

المحاضرة الثامنة

الفصل الثالث : أضرار وجرائم شبكة الانترنت (Damages and Crimes of Internet)

❖ طرق الحماية من مخاطر وجرائم الانترنت .

في الحقيقة هناك العديد من وسائل الحماية التي يمكن استخدامها في تجنب المخاطر وجرائم شبكة الانترنت ومنها :-

- ١- اذا قررت الاشتراك بخدمة الانترنت فلا بد ان يسبق هذا القرار تحديد الهدف الاساس من الاشتراك بخدمة الانترنت ، وماهي الاستخدامات العامة التي من الممكن استخدامها لشبكة الانترنت ؟
 - ٢- امتلاك المعلومات والمعرفة الكافية حول كيفية التعامل مع المواقع المتنوعة على شبكة الانترنت ، وذلك من خلال اخذ بعض الدورات المتخصصة في مجال تكنولوجيا المعلومات مثل "ICDL" او "C3"، أو من خلال الاطلاع والدراسة ، لان الجهل بكيفية الاستخدام يعد من أكثر الأسباب التي تؤدي إلى التعرض للجرائم والمخاطر .
 - ٣- تقول العبارة "درهم وقاية خير من قنطار علاج" ، بناءً عليه يتوجب على كل مستخدم لشبكة الانترنت ان يبتعد عن ارتياد المواقع المشبوهة سواء أكانت مواقع اباحية او سياسية او مواقع معادية للدين او مواقع للعب القمار والالعب المؤذية للأخلاق ، او المواقع الخاصة بالزواج او مواقع الدردشة العامة وغيرها من المواقع التي يشتبه بها .
 - ٤- استخدام كلمات مرور Passwords لجهازك الشخصي ولبقية الحسابات الشخصية ، واحصر على ان لا تطلع احد على كلمة المرور وخاصة للأشخاص الأقرب اليك ، بالإضافة الى عدم كتابة كلمة المرور على الجوال او على جهازك الشخصي ، وان لا تكون كلمة المرور متعلق بك (اسمك ، تاريخ الميلاد ، الهوايات ، اسماء الابناء الخ) وكلما كانت الكلمة اكبر ومتنوعة (أرقام وحروف) صعبت عملية الحصول عليها او اختراقها ، ويفضل بعدم استخدام نفس الكلمة لعدة حسابات ، ويفضل ايضاً بتغيير كلمة المرور بشكل دوري .
 - ٥- عدم إعطاء أية معلومات خاصة بك (الاسم ، العنوان ، صور ، أفلام ، وثائق ، أرقام البطاقات الائتمانية) لأي جهة تتواصل معها عن طريق المجموعات الإخبارية او الدردشة او المنتديات او البريد الالكتروني ، إلا إذا كنت متأكداً من هوية الطرف الذي تتواصل معه . وفي بعض الأحيان يمكنك استخدام بعض المعلومات الوهمية والأسماء المستعارة "Nickname" في الدردشة او المنتديات و ساحات الحوار . بمعنى أكثر دقة " فكر قبل أن ترسل "
 - ٦- التعرف عن طريق الدردشة او المنتديات لا يوفر لك اية وسيلة حقيقية لمعرفة الشخص الموجود على الطرف الاخر ، حيث يحاول الطرف الاخر استخدام كافة الاساليب والوسائل لاستدراجك من خلال عبارات الحب والغرام والصداقه او عبارات الدين او ارسال بعض الصور التي لا تكون له في الاساس ، لذلك احصر على إتباع التعليمات التالية :
- ٦-١- حاول قدر المستطاع على عدم قبول أية دعوة للانضمام للدردشة إلا إذا كنت تعرف الجهة التي قامت بإرسال الدعوة إليك .
 - ٦-٢- عدم مواعدة اي شخص تعرفت عليه عن طريق الدردشة او المنتدى او الايميل وخاصة في اماكن غير عامة .
 - ٦-٣- عدم التلطف بكلمات مخلة بالأدب والدين .

٦-٤- عدم إرسال أية معلومات خاصة بك (معلومات السكن ، رقم الجوال ، صور وأفلام شخصية) لان ذلك قد يعرضك للابتزاز

٦-٥- ضرورة ارتداء ملابس محتشمة إثناء التواصل مع الآخرين ، حيث ان بعض برامج المحادثة الفورية تمتلك صلاحيات تسجيل المحادثة ، او قد يقوم الشخص بالطرف الأخر من تسجيل المحادثة بالصوت والصورة .

٦-٦- الحرص على ضرورة استخدام اللغة العربية الفصحى في المحادثة او في إدراج تعليق في المنتديات او في المواقع الاجتماعية

٧- يعد الایمیل E-mail من أكثر الوسائل المستخدمة من قبل مجرمی الانترنت للوصول الى الضحية لذلك يجب عليك التقيد بالتعليمات التالية حتى لا يلحق بك ضرر من قبل الایمیل وهي :-

٧-١- لا تفتح اي ایمیل مرسل اليك من قبل شخص غير معروف ، والتي في بعض الاحيان تحمل عناوين مميزة

(you are the best friend ; I love you ; I miss you ; You win) واغلب هذه الایميلات تصل الى صندوق Spam

٧-٢- لا تفتح اي ملف مرفق مع رسالة من شخص مجهول ، حتى وإن ظهر أنه ملف نصي أو صورة لا تحمل فيروساً ، لأنه يمكن التلاعب باسم الملف ليظهر الملف الذي يحمل فيروساً بمظهر ملف يحمل صورة أو نص .

٦-٣- لا تفتح اي ملف مرفق مع رسالة من شخص معروف الا إذا كنت تتوقع ذلك الملف ، وإذا كنت شاكاً في سلامة الملف يمكنك التحقق من صديقك بأي طريقة اتصال ، اسألها ارسال رسالة بريدية الكترونية استفسارية .

٦-٤- افحص اي ملف تريد تحميله (سواء من احدى وسائط التخزين او الایمیل او مواقع ويب) لجهازك بواسطة برنامج مكافح الفيروسات للتحقق من خلوه من التهديدات المحتملة .

٦-٥- لا تقم بإرسال او تمرير اية رسالة قبل التأكد من محتوياتها والتأكد من خلوها من الاضرار المعنوية او المادية .

٨- تعد الفيروسات باختلاف اشكالها من اكثر المخاطر انتشارها على شبكة الانترنت ، وتعتمد طريقة المعالج من الفيروس على نوع وتأثير ذلك الفيروس ومن طرق المعالجة ما يلي :-

٨-١- استخدام احدى البرامج التجارية لمكافحة الفيروسات Antivirus ومنها

Kaspersky Internet Security 2011– Microsoft Security Essentials – Bitdefender – AVG
Anti-Virus – Avast

٨-٢- استخدام احدى البرامج المجانية لمكافحة الفيروسات Antivirus ومنها

MacAfee– Avira – Nod32

٨-٣- عند تنزيل برنامج Antivirus على جهازك تأكد من عمل خاصية المراقبة المباشرة ، وذلك لكشف الفيروسات حال دخولها الى الجهاز .

٨-٤- تأكد من تحديث برنامج Antivirus بشكل دوري ، وذلك لكشف الفيروسات الجديدة .

٨-٥- فحص ملفات الجهاز بشكل دوري .

أشهر مضادات الفيروسات Antivirus لعام ٢٠١٢ .

2012 Compare The Best Antivirus Software Products										
Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
★★★★ Excellent ★★★★ Very Good ★★★ Good ★★ Fair ★ Poor	Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Panda Antivirus Pro	F-Secure Anti-Virus	AVG Anti-Virus	Avast! Pro Antivirus	G-Data AntiVirus	BullGuard Antivirus	Avira AntiVir Premium	ESET NOD32 Antivirus
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
Overall Rating	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Ratings										
Performance	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Features	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Help & Support	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★

٩- الحماية من البرامج التجسسية كأحصنة طروادة Trojan Hours او Spyware نتبع ما يلي :-

٩-١- تحميل برنامج جدار الحماية Firewall وهو عبارة عن برنامج يقوم بفحص كافة الرسائل التي تصل الى جهاز المستخدم من الانترنت من خلال التأكد من ان هذه الرسائل تحقق الشروط التي تم تحديدها المستخدم الذي يدير جدار الحماية . حيث أن برامج الحماية Antivirus تستطيع ان تكشف جزءاً من البرامج التجسسية ولكن ليس جميعها ، لذا يلزمك ذلك من تحميل برامج جدار الحماية ومن هذه البرامج ماييلي :

ZoneAlarm PRO Firewall – F-Secure Internet Security 2011 – Panda Firewall - Global Protection 2011 – Net Firewall 2011 - ESET Smart Security 4 - Firewall

٩-٢- اذا تم اكتشاف اي حصان طروادة او برامج تجسسية Spyware من خلال هذه البرامج يجب عليك ان تقوم باستبدال كلمات المرور المسجلة على جهاز والتي يمكن ان تكون قد سرقت من قبل المهاجم واجراء فحص لملفات الجهاز باستخدام برنامج Antivirus تحسباً من ان يكون المهاجم قد زرع فيروساً في جهاز .

أشهر مضادات البرامج التجسسية Anti-spyware لعام ٢٠١٢ .

2012 Best Anti-Spyware Software Comparison and Reviews										
Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
★★★★ Excellent ★★★★ Very Good ★★★ Good ★★ Fair ★ Poor	Webroot Secure Anywhere Antivirus	STOPzilla	Spyware Doctor	Ad-Aware Pro	PC Spyware Protection	Malwarebytes Anti-Malware	SUPER Anti-Spyware Professional	SpyHunter	ZeroSpyware	SpyZooka
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
Overall Rating	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Ratings										
Ease of Setup/Use	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Detection Effectiveness	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Removal Effectiveness	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
System Performance	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Scan Performance	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Support/Documentation	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★

١٠ - الحماية من البرمجيات الخبيثة Malware وهي اختصار لكلمتين هما malicious software وتعني البرمجيات الماكرة أو الخبيثة، وهي برنامج مخصص للتسلل إلى أجهزة الحاسب لتدميره بدون رضا المستخدم . وما إن يتم تثبيت البرمجية الخبيثة فإنه من الصعب جداً إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح أذاها من إزعاج بسيط (بعض النوافذ الإعلانية الغير مرغوب بها خلال عمل المستخدم على الحاسب متصلاً أم غير متصلاً بالشبكة) إلى أذى غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرمجيات الخبيثة .

أشهر مضادات البرامج الخبيثة Anti- Malware لعام ٢٠١٢

2012 Best Anti-Malware Software Comparisons and Reviews										
Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
	BitDefender Antivirus Plus	Malwarebytes Anti-Malware	Norton AntiVirus	ClamAV	Webroot SecureAnywhere Antivirus	Kaspersky Anti-Virus	ESET NOD32 Antivirus	Avast! Antivirus	Avira AntiVir Desktop	Avast! Pro Antivirus
										
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
Overall Rating	\$29.95	\$24.95	\$39.99	\$24.95	\$39.95	\$59.95	\$39.99	\$29.95	\$29.95	\$39.95
Ratings										
Malware Protection	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Malware Detection	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Malware Removal	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Ease of Use	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
Support and Documentation	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★

١١ - الحماية من الاعلانات الفقاعية او المنبثقة Popup التي تخرج بين الحين والآخر كإعلانات أثناء تصفح الانترنت ، وقد تحتوي هذه الاعلانات على المشاركة في اللعب ، او الدخول الى مسابقات او التهنة بحصولك على فيزا لحدى الدول الخ ، وافضل وسيلة حماية من هذه الاعلانات عدم فتحها واغلاقها بشكل مستمر ، بالإضافة الى انه يمكنك تعطيل هذه الاعلانات من خلال متصفح الانترنت .

١٢ - التأكد من عدم تشغيل كاميرا الويب دون إذن منك ، علما بأن كل كاميرا مزودة بضوء صغير يشير الى تشغيلها ، ولكن مع انشغال المستخدم في تصفح المواقع الالكترونية او عدم وجوده خلف الجهاز قد لا ينتبه الى تشغيل الكاميرا من قبل احد المخترقين او المتطفلين ، لذلك ينصح بوضع لاصق على الكاميرا او ازالته اعداداتها من نظام التشغيل .

١٣ - عمل نسخة احتياطية لكافة الملفات الموجودة على جهازك الشخصي Backup وذلك خوفا من تدمير الملفات والبرامج من قبل احد المهاجمين ، كما ويفضل بعد الاحتفاظ بمعلومات سرية او خاصة (ارقام الحسابات للبطاقات الائتمانية ، العنوان الخاص بالمستخدم ، صور وافلام عائلة) على الجهاز المراد ربطه بشبكة الانترنت ، ويفضل حفظ هذه المعلومات على وسائط تخزين خارجية .

١٤ - العمل على وضع أجهزة الحاسب في أماكن عامة داخل المنزل .

١٥ - مراجعة سجل الزيارات History والعناوين المحفوظة في برنامج مستكشف الانترنت Internet Explorer

١٦ - القيام بإدارة المحتوى لبعض المواقع Content، باستخدام الأوامر الخاصة بذلك والموجودة ببرنامج Internet Explorer.

١٧ - القيام بحظر بعض المواقع من خلال برنامج Internet Explorer.