مفهوم أمن ألانترنت

Q-CERT - ورشة تعليمية لطلاب المراحل الاعدادية والثانوية

ict QATAR

Q-CERT

Copyright Q-CERT 2007

أعداد ؛ وئام يونس

ماذا يعني أمن الانترنت ؟

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

الجرائم الإلكترونية و المخاطر الأمنية

الجريمة الإلكترونية عبارة عن سلوك إجرامي أو غير قانوني تم تسهيله باستخدام الحاسوب. هذا السلوك يشمل سلوك غير قانوني متعمد لإيذاء الناس ، مثل التحرش الالكتروني أو الملاحقة الالكترونية ، إلى استخدام البرامج الخبيثة أو استغلال نقاط الضعف عند المستخدم او البرامج الالكترونية لسرقة الممتلكات مثل بطاقات الائتمان أو بيانات الهوية الشخصية.
الجرائم الالكترونية تشمل أيضاً الغش أو التدمير المتعمد للبيانات الإلكترونية الكامنة على جهاز الحاسوب الشخصي أو الشبكة الإلكترونية.

الجرائم الإلكترونية تشمل ايضاً:

1. **القرصنة** (Piracy) – عبارة عن استخدام غير قانوني لحق التأليف مثل سرقة المؤلفات أو التنزيل غير القانوني للموسيقى ، الأفلام ، الكتابات ، أو غيرها من الملفات.

2. **الاقتحام**(Intrusion) – عبارة عن محاولات لأشخاص غير مصرح لهم اقتحام أنظمة الحاسوب لسرقة المعلومات ، إفساد للملفات ، مشاهدة البيانات بطريقة غير شرعية ، أو بهدف السيطرة على الحاسوب.

3. **سرقة الهوية** (Identity theft)– دخلاء على الحاسوب بهدف سرقة البيانات الشخصية لإرتكاب الغش أو السرقة.

4. **السلوك السلبي** (Predatory behavior)– سلوك على الانترنت يستهدف الوصول إلى بعض البيانات الالكترونية بطرق مختلفة من أجل السرقة أو التدمير.

5. **الجرثومة أو الفايروس** (Virus) - شفرة مبرمجة تنتشر بإعادة نسخ نفسها على برامج أخرى ووثائق مخزنة.

6. **الفيروس المتكرر** (Spam)- هي برامج آلية المضاعفة ترسل رسائل إلى العديد من مستخدمي الحاسوب ، و القوائم البريدية ، والبريد الإلكتروني للمجموعات.

7. **الدودة** (Worm)- برامج خبيثة ذاتية المضاعفة و ذاتية الانتشار.

8. **حصان طروادة** (Trojan horse)- برنامج خبيث يتخفى كبرنامج ذو مشروعية.

9. **الفيروسات الخبيثة**(Malware) – برامج مصممة لزرع الأذى بالحاسوب.

10. **برامج التجسس** (Spyware) - برنامج يرسل معلومات من حاسوبك إلى طرف ثالث دون علمك أو موافقتك.

خطورة الجرائم الإلكترونية!

كل من يرتكب الجرائم الالكترونية قد يواجه مجموعة من العواقب السلبية والخطيرة. يمكن أن تنتهي إما في السجن ، أو مواجهة إجراءات قانونية ، أو يجد نفسه مطالب من قِبل الهيئات القانونية دولياً أو وطنياً. وقد يواجه أيضاً خسائر مالية ويُنبذ اجتماعياً.

نصائح للسلوك السليم لِمُستخدم الانترنت

احمي نفسك وعائلتك على شبكات الانترنت

1. **شكل كلمة سّر قوية** - فإن كلمة السّر تسمح بالعبور المؤمن إلى المعلومات و البيانات الشخصية , بالضبط مثل الدخول إلى البيت باستخدام المفتاح. لذا استخدم كلمة سّر أو جملة سرّ يسهل عليك تذكرها و تغيرها. كلمة السر القوية تتكون على الأقل من ثمانية مقاطع تحتوي على حروف و أرقام وعلامات مثل علامات الترقيم.

