
القرصنة الألكترونية

أصبح الولوج إلى عالم الهاكرز حلماً يسعى إليه الكثير من الشباب، وأصبحت مواضيع التجسس الإلكتروني تستحوذ على اهتماماتهم، وأصبحت شبكة الإنترنت ميداناً لصراعات من نوع جديد حملت كل أدوات التدمير الإلكتروني كالتجسس والاختراق وتدمير المواقع الإلكترونية الحكومية وغير الحكومية، والتحكم في تغيير قواعد بيانات قد تصل في خطورتها إلى تهديد الأمن القومي لبعض الدول، مما دفع بعض خبراء الإنترنت للاعتقاد أن الشبكة العنكبوتية أصبحت على حافة الانهيار، ولخص آخرون ما يحدث بقولهم: إن التكنولوجيا يأكل بعضها بعضاً.

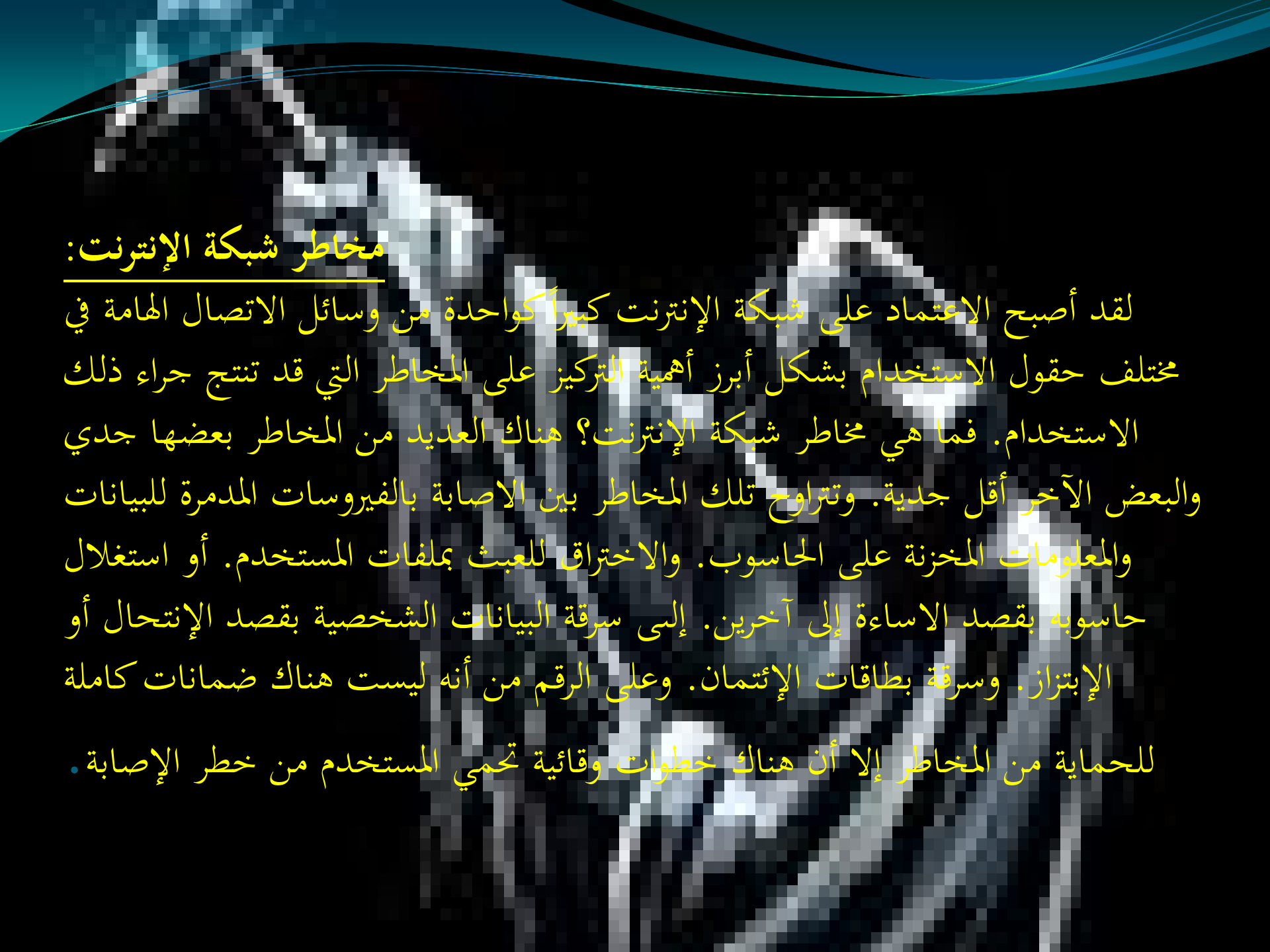
ككلمة تحمل معنى يختلف تماماً عما تحمله هذه الأيام، فقد بدأت hackers بدأت كلمة كصفة تشير لعبقرية مبرمجي الكمبيوتر وقدرتهم على ابتكار أنظمة وبرامج حاسوب أكثر سرعة، ومن أشهر من اكتسب هذه الصفة > دينيس ريتش < و > كين تومسون < اللذان صمما برامج اليونكس عام 1969.

على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت، وعلى الرغم من المتعة التي يعيشها المستخدم عند استخدامه لخدماتها أو حين ابحاره في صفحاتها، تبقى المشكلة العالقة هي كيفية تأمين الحماية الشخصية التي باتت هاجساً يشغل بال المستخدمين ومطوري صناعة خدمات الإنترنت على حد السواء.

تنقسم الحماية الشخصية على شبكة الإنترنت إلى قسمين هما:

1. السلامة
2. الأمن.

فالسلامة هي توفير الحماية لضمان سلامة المستخدم نفسه من العرض للإستغلال أو الإبتزاز أو الإنتهاك أو الاساءة. علاوة على أنها اصطلاح يستخدم للإشارة إلى حماية الأطفال أثناء استخدامهم لشبكة الإنترنت. أما الأمن فهو توفير الحمابة لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد.



## مخاطر شبكة الإنترنت:

لقد أصبح الاعتماد على شبكة الإنترنت كبيراً كواحدة من وسائل الاتصال الهامة في مختلف حقول الاستخدام بشكل أبرز أهمية التركيز على المخاطر التي قد تنتج جراء ذلك الاستخدام. فما هي مخاطر شبكة الإنترنت؟ هناك العديد من المخاطر بعضها جدي والبعض الآخر أقل جدية. وتتراوح تلك المخاطر بين الاصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب. والاختراق للعبث بملفات المستخدم. أو استغلال حاسوبه بقصد الاساءة إلى آخرين. إلى سرقة البيانات الشخصية بقصد الإنتحال أو الإبتزاز. وسرقة بطاقات الإئتمان. وعلى الرقم من أنه ليست هناك ضمانات كاملة للحماية من المخاطر إلا أن هناك خطوات وقائية تحمي المستخدم من خطر الإصابة.

## السلامة على الإنترنت:

اعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات.

تجنب الافصاح عن أية معلومات شخصية في خدمات المشاركة الحية كغرف المحادثة والمنتديات.

احرص على استخدام اسم الاول فقط عند المشاركة في المحادثات أو المنتديات.

احرص على عدم ارسال أية معلومات حساسة ككلمات السر وأرقام بطاقات الإئتمان عبر البريد الالكتروني، واعلم أن الجهات الرسمية لا تطلب تلك المعلومات عبر البريد الإلكتروني.

استخدم كلمات سر صعبة التخمين وتجنب المعلومات العامة كتواريخ الميلاد وأرقام السيارات أو الهواتف وأسماء الأبناء، وحاول المزج بين الأحرف الصغيرة والكبيرة والأرقام والرموز.

تجنب المنتديات المشبوهة والمعروفة بالمنتديات السفلية والتي عادة ما يجتمع فيها مخترقوا الأنظمة.

تجنب خاصية التخزين التلقائي للمعلومات الشخصية على الحواسيب التي لا تخصك في حال استخدامها.

قم بعملية مسح ملفات ( cookies) بين فترة وأخرى.

تجنب الاحتفاظ بالصور والمعومات الشخصية على جهاز الحاسوب، واستخدم عوضاً لذلك ذاكرة التخزين المحمولة.

قم بفصل كاميرا الويب في حال عدم استخدامها.

استخدم كلمات سر للملفات الحساسة.

تجنب الرد على رسائل البريد الإلكتروني المشبوهة

## أمن الإنترنت:

لتأمين جهاز الحاسوب واعمل على تحديثها باستمرار. (firewallsاستخدم برامج مكافحة الفيروسات والجدران النارية (
استخدم برامج الكشف عن الملفات الخبيثة كملفات التجسس والملفات الدعائية والملفات التي تسيطر على متصفح الإنترنت.
افحص الملفات المنزلة من المواقع غير المعروفة أو خدمات مشاركة الملفات أو الواردة عن طريق البريد الإلكتروني.
لا تفتح الملفات المرفقة بالبريد الإلكتروني المجهولة المصدر.
(files encryptionاستخدم برامج تشفير الملفات (.
(anti-spamوخدمات مكافحة البريد غير المرغوب فيه (filters)استخدم مرشحات رسائل البريد الالكتروني (.
قم بعمل نسخ احتياطية للملفات بشكل دوري.
كن حذراً أثناء استخدام برامج المحادثة الفورية، وافحص الملفات التي تردك بواسطتها قبل فتحها.
(online port scannersللتأكد من عدم وجود منافذ مفتوحة للمخترقين، وتعرف تلك المواقع باسم (portsاستخدم مواقع فحص المنافذ (.
قم بعمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية.
غير الآمنة كالموجودة في (wi-fiتجنب فتح حساباتك المصرفية على الشبكة أو ارسال أرقام بطاقات الإئتمان عبر الشبكات اللاسلكية (
المطارات والمقاهي على سبيل المثال.

