

معلومات الأمن العامة: www.sophos/com/security/

SpywareGuide

www.spywareguide.com

يصف SpywareGuide أنفسهم بأنهم "الموقع المرجعي العام الرائد للبحث في برامج التجسس والشبكة الرمادية وتفاصيل عن تطبيقات التجسس والإعلانات والشبكة الرمادية وسلوكياتها، والتي يتم ضمها في قاعدة بيانات مكثفة ومحدثة."

استخدام الرسومات الكرتونية لتدريس الأمن على الشبكة الإلكترونية

Using Cartoons to Teach Internet Security بقلم S. Srikwan و M. Jakobsson

ظهرت في Journal of Cryptologia، في ربيع عام م٢٠٠٨.

كما أنه متوافر أيضًا من: www.markus-jakobsson.com

VirusTotal
www.virustotal.com
تصف VirusTotal نفسها بأنها "خدمة تحلل الملفات المشبوهة وتسهل الاكتشاف السريع للفيروسات والديدان وأحصنة طروادة وجميع البرامج الضارة التي تكتشف من قبل محركات مكافحة الفيروسات". إن هذه خدمة مجانية وقامت PCWorld بتصنيفها في أعلى ١٠٠ منتج لعام ٢٠٠٧م.

WiredSafety.org
www.wiredsafety.org/youth.html
www.wiredteens.org
www.wiredpatrol.org
توفر عائلة WiredSafety للمواقع الإلكترونية مصادر للمراهقين.

ZoneAlarm.com
www.zonealarm.com/store/content/home.jsp
برنامج جدار ناري معروف وشائع جدا لمالكي اجهزة الحواسيب الشخصية من قبل Check Point Software.
كما تنتج ZoneAlarm تنتج ملف PDF تنزيله مجاني عنوانه " كيف تحمي الحاسوب الشخصي لعائلتك""Your How to Protect Your Family's PC"
www.zonealarm.com/store/content/promotions/defendthenet/index.jsp
يحتوي على معلومات قيمة لجميع مستخدمي الحاسوب التي تعزز بعض من توصيات هذا الكتاب.

المصادر الكشافة

أسرار ويندوز Windows secrets
www.windowssecrets.com

أسرار ويندوز Windows secrets هي عبارة عن رسالة إخبارية مجانية توفر العديد من النصائح التقنية الرائعة حول استخدام Windows OS. يقدم هؤلاء الخبراء في العادة نصيحة رائعة للمحافظة على الـ Windows في حاسوبك أكثر أمانا وفي نظام جيد للعمل.

ما يلي أدناه هو عبارة عن مقتطف من مقالة نشرت في Windows secrets، العدد ٢٠، في شهر أغسطس/ آب لعام ٢٠٠٧ (www.windowssecrets.com/comp/070816#story1) وتطبق فقط نظام تشغيل ويندوز. وعليه، تبين هذه المقالة الهدف الواضح جدًّا حول سبب أهمية قيام جميع مستخدمي الحاسوب بتحديث برامجهم بانتظام بأحدث رقعة للأمن. تحتوي المقالة الأصلية على معلومات مفصلة إضافية حول كيفية تحديث كافة مشغلات الوسائط الإعلامية المذكورة.

مشغلات الوسائط أكثر خطورة من ويندوز
Media Players more dangerous than Windows
بقلم سكوت دان Scott Dunn

يواجه مستخدمة ويندوز مخاطر أمن كبيرة اليوم ليس من التدفقات في ويندوز بحد ذاته بل من عدم وجود رقع لمشغلات الوسائط الإعلامية.

يعود السبب إلى أن العديد من قارئي Windows Secrets وفقًا لاختبار على الشبكة الإلكترونية قمنا بتمويله، يشغلون نسخ من Flash و Java و QuickTime غير المحدثة ضد تهديدات الأمن الحديثة.

قارئ الأنظمة مملوءة بتوابع منتهية الصلاحية

أظهرت اختبارات لمشتركينا أي من التطبيقات التي يتم على الأرجح تثبيتها ولكنها غير ملتصقة على الحواسيب الشخصية للمستخدمين. في القائمة التالية، يمثل رقم ١ التطبيق غير الملتصق الذي تم العثور عليها على أكبر عدد لآلات القراءة، مع أرقام أكبر تمثل آلات أقل:

١. Adobe Flash Player 9.x
٢. Sun Java JRE 1.6.x/6.x
٣. Macromedia Flash Player 6.x

٤. Macromedia Flash Player 8.x
٥. Macromedia Flash Player 7.x
٦. Apple QuickTime 7.x
٧. Macromedia Flash Player 5.x
٨. Mozilla Firefox 2.0x
٩. Macromedia Flash Player 4.x
١٠. Adobe Reader 7.x
١١. Apple QuickTime 7.x
١٢. Macromedia Flash Player 5.x
١٣. Mozilla Firefox 2.0x
١٤. Macromedia Flash Player 4.x
١٥. Adobe Reader 7.x

إن جميع هذه التطبيقات هي مشغلات الوسائط الإعلامية، ومتصفح البرامج الإضافية التي تشغل الملفات الإعلامية أو متصفح بحد ذاته (أي فايرفوكس Firefox). يمكن أن تتعرض جميع هذه البرامج لهجومات على الشبكة الإلكترونية – على سبيل المثال، إذا لعبت لعبة تحتوي على فيروس على موقع إلكتروني أو كنت قد استلمتها عبر البريد الإلكتروني. ونتيجة لذلك، فإن استخدام نسخة قديمة من هذه البرامج يطرح خطر أمني حقيقي.

حافظ على أدواتك على الشبكة الإلكترونية محدثة

لحسن الحظ، تدعم جميع التطبيقات المذكورة أعلاه التحديث التلقائي. بالإضافة إلى ذلك، تسمح لك باختيار تحديثها بشكل يدوي، إذا كنت تفضل إجراء تحديثات بصورة شهرية بنفسك. فيما يلي الخطوات التي يجب القيام بها لتحديث كل برنامج:

تحديث Adobe Flash Player

إن إعدادات التحديث لـ Adobe Flash Player مخزنة على حاسوبك ولكن يتم الدخول إليها عبر الشبكة الإلكترونية.

الخطوة الأولى	قم بتشغيل متصفح الشبكة الإلكترونية والملاحة في لوحة Glpba; Mptoofocaton لمنظم الإعدادات باستخدام رابط Macromedia
الخطوة الثانية	استخدام خانة التأشير لتشغيل التحديث التلقائي (تم تأشيره) أو إطفائه (لم يتم تأشيره). ضبط القائمة المنسدلة لتحديد كيفية البحث في البرنامج عن تحديثات.

إذا كنت تفضل تحديث Flash Player يدويًا , يجب أن تزور صفحة تحميل Adobe بصورة دورية .

لتحديث Sun Java

الخطوة الأولى	في لوحة التحكم بويندوز Windows Control Panel، قم بتشغيل برنامج QuickTime. يمكنك أيضا النقر على يمين أيقونة QuickTime في لوحة شريط المهام واختيار QuickTime Preferences أو البحث عن تحديثات QuickTime Updates.
الخطوة الثانية	إن لزم الأمر، انقر على مفتاح التحديث Update. استخدم مربع التأشير لتحديد إن كنت ترغب ان يبحث البرنامج عن تحديثات تلقائيا. انقر على موافق OK.

إذا كنت تفضل تحديث Java يدويا، قم بإلغاء التاشير على مربع التحديث التلقائي. ثم قم بالعودة إلى هذا المربع الحواري بصورة دورية وانقر على تحديث الآن Update Now على زر مفتاح التحديث.

لتحديث Apple QuickTime:

الخطوة الأولى	في لوحة التحكم بويندوز Windows Control Panel، قم بتشغيل بريمج QuickTime. يمكنك أيضا النقر على يمين أيقونة QuickTime في لوحة شريط المهام واختيار QuickTime Preferences أو البحث عن تحديثات QuickTime Updates.
الخطوة الثانية	إن لزم الأمر، انقر على مفتاح التحديث Update. استخدم مربع التأشير لتحديد إن كنت ترغب ان يبحث البرنامج عن تحديثات تلقائيا. انقر على موافق OK.

إذا كنت تفضل تحديث QuickTime بشكل يدوي، قم بإلغاء التأشير عن مربع التحديث التلقائي. قم قم بالعودة إلى مربع الحوار بشكل دوري وانقر على زر التحديث Update. إن لم يتم العثور على أي تحديث، انقر على موافق Ok للمتابعة.

لتحديث Mozilla Firefox:

الخطوة الأولى	في Firefox، قم باختيار أدوات، ثم خيارات

الخطوة الثانية: انقر على مفتاح التحديث. استخدم مربع تأشير Firefox لإعداد تفضيلك للتحديث التلقائي. عندما يتم التأشير عليه، يسمح لاختيارات إضافية لتخصيص كيفية حدوث التحديثات. انقر على موافق OK

إذا كنت تفضل تحديث Firefox بشكل يدوي، قم بإلغاء التأشير عن مربع Firefox في مربع الحوار. ثم قم بشكل دوري باختيار مساعدة Help، انقر على التحديثات Updates.

لتحديث Adobe Reader:

الخطوة الأولى: في Adobe Reader، قم باختيار المساعدة Help، ثم قم بالتأشير على التحديثات Updates.

الخطوة الثانية: إذا كان عنوان الحوار هو "Adobe Updater"، قم انقر على التفضيلات Preferences.

الخطوة الثالثة: استخدم الضوابط في مربع الحوار Adobe Updater Preferences لإعداد إشعار التحديث. انقر على موافق OK.

http://windows.com/comp/070816/#story1

الملحق (ب)

معايير التكنولوجيا التعليمية
الوطنية للطلاب (NETS*S)

إن معايير التكنولوجيا التعليمية للطلاب مقسمة إلى ستة فئات واسعة. سوف يتم تقديم المعايير ضمن كل فئة وتعزيزها وممارستها من قبل الطلاب. يستطيع المعلمون استخدام هذه المعايير كإرشادات لتخطيط النشاطات القائمة على التكنولوجيا التي يستطيع الطلاب أن يحققوا فيها النجاح في التعلم والتواصل ومهارات الحياة.

١. الإبداع والابتكار

يظهر الطلاب تفكيرًا إبداعيًا ويبنون المعرفة ويطورون منتجات وعمليات مبتكرة باستخدام التكنولوجيا. الطلاب:

أ. يطبقون المعرفة الحالية لتوليد أفكار جديدة ومنتجات أو عمليات.
ب. يبتكرون أعمال أصلية كوسيلة للتعبير الشخصي أو عن المجموعة.
ت. يستخدمون نماذج أو إيحاءات للكشف عن أنظمة ومسائل معقدة.
ث. يحددون المساعي ويتوقعون الاحتمالات.

٢. التواصل والتعاون

يستخدم الطلاب الإعلام الرقمي وبيئات للتواصل والعمل بشكل تعاوني بما في ذلك فاصل، لدعم التعلم الفردي والمساهمة في تعلم الآخرين. الطلاب:

أ. يتفاعلون ويتعاونون وينشرون مع نظرائهم أو الخبراء أو غيرهم باستخدام مجموعة من البيئات الرقمية ووسائل الإعلام.
ب. يوصلون المعلومات والافكار بفعالية إلى العديد من الجماهير باستخدام مجموعة من وسائل الإعلان والنماذج.
ت. ينمون الفهم الثقافي والوعي العالمي من خلال الإرتباط مع المتعلمين في ثقافات أخرى.
ث. يساهمون في مشروع الفريق لإنتاج أعمال أصلية أو حل المشاكل.

٣. سهولة البحث والمعلومات

أ. يخططون الإستراتيجيات لتوجيه الإستفسار.
ب. يحددون وينظمون ويحللون ويقيمون ويفترضون ويستخدمون المعلومات بشكل أخلاقي من مجموعة متنوعة من المصادر الوسائل الإعلامية.

ت. يقيمون ويختارون مصادر المعلومات والأدوات الرقمية القائمة على ملائمة المهمات المحددة.
ث. متابعة المعلومات وتقديم تقرير بالنتائج.

٤. التفكير الناقد، وحل المشاكل، واتخاذ القرارات
يستخدم الطلاب مهارات التفكير الناقد لتخطيط وإجراء البحوث، وإدارة المشاريع، وحل المشاكل، واتخاذ قرارات ضليعة باستخدام الأدوات والمصادر الرقمية المناسبة.
الطلاب:
أ. يحددون ويعرفون المشاكل الأصلية وأسئلة مهمة للتحقيق فيها.
ب. يخططون ويديرون النشاطات لتطوير حل أو إكمال مشروع.
ت. يجمعون ويحللون البيانات لتحديد الحلول واتخاذ القرارات الضليعة.
ث. يستخدمون طرق متعددة ومنظرات مختلفة للكشف عن الحلول البديلة.

٥. المواطنة الرقمية
يفهم الطلاب المسائل الإنسانية والثقافية والإجتماعية المتعلقة بالتكنولوجيا ويمارسون السلوك القانوني والإخلاقي.
الطلاب:
أ. يحبذون ويمارسون الإستخدام الآمن والقانوني والمسؤول للمعلومات والتكنولوجيا.
ب. يظهرون موقفا إيجابيا نحو استخدام التكنولوجيا التي تدعم التعاون والتعلم والإنتاجية.
ت. يظهرون مسؤولية شخصية للتعلم مدى الحياة.
ث. يظهرون القيادة للمواطنة الرقمية.

٦. عمليات ومفاهيم التكنولوجيا
يظهر الطلاب فهم معتدل لمفاهيم وأنظمة وعمليات التكنولوجيا.
الطلاب:
أ. يفهمون ويستخدمون أنظمة التكنولوجيا.
ب. فعالية ويختارون ويستخدمون التطبيقات بإنتاجية.
ت. يشخصون الخطأ ويصلحونه في الأنظمة والتطبيقات.
ث. ينقلون المعرفة الحالية إلى تعلم تقنيات جديدة.