2. **لا تنشر معلوماتك وصورك الخاصة على شبكات الانترنت** – إذا قمت بنشرها فكأنك تنشرها على لافتة كبيرة بسوق مكتظ بألوف أو ملايين من الناس لقرائتها. لذا حافظ على بياناتك الشخصية لنفسك, لحماية هويتك و خصوصياتك و عائلتك من اللصوص والمتربصين.

3. **لا تقم بالترتيب للمقابلة شخصياً** – إن المتربصين و المجرمين على شبكات الانترنت سيحاولون خداعك لمقابلتهم شخصياً بإيهامك أنهم أصدقاء يهمهم أمركَ. فخذ حذرك بعالم مجهول لديك كالمثل القائل " لا تكن كالحمل في وكر الذئاب".

4. **اعتبر دائماً أن المعلومات التي تقرأها أو تسمعها على الانترنت غير صحيحة** (إلا اذا كان ناشر المعلومات هيئة موثوق بها) – فإن الكثير من الناس يكتب وينشر معلومات غير صحيحة, لنشر الاشاعات, وتلفيق القصص, وتغيير الصور, وتولي شخصيات مزيفة. من الأرجح إنك لن تصدق أو تثق بأي شخص أو قصة يدليها عليك من يدق على بابك, إذا لمَ تصدق و تثق بأي كان على الانترنت؟

5. **كلم أحداً من الكبار إذا شعرت بعدم الراحة أو الخوف من أي شيء تراه أو تسمعه على شبكات الانترنت** – استخدم نفس الطرق التي تتبعها بعدم السماح لأي كان من التحرش بك ومضايقتك داخل المدرسة أو الحيّ, على شبكات الانترنت. وأخبراحد من المدرسين بمدرستك أو والديك, عند قرائتك أو سماعك أي شيء غير مريح, أو مُخيف, أويُشعرك بالغضب.

6. **شجع أفراد عائلتك لفصل حسابات المستخدمين** - إن كل منا يحب ان تكون لديه غرفة خاصة به أو زاوية خاصة بالغرفة التي يتشارك بها جميع افراد العائلة, وذلك لحفظ ما يخصنا, فالآباء يحتفظون بالوثائق الهامة بمكان مُقفل. هذا السلوك علينا جميعاً الاقتداء به عند حفظ معلوماتنا الخاصة مثل المُذكرات, وبيانات حسابات البنوك, أو أي من البيانات الهامة.

7. **شارك عائلتك بما تعرفه عن علم أمن الانترنت** – قد يكون الكثير منكم على معرفة أوسع بعلم الحاسوب و أمن الانترنت من والديه أو إخوته, لذا خذ بعضاً من الوقت لتعليمهم كيف يحمون أنفسهم وبياناتهم من مخاطر الانترنت.

احمي بياناتك

1. **اعتبر دائماً أن بريدك الإلكتروني** و مناقشاتك على المنتديات الإلكترونية , **ورسائلك الالكترونية تُقرأ على الجمهور** فمعظم صفحات الانترنت كمنتدى عام يمكن قراءة أي ما ينشر عليها من قِبل الملايين من غير استطاعة محوه.

2. **أخذ الحذر عند فتح البريد الالكتروني** – إن البريد الالكتروني من قِبل أشخاص لا تعرفهم , أو خطاب إلكتروني غير متوقع من أشخاص تعرفهم, يحمل على الأغلب فيروسات و فيروس متكرر. لذا احذف هذا النوع من البريد قبل فتحه . واذا اعتقدت أن صديقاً بعث لك بخطاب إلكتروني غير متوقع فأتصل به قبل فتح البريد.

3. **أعدّ مراجع مؤمنة لبياناتك** – احفظ جميع ملفاتك و معلوماتك و برامجك الهامة بمراجع إلكترونية كل مرة تُحدث أي تغيير عليها (على الأقل مرة اسبوعياً). احتفظ بهذه المراجع بمكان آمن.

4. **خذ الحذر من استخدام الملفات المشتركة أو استخدام الحاسوب مع الآخرين** - الملفات المشتركة عبارة عن ملفات تسمح للعديد من المستخدمين تنزيل ملفات عن طريق الانترنت من حاسوب إلى آخر (تسمى احياناً [Peer 2 Peer] زميل لزميل). هذه الملفات المشتركة تسمح لك بتنزيل الملفات من حاسوب أشخاص آخرين الى حاسوبك , كما وتسمح لهم الدخول إلى حاسوبك وبياناتك للنظر اليها وتنزيل ما يحلو لهم من البرامج والبيانات الكامنه على حاسوبك .

5. **لا تشارك كلمة السّر مع أحد** – هل تشارك مفتاح بيتك مع اصدقائك؟ إذا كان الجواب بلا, إذا لما تشارك معهم كلمة السّر؟

احمي ممتلكاتك

1. **قم بتحديث برامج مكافحة الفيروسات و برامج مكافحة التجسس** – برامج مكافحة الفيروسات و برامج مكافحة التجسس تقوم بمسح الملفات المخزنة بذاكرة الحاسوب عن أنماط تنم عن عدوى و خلل. لذا من المهم تحديث برامج مكافحة الفيروسات و التجسس للحصول على التعريفات الحديثة للفيروسات وبرامج التجسس الموجودة على الحاسوب.

2. **استخدام وصيانة برامج الحائط الناري** – الحائط الناري كالحارس لا يتيح لأي من الملفات والطلبات و البرامج الخطرة من الوصول إلى حاسبك, ويسمح لمرور ما هو المناسب من الدخول والخروج إلى حاسبك. يمكنك تحديد الحاجز الناري لمنع الوصول إلى بعض المواقع والسماح الوصول لغيرها.

3. **افصل الحاسوب عن الانترنت عند عدم إستخدامه** – بعض أنواع الفيروسات الخبيثة مُبرمجة لتدمير حاسوبك عند توقفك استخدام الحاسوب مع أن حاسوبك لا زال متصل بالانترنت. وغيرها يُحرك الخبيث من حين يكون الحاسوب ساكناً.
4. **اتخذ الحذر عند فتح الملفات المرفقة التي تصلك عن طريق البريد الإلكتروني, أو المنتديات الإلكترونية, أو رسائل الهاتف الخلوي** – الملفات المرفقة يمكن أن تحتوي على فيروسات, ديدان, برامج تجسس, لذا عليك مسح الملفات المرفقة قبل فتحها. ولا تفتح ملفات مرفقة بُعثت من قبل أشخاص لا تعرفهم أو تحمل عناوين أو أسماء لا معنى لها.

5. **أنزل أحدث الرقع و التحديثات الأمنية الالكترونية إلى أنظمة الحاسوب بتكرار**- إن الكثير من الشركات المنُتجة لبرامج و أجهزة الحاسوب تصدر باستمرار تحديثات للثغرات ببرامجها. هذه التحديثات تصحح ما وجد من المشاكل الأمنية الموجود بأنظمة التشغيل, أو الصفحات الالكترونية, أو البرامج. بعض الشركات مثل مايكروسوفت تُصدر تحديثات بشكل مُنتظم مرة كل شهر. لذا ننصحك بتفقد الصفحات الالكترونية للشركات الصانعة بأنظمة التشغيل أو الصفحات الالكترونية مثل مايكروسوفت و آبل. كما يمكنك زيارة صفحات كيوسيرت (Q-CERT) لتجد المعلومات اللازمة عن تحديثات أمن الانترنت و الثغرات المعلن عنها.

المراجع:

www.qcert.org
www.cert.org
www.mysecurecyberspace.com
www.us-cert.gov

- Security Tips for Non-Technical Users (http://www.us-cert.gov/cas/tips/)
- "Home Computer Security" (http://www.us-cert.gov/reading_room/HomeComputerSecurity/)

www.netsmartz.org

Copyright Q-CERT 2007