## انواع الهكر

هاكر يستخدم برامج او تقنيات في محاولات لاختراق الأنظمة او الاجهزه للحصول على معلومات سرية او للتخريب كا ختراق مزودات شركة و حذف او إضافة معلومات . وكان هذا الاسم يطلق على من يحاول إزالة أو فك الحماية التي تضيفها شركات إنتاج البرمجيات على برامجها لمنع عمليات النسخ غير القانوني، أما الأن ،تم تصنيف هذا النوع من المخترقين في فئه خاصة سميت بالقراصنة ( Pirates)

**Phreak**

هاكر يحاول التسلل بر الشبكات الهاتفيه اعتماداً على أساليب تقنية غير قانونية أو التحك بهذه الشبكات و يستخدم هؤلاء أدوات خاصة مثل مولدات النغمات الهاتفية. ومع تحول شركات الهاتف إلى استخدام المقاسم أو البدالات الرقمية عوضا عن الكهروميكانيكية القديمة، تحول هؤلاء إلى استخدام الأساليب البرمجية ذاتها التي يستخدمها ال

**Crackers**

**مؤلفوا الفيروسات**

**يقوم هذا النوع من الهاكر بتصميم الفيروسات محبة في التخريب و تدمير الاجهزه و يعتبر المحللون النفسيون أن من ينتمي إلى هذا النوع من المبرمجين مصاب بمرض عقلي أو نفسي ، يدفعه إلى هذه العمليات التخريبية التي لا يجني منها أي فائدة شخصية ، ويعتبر هذا النوع من أخطر الانواع**

***Cypherpunks***

**يحاول هذا النوع من الهاكر الحصول على أدوات و خوارزميات التشغير المعقدة و القوية و توزيعها بصورة مجانية حيث تسمح هذه الادوات بإجراء عمليات تشفير لا يمكن فكها إلا باستخدام أجهزه كمبيوتر فائقة**

***Cyberpunk***

**تطلق هذه التسمية على كل من يستخدم مزيجا من الطرق المسبقة للقيام بعمليات غير قانونية**

***Anarchists***

**وهذا النوع هو الذي يروج معلومات مخالفة للقانون او مشبوهة على أقل تقدير مثل طرق ترويج صناعة المخدرات أو المواد المتفجرة أو قرصنة القنوات الفضائية و غيرها**

**ويوجد غير هذه الانواع من الهاكر ولكن هؤلاء الاهم**


تعرضت سيرفرات شركة سوني إلى عملية إختراق كبيرة، إلا أنها بائت بالفشل بحسب رئيس قسم الأمن والحماية في الشركة. فقد تم إجراء عمل استباقي أمام الهاكرز باغلاق 93 ألف حساب

## تكنولوجيا الأمن

هناك عدد من الحلول القائمة باستخدام المفتاح العمومي القائم على الترميز. في هذه النظم المستخدم لديه مفتاحين رمزيين للمحافظة على أمن مصادر البيانات؛ المفتاح الأول هو المفتاح العمومي المشهور، والآخر هو مفتاح الحفاظ على السرية بالنسبة للمستخدم، وباستخدام الطرق الرياضية يمكن استخدام المفتاح السري الخاص لتوقيع مجرى البيانات مثل رسائل البريد الإلكتروني، وهذا التوقيع يدعى "التوقيع الرقمي" الذي يجري جنبا إلى جنب مع البيانات عند نقلها، وعندئذ يمكن استخدامها للتحقق من أن الرسالة لم يحدث ليها تغيير أثناء نقلها وذلك باستخدام المفتاح العمومي ويجب أن يكون المرسل على علم ودراية بالمفتاح الخاص.


## تأمين الرسالة الإلكترونية

هناك ثلاثة أنظمة رئيسية ستخدم هذه التقنية للمحافظة على أمن نقل الرسائل وهي: PGP، PEM، X400-. ففي النظام الأول (PGP) مستخدم الرسالة يحدد الاسم ثم ينشئ زوج من المفتاحين العام والخاص باستخدام البرمجيات المتاحة للاسم، أما الجزء الخاص فيبقى سري لدى المستخدم. وعندما ترسل الرسالة تكون قد شفرت بالمفتاح الخاص مع المحافظة على أمن المعلومات التي بالرسالة.

هذا نموذج بسيط تنامى بسرعة كبيرة لتأمين الحماية للرسائل والإنترنت بشكل خاص، لكن الأسماء ليست مضمونة فهناك إمكانية لاستخدام مفتاح خاطئ لتشفير البيانات وليس هناك طريقة للسيطرة التامة إذا تم كشف المفتاح الخاص عن طريق الصدفة مثلا.


Microsoft
Windows


القرصنة ... الى متى ؟

عمل الطالبة: سلمى علي محمد سعيد القريصي

الصف: 9

المادة: تنكنولوجيا المعلومات