
# أمن تكنولوجيا المعلومات

# It security

اليوم الثاني

## تشفير المستندات :

## سهلة وبسيطة وغير كافية

# البرامج الخبيثة The Malicious Software



هي أحد تهديدات الحاسوب في هذا العصر. ونقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض. و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.و يمكن يتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

١. الفيروسات (Viruses)
٢. الديدان (Worms)
٣. برامج التجسس (Spywares)
٤. الخداع (Hoax)
٥. عمليات الاحتيال واصطياد الضحايا The Phishing Scam
٦. أحصنة طروادة Trojan Horses

# الفيروسات Viruses



- فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة ، كما تقوم بالتلاعب بمعلومات الكمبيوتر المخزنة
- ينتقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك أو عند زيارة احد المواقع المشبوهة او اثناء تبادل السي ديات أو الفلاشات مع الأصدقاء و ينشط الفيروس عند محاولة فتحه ويمكن ان يصلك ايضا عن طريق البريد الألكتروني على هيئة مرفقات

# الديدان Worms



- ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها
- يمكن أن تسبب الضرر بشكل واسع.
- على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة.
الديدان تعتبر برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

# برامج التجسس Spywares



- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- المعلنين وغيرهم يرغبون في معرفة ماهي المواقع الإلكترونية التي يقوم المستخدمون بزيارتها وما هي عادات وأساليب تصفح الإنترنت لديهم.
- في بعض الأحيان تقوم برامج التجسس بإعادة توجيه مدخلات المتصفح لتوجه المستخدم إلى موقع آخر غير المقصود.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

# أحصنة طروادة The Trojan Horses



- وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم.
- فيتم بذلك تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار

# أضرار الإصابة بالفيروسات و البرامج الخبيثة



١. تعطيل الحاسوب
٢. ظهور شاشة الموت الزرقاء
٣. سرقة النقود إلكترونيا
٤. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات
٥. تسرق البيانات
٦. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات
٧. تبطئ الحاسب
٨. تبطئ الاتصال بالانترنت

# أعراض الإصابة بالفيروسات و البرامج الخبيثة



- تباطؤ أداء الحاسوب.
- زيادة حجم الملفات، أو زيادة زمن تحميلها للذاكرة .
- ظهور رسائل تخريبية على الشاشة، أو الرسوم أو صدور بعض الأصوات الموسيقية.
- حدوث خلل في لوحة المفاتيح كأن تظهر على الشاشة أحرف ورموز غير التي تم ضغطها أو حدوث قفل للوحة المفاتيح .
- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كان يعمل سابقاً بشكل عادي.
- سعة الأقراص أقل من سعتها الحقيقية.

# الفيروسات



- **بعض طرق الحماية:**
  - برامج مكافحة الفيروسات مثل:

**( Macafee , Kaspersky, Norton, Avira, AVG, NOD32)**

  - توفير نسخ احتياطية (backup) .
  - جدار الحماية.
  - كلمة المرور(Password).

# نصائح عند فتح ملحقات البريد الإلكتروني



- لا تفتح أية ملفات ملحقة ببريد إلكتروني من مصدر غير موثوق.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني ما لم تعرف محتواها.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني إذا كان حقل الموضوع مشكوكاً فيها وغير متوقع.
- احذف سلسلة رسائل البريد الغير هامة وتجنب الرد عليها.
- لا تقم بتحميل أية ملفات من الغرباء.
- توخي الحذر عند تحميل الملفات من الانترنت، تحقق من شرعية المصدر وحسن سمعته.

# الهدف من إعداد البرامج الخبيثة



- تختلف دوافع إعداد الفيروسات فمنها الدوافع الحسنة ومنها الدوافع المادية ومنها الدوافع الانتقامية ، فبعض الناس يقوم بإعداد الفيروسات للتسلية أو لإظهار القدرة على البرمجة ولكن هناك من يعدها لهدف مادي وذلك لضمان تردد المستخدم لمحلات الكمبيوتر للصيانة او التخلص من هذا الفيروس او السطو على حسابات البنوك او المعومات العامة للشركات والمؤسسات الكبرى ، ومهما كان هدف اعداد الفيروس لابد من الوقاية منه لأنه يسبب الكثير من المشاكل والخسائر لمستخدمي الكمبيوتر .

**الهندسة الاجتماعية** أو ما يعرف بفن اختراق العقول هي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سرية. تُستخدم الهندسة الاجتماعية أحياناً ضمن احتيال الإنترنت لتحقيق الغرض المنشود من الضحية، حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هذه الأسئلة دون إثارة الشبهات).

**الأساليب المتبعة في الهندسة الاجتماعية.**

ان أشهر الأساليب المتبعة في مثل هذا النوع من الاختراق :

**الهاتف:** فأكثر هجمات الهندسة الاجتماعية تقع عن طريق الهاتف . يتصل المهاجم مدعياً أنه شخص ذو منصب له صلاحيات و يقوم تدريجياُ بسحب المعلومات من الضحية.

**البحث في المهملات:** حيث يوجد الكثير من المعلومات الهامة عن المنظمة يمكن الحصول عليها من سلة مهملات الشخص أو الضحية.

**الإقناع:** حيث يحصل المهاجم على المعلومات التي يريدها من خلال التحدث مع الضحية وحثها على الإدلاء بمعلومات حساسة أو ذو علاقة بهدف المهاجم وذلك من خلال إثارة انطباع جيد لدى الضحية والتملق وغيرها من الأساليب.

**الهندسة الاجتماعية المعاكسة:** وهي إيهام الضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بالإدلاء بمعلومات يريدها الضحية وإذا ما نجح الأمر وسارت الأمور كما خُطط لها فقد يحصل المهاجم على فرصة أكبر للحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضير المسبق وحجم المعلومات التي بحوزة المهاجم.

# رسائل الاصطياد الخادعة The Phishing Scam




- التصيد هو محاولة الحصول على معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان من قبل محتالين متنكرين بوصفهم أنهم يعملون في منظمات جديرة بالثقة.
- التصيد هي عملية يحتال فيها المهاجم حيث يرسل رسالة بالبريد الإلكتروني يطلب فيها بطاقات ائتمانية أو بطاقات التجارة الإلكترونية وتكون صالحة وسارية المفعول
- البريد الإلكتروني غالبا ما يستخدم أساليب التخويف في محاولة الإغراء الضحية إلى زيارة مواقع ويب مخادعة. يشعر فيها الضحية بانها مواقع عامة مثل التجارة الإلكترونية أو الخدمات المصرفية

# أساليب الهجوم باستخدام الهندسة الاجتماعية

أ– أسلوب الإقناع (Persuasion):

هذا هو أهم أساليب هذه الطريقة ؛ ولذلك سنفصل الكلام فيه. وبادئ ذي بدء نقول إن سيكولوجية الإقناع لها جوانب متعددة أهمها[1]:

(1) طـــــرق الإقنـــــاع: تـدل الدراسـات الـتي أجريـت في علـم الـنفس الاجتماعـي (Social Psychology)أن هنـاك طريقتين لإقناع شخص لعمل شيء ما:

(أ) طريقـة الإقنـاع المباشـرة: في هـذه الطريقـة يتـذرع المهـاجم بـالحجج المنطقيـة والبراهين لحفز المستمع – في هذه الحالة الضحية – على التفكير المنطقي والوصول إلى نتيجة يرغب المهاجم في جر الضحية إليها.

(ب) الطريقة غير المباشرة: هنا يعتمد المهاجم على الإيحاءات النفسية، والقفز فوق المنطق، وتحاشي استنفار قدرة التفكير المنطقي لدى الضحية، وحث الضحية على قبول مبررات المهاجم دون تحليلها والتفكير فيها جدياً.

أساليب التأثير المستخدمة في طريقة الإقناع غير المباشرة:

(أ) **التربي بمظهر صاحب السلطة:** إن الغالب على الناس سرعة تلبية طلبات ذي السلطة، حتى وإن لم يكن موