دور المعلم للأستخدام الآمن للحاسوب

Copyright Q-CERT 2007

دور المعلم للأستخدام الآمن للحاسوب

Q-CERT– الورشة التعليمية الأولى لمُعلمين المراحل الاساسية
إعداد : وئام يونس

مُقدمة

إن المعلمين في المراحل التأهيلية من الروضة إلى الصف الثاني عشر ، لهم عدة أدوار تجاه الطلاب – فهم مدرسون، و شخصيات ذوو سلطة ، و وسطاء لمسيرة العلم ، ومرشدون، ومربون ، و محافظون على الأمن. يقوم المعلمون بهذه الأدوار بجّدٍ وعَفوية خلال و خارج نطاق تدريس المواد التعليمية. و كما يتولى المُعلم هذه الأدوار داخل البيئة الملموسة حسياً و اجتماعياً في المدرسة ، فإن عليه القيام بنفس هذه الأدوار داخل نطاق أمن الانترنت.

لا يحصل المعلم عادة على التدريب أو المعلومات الكافية التي تؤهله بتدريس المبادئ الأساسية و قواعد الأمن على الانترنت ، خلافاً لما يحصل عليه من التدريب و التأهيل لتدريس المواد الأساسية مثل الرياضيات والعلوم واللغات.

نُصنف علم أمن الانترنت إلى ثلاثة مواضيع أساسية ، منها:

1. أمن الانترنت
2. الخُلق الحَسن على الانترنت
3. السلامة على الانترنت

تهدف هذه الورشة إلى إعطاء نبذة عن الموضوع الأول وهو أمن الانترنت لمعلميّ المراحل الأساسية من الروضة إلى المرحلة الثانية عشر. لذا فأول ما نبدأ به هو تعريف أمن الانترنت:

أمن الانترنت هو عبارة عن مجموعة من المبادئ والممارسات التي تستهدف تعليم كيفية حماية الحاسوب وأصول المعلومات من التهديدات الكامنة على شبكة الانترنت.

التكنولوجيا في المدارس

دَرَجَ استخدام التكنولوجيا بالحياة اليومية داخل المدارس و خارجها ، حيث نعتمد كثيراً على استخدام الآلات التقنية المتعددة. و نجد أن معظم التكنولوجيا التي نستخدمها للاتصالات متصلة بالانترنت – وهذه الشبكة أو بالأحرى الشبكات العالمية تحدد المفهوم العام عن تصورنا بما ينمّ عليه "الفضاء الإلكتروني".

فإن الانترنت (الشبكات الالكترونية) عبارة عن شبكة عالمية تصل بين أكثر من بليون شخص و أكثر من ستة مئة مليون حاسوب. و أكثر من مئة بلد بالعالم متصلين من خلال تبادل البيانات و الأخبار و الآراء.[1]

لا شك أنك تعرف العديد من الآلات التقنية المتصلة بالانترنت ، و المستخدمة من قِبل المعلمين داخل وخارج المدرسة. نذكر منها:

- الحاسوب ، وذلك من أجل
  - التصفح
  - البريد الإلكتروني
  - المنتديات الإلكترونية
  - الرسائل الإلكترونية
  - برامج تعليمية على شبكات الانترنت
  - البرامج الإعلامية
- أجهزة المعلومات الشخصية (PDA) ، وذلك كوسيلة

[1] www.internet.com (translated from)

- لتبادل البيانات
- لتبادل الاتصال الصوتي
- لتبادل الاتصال الصوري و الإعلامي
- لتحديد الموقع الجغرافي عالمياً

- الهواتف الخلوية ، وذلك كوسيلة
  - لتبادل البيانات
  - لتبادل الاتصال الصوتي
  - لتبادل الاتصال الصوري و الإعلامي
  - لتحديد الموقع الجغرافي عالمياً

- الخطوط (الكوابل) الإلكترونية للقنوات المرئية ، و تقنية صحن التقاط موجات القنوات الفضائية (Dish).
- آلات السحب المالية ، بطاقات الاعتماد المالية ، و بطاقات ائتمان البنوك.
- برامج النظام العالمي لتحديد المواقع جغرافياً

"و لكنها ليست مهمتي – فسلامة الحاسوب من مسؤولية العاملين بقسم التقنيات بالمدرسة!"

كثيرٌ من المعلمين يختبئون خلف هذه الذريعة لإعفاء أنفسهم من مسؤولية تدريس و تطبيق الاستخدام الآمن للحاسوب داخل الصفوف. بغض النظر عن ما نتمناه ، فإن أمن الانترنت ليس مقتصراً فقط على المدرسين و العاملين على التكنولوجيا. حالياً في العالم ، جميع العاملين في المدارس عليهم إدراك ماهية الممارسات الآمنة للانترنت ، و الالتزام بالمبادئ الأساسية لخلق جو آمن للطلاب، و المعلمين ، والعاملين ، و لحماية ممتلكات المدرسة. كذلك فإن مدرسين المواد الأساسية يمكنهم أن يُشمِلوا جوانب من مبادئ أمن الانترنت بخططهم التعليمية.

و كمربيّ ، فإن من المهم فهم طبيعة و أسباب الأخطار الكامنة على الانترنت ، وآثارها المحتملة ، و الحلول المُتاحة لحماية نفسك و طلابك و المدرسة التي تعمل بها. و كمعلم ، فتمكنك من معرفة علم أمن الانترنت ، يُسهّل عليك وبشكل طبيعي مشاركتك لهذه المعرفة مع الآخرين و ذلك بتدريسها لطلابك و زملائك و عائلاتهم.

أخطار الانترنت

هناك بعض الفئات الرئيسية التي سنُدرجها من أخطار الانترنت للمعرفة و لتعليمها طلابك. و تشمل:[2]

أ. القرصنة – عبارة عن استخدام غير قانوني لحق التأليف مثل سرقة المؤلفات أو التنزيل غير القانوني للموسيقى ، الأفلام ، الكتابات ، أو غيرها من الملفات
ب. الاقتحام – عبارة عن محاولات لأشخاص غير مصرح لهم اقتحام أنظمة الحاسوب لسرقة المعلومات ، إفساد للملفات ، مشاهدة البيانات بطريقة غير شرعية ، أو بهدف السيطرة على الحاسوب
ت. سرقة الهوية – دخلاء على الحاسوب بهدف سرقة البيانات الشخصية لإرتكاب الغش او السرقة
ث. السلوك الوحشي – سلوك على الانترنت يستهدف بعض البيانات الالكترونية من أجل السرقة أو التدمير
ج. الجرثومة - شفرة مبرمجة تنتشر بإعادة نسخ نفسها على برامج أخرى و وثائق مخزنة
ح. الفيروس المتكرر - هي برامج آلية المضاعفة ترسل رسائل إلى العديد من مستخدمي الحاسوب ، و القوائم البريدية ، و البريد الالكتروني للمجموعات
خ. الدودة - برامج خبيثة ذاتية المضاعفة و ذاتية الانتشار
د. حصان طروادة - برنامج خبيث يتخفى كبرنامج ذو مشروعية
ذ. الفيروسات الخبيثة(Malware) – برامج مصممة لزرع الأذى بالحاسوب
ر. برامج التجسس - برنامج ترسل معلومات من حاسوبك إلى طرف ثالث دون علمك أو موافقتك

آثار الأخطار الكامنة على الانترنت

[2] المعلومات تُرجمت من
www.us-cert.gov; www.mysecurecyberspace.com; www.webopedia.com

يمكن لأخطار الانترنت أن تؤثر عليك وعلى عائلتك و طلابك وزملائك بالمدرسة بطرق متعددة. و من الممكن أن يمتد اختلاف العرقلة التي تسببها هذه الأخطار من إفساد ملف أو اثنين ، ومن فيروس واحد بسيط إلى إفساد شامل لشبكة الانترنت بالمدرسة مما يُدمرّ الملفات الهامة المُخزنة على هذه الشبكة.

مما يلي بعض الأمثلة التي تبين إمكانية أن تصبح ضحية (أو سبب بغير عمد) لإحدى أخطار الانترنت و احتمالات نتائجها:

أ. إذا قمت أنت أو أحد طلابك بتنزيل أو توزيع برامج أو مؤلفات (محمية تحت قانون حقوق التوزيع والطبع) عن طريق الانترنت متعمداً أو غير متعمد ، أو حاسوب استخدم تحت إشرافك لتنزيل أو توزيع هذه المؤلفات ، قد يتسبب هذا الاستخدام غير القانوني إلى غرامات مادية ، فقدان العمل ، أو مشاكل مع رجال الأمن (يعتمد على خطورة ما ارتكب من التوزيع أو النسخ). فمثلاً بعض الطلاب بجامعات الولايات المتحدة ممن ينزل أو يوزع ملفات ومؤلفات محمية تحت قوانين حقوق الطبع والتوزيع ، كثيراً ما يُكتشف ما قاموا بارتكابه ، مما يؤدي إلى تغريمهم مادياً و فصلهم من الجامعة. و إذا اكتُشف أن من يقوم بهذه الجرائم هم من طلاب المدارس الثانوية أو أصغر ، مما استخدم حاسوب آبائهم للقيام بهذا العمل غير القانوني فإن آبائهم سيعانون أيضاً من عواقب قانونية.

ب. اقتحام شبكة الانترنت لإحدى المدارس من طرف فرد من داخل المدرسة ("اقتحام داخلي" مثل زميل أو تلميذ) أو من قبل شخص من خارج المدرسة ("اقتحام خارجي") قد يؤدي إلى نتائج سيئة: ممكن أن تشمل تغيير البيانات مثل تغيير علامات الطلبة ، سرقة او تدمير اسئلة الامتحانات ، سرقة معلومات قد تؤدي الى سرقة هوية أي شخص معلوماته محفوظة على شبكة المدرسة ، نسخ أو تدمير أي بيانات خاصة بك أو بالمدرسة.

ت. عند الضغط بالقبول على الشاشات الومضية لإعلانات الانترنت (Pop up) أو فتح الملفات المرفقة المرسلة بالبريد الإلكتروني أو الرسائل الالكترونية المختصرة (IM) , أو على المنتديات الإلكترونية ، قد تتسبب باستلامك لكم هائل من البريد الالكتروني غير المرغوب به (Spam) : بعض الملفات المرفقة أو برامج مختفية داخل الملفات المرفقة قد تسمح لإقتحام العناوين الإلكترونية المخزنة ببريدك الإلكتروني لتبعث ببريد إلكتروني يسمح بإقتحام العنواين المخزنة داخل كل عنوان إلكتروني وصلته هذه الرسالة ، ليكرر عملية إرسال هذه الرسائل أو الأرقام السرية و هكذا. إن الشاشات الومضية لإعلانات الانترنت والملفات المرفقة قد تخفي برامج للتجسس التي تسمح لمقتحم النظر عن بعد على كل ما هو محفوظ داخل جهاز الحاسوب طالما كان الحاسوب موصول بالانترنت.

ث. إذا وصلك و بالخطأ و ساعدت على توزيع كل من الفيروس أو الدودة ، حصان طروادة ، الفيروسات الخبيثة عن طريق الملفات المرفقة ، أو الملفات و الوثائق الحاملة لهذه المخاطر. فمن الممكن أن تنتشر هذه المخاطر إلى وثائق أخرى ، فتغير وتُتلف البرامج ، أو تعطيل نظام التشغيل كله على حاسوبك. هذه الأنواع من التشفيرات الخبيثة يمكن أن تسبب بمحو الوثائق و سرقة البيانات ، واختراق الحاسوب لتعطيله. إن التشفيرات الخبيثة يمكن أن تؤذي شبكة الانترنت للمدرسة و كل حاسب و شبكة انترنت للعناوين الالكترونية المخزنة على شبكة المدرسة.

كيف تقوم بالحماية ضّد مخاطر الانترنت؟

إذاً كيف تقوم بحماية بياناتك ، وحاسوبك ، و بيانات المدرسة و شبكة الانترنت؟ نوصي بما يلي من الممارسات الأساسية للحماية من المخاطر الإلكترونية:

1. **شكل كلمة سّر قوية**. كلمة أو عبارة السّرالقوية تتكون على الأقل من ثمانية مقاطع تحتوي على خليط من الأحرف و الأرقام و الرموز. إن كلمة السر الخاصة بك كمفتاح فريد لمعلوماتك فلا تشارك به زملائك أو أفراد عائلتك. تأكد أن المربع الذي يحثك على أن يحفظ الحاسوب كلمة السّر خالي من التأشير.

2. **اقفل الحاسوب** في المدرسة أو البيت حين تخرج ولو لحين من الغرفة أو عند توقفك استخدام الحاسوب – الحاسوب غير المُقفل دعوة مفتوحة للدخلاء (أو حتى الاطفال الفضولين!) للوصول إلى معلوماتك أو حساباتك. معظم برامج أنظمة التشغيل تسمح لك بتحديد كلمة سر تحثك لإدخالها عند إعادة استعمال الحاسوب متى كانت الشاشة بحالة الركود (Screen Saver).

3. **انشاء حسابات استخدام فريدة لكل من يستخدم حاسوبك**. اذا كنت تتشارك وطلابك واخرين بحاسوب واحد , كما هو الحال داخل الكثير من الفصول , فأغلق حسابك عند توقفك استخدام الحاسوب ووفر لغيرك حسابات عامة لاستخدام الحاسوب. هذه الحسابات ممكن ان ينُشأها أحد موظفي قسم التقنيات (كأنشاء حساب استخدام عام يسمى "تلميذ"), وتحدد الصلاحيات المسموح بها لهذا الحساب

4. **اعتبر دائماً أن لا خصوصية داخل البريد الإلكتروني ، و المنتديات الإلكترونية ، والرسائل الإلكترونية**. فأي شيء ترسله عن طريق الانترنت ممكن للآخرين قراءته أو تغيره ، أو إعادة إرساله إلى أي شخص بأي مكان ، إلا بحالة تشفيرهذه الرسائل أو البريد. تعتبر معظم جوانب الانترنت مُنتدى عام ، مما تسمح بقراءة كل ما تكتبه على طياتها من قِبل الملايين من الناس ، ولا تستطيع محو ما كتبته أبداً مهما حاولت.

5. **خذ الحذر عند فتح أي بريد إلكتروني غير متوقع** . إن أي بريد الكتروني من أفراد لا معرفة لك بهم ، أو بريد إلكتروني غير متوقع من قبل شخص معرف لديك قد يحمل على الأغلب فيروس أو فيروس متكرر. لذا عليك محو هذا النوع من البريد الإلكتروني قبل فتحه و قراءته. إذا اعتقدت أن صديق بعث بهذا البريد غير المتوقع ، فاتصل بهذا الصديق للتأكد أنه هو من بعثه لكَ ، ثم قم بمسح البريد و الملفات المرفقة به من الفيروسات قبل فتحه. و اعلم أنه من الممكن أن تحدد عمل برنامج ضّد التجسس الذي تستخدمه ليقوم بفحص تلقائي لأي بريد أو مرفقات إلكترونية عند استلامها.

6. **اعد مراجع مؤمنة لبياناتك**. أعّد مراجع مؤمنة لملفاتك و معلوماتك وبرامجك ومراجعك الهامة , ولأي تغير تُحدثه على أي معلومات داخل هذه المراجع والملفات (على الأقل مرة اسبوعياً). واحتفظ بهذه المراجع بمكان آمن.

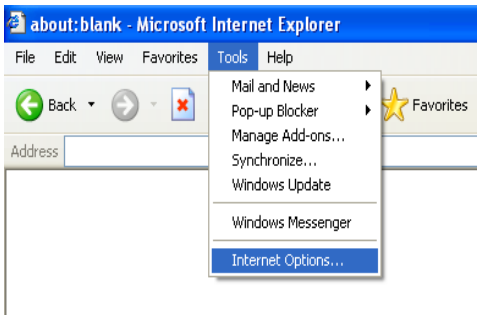
7. **احذر من استخدام الملفات المشتركة أو مشاطرة استخدام حاسوبك مع الآخرين**. إن الملفات المشتركة تعمل على السماح لآخرين عن طريق الانترنت من تنزيل الملفات بين حاسوب و آخر(يسمى أيضاً "زميل لزميل Peer to Peer [P2P]"). الملفات المشتركة تسمح لك من تنزيل الملفات و تبادل البيانات. إلا أن السماح بإستخدام الملفات المشتركة من حاسوبك إلى آخر ، يعرضك لنفس المخاطر التي تواجهها عند دخول أحدهم من بعد إلى ملفاتك ، حيث يمكن نشر الفيروسات بملفاتك وحاسوبك عن قصد أو غير قصد.

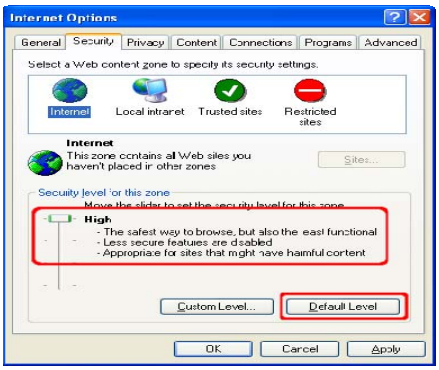
8. **قم بتحديث تعريفات برامج ضّد الفيروسات و ضّد التجسس**. إن برامج ضّد الفيروسات و برامج ضّد التجسس تقوم بمسح كامل للبيانات والملفات الموجودة على حاسوبك بحثاً عن أي نمط ينم على وجود عدوى. لذا فمن المهم تحديث هذه البرامج بإستمرار لتحتوي على آخر تعريفات للشفرات الفيروسية والتجسسية لتتمكن من التنبه والقضاء عليها إن وجدت. الكثير من برامج ضّد التجسس و ضّد الفيروس تسمح لك بتحديد قيامها بتزيل أحدث التعريفات تلقائياً و القيام بمسح الحاسوب بانتظام.

9. **قم بإستخدام و صيانة الحائط الناري**. يعمل الحائط الناري كحارس يمنع عبور ما هو خطر من الملفات، و الطلبات ، و البرامج إلكترونية إلى حاسوبك. كما ويمكنك تحديد الحائط الناري ليمنع الوصول إلى صفحات إلكترونية معينة و يسمح الوصول لغيرها.

10. **حدد محركات البحث المستخدمة إلى أعلى درجة أمنية**. يمكنك أن تحدد محركات البحث Internet Browser التي تستخدمها إلى درجة أمنية عالية لتمنع الوصول إلى الصفحات الالكترونية غير المرغوب بها. (اعلم أن اختيارك لدرجة أمنية عالية قد يقلل من بعض وظائف المحرك إذا كانت

الصفحات الالكترونية تعتمد بعرض المعلومات على برامج مثل جافا Java أو فلاش Flash أو برامج تعزز من خصائص العرض). إذا كنت تستخدم محرك البحث اكسبلورار Internet Explorer ، فيمكنك تحديد أعلى درجة أمنية بالضغط على "أدوات Tool" المجودة بقائمة العرض للمحرك ثم اضغط على "خيارات الانترنت Internet Options". التي تأخذك إلى شاشة صغيرة تحتوي على قائمة تسمح لك تحديد الدرجة الامنية من "منخفضة Low" أو "وسط Medium" أو "مرتفعة High" , عليك اختيار الدرجة المرتفعة (انظر إلى الصور التوضيحية التالية)[3]





11. **اسمح بعمل أداة منع "الشاشات الومضية pop-up"**. إذا كنت تستخدم محرك البحث اكسبلورار ، فعليك الضغط على الخيار "أدوات Tools" بقائمة العرض ، عندها تجد بالقائمة التي تهبط أمامك خيار "منع الشاشات الومضية pop-up blocker" ، اضغط عليه و اختر السماح للآداة بالعمل لمنع الشاشات الومضية بالظهور عند قيامك بالبحث على صفحات الانترنت.

12. **افصل حاسوبك عن الانترنت عند توقفك استخدامه**. بعض أنواع الفيروسات الخبيثة "Malware" مبرمجة لتقم بتدمير الحاسوب عند إغلاق حسابك كمستخدم ، إلا ان الحاسوب لا زال متصلاً بالانترنت. غيرها مبرمج ليقوم بـإجراءات خبيثة عندما يكون الحاسوب بوضع الركود.

13. **الزم الحذر عند فتحك للملفات المرفقة ببريد إلكتروني ، أو المنتديات الالكترونية ، أو الرسائل الخلوية.** إن الملفات المرفقة ممكن أن تحتوي على فيروسات أو ديدان ، أو برامج التجسس ، لذا عليك القيام بمسحها قبل فتحها. و نكرر التحذير من فتح الملفات المرفقة المبعوثة من أشخاص لا معرفة لك بهم ، أو تحمل أسماء وعناوين غير مفهومة.

14. **قم بتزيل تحديثات على حاسوبك بأحدث الرقع الامنية لنظام التشغيل والبرامج المستخدمة**. إن شركات البرامج الإلكترونية و أنظمة التشغيل تقوم باستمرار إصدار تحديثات تسمى بالرقع " Patches" لتصحيح الثغرات ببرامجها. هذه الرقع تقوم بتصليح المشاكل الموجودة على أنظمة التشغيل ، محركات البحث ، أو برامج الحاسوب. بعض الشركات تُصدر بشكل منتظم رقع أمنية ، على سبيل المثال فإن شركة ميكروسوفت تصدر تحديثات شهرية. يمكنك تحديد أنظمة التشغيل لتقوم بتنزيل التحديثات للرقع الأمنية تلقائياً. حافظ على زيارة موقع الشركات الصانعة لنظام التشغيل الذي تستخدمه ، أو محركات البحث مثل شركات ميكروسوفت و آبل Apple. كما يمكنك زيارة موقع كيوسيرت Q-CERT لتجد معلومات عن الرقع الأمنية و الثغرات للحاسوب و أنظمة التشغيل.

[3] هذا التوضيح بالصور مأخوذ من الموضوع " Securing your Web Browser" المعروض على صفحات http://us-cert.gov/reading_room/securing_browser/

الآن بعد أن أصبح لديكم معلومات عن أمن الانترنت ، كيف تستطيع كمدرس تعليم أمن الانترنت لطلاب فصلك؟ (للتدريب, اعتبر نفسك مدرس أدب عربي).

مثال: إن موضوع درسك اليوم عن الشعر الجاهلي ، و تحديداً عن امرؤ القيس. كنشاط مدرسي ، تطلب من طلاب فصلك جمع معلومات عن الفترة التي عاش بها امرؤ القيس ، وعن القصة التي ألهمته بقصد أشهر و أول معلقة بتاريخ الشعر العربي. و للبحث تطلب من الطلاب استخدام معمل الحاسوب بالمدرسة أو البحث بإستخدام الحاسوب بالبيت كواجب مدرسي لتسليمه بالحصة القادمة. وتدون بوثيقة النشاط مبادىء توجيهية لموضوع البحث ، خلالها يمكنك أن تضيف فقرة على الأقل عن مبادئ النسخ والطبع والتوزيع ، مع اثنتين أو ثلاثة من الإرشادات للتمييز بين المواقع الموثوق بها.

المراجع

www.qcert.org
www.us-cert.gov
www.mysecurecyberspace.com
www.webopedia.com
www.internet.com
www.csialliance.org

Copyright Q-CERT 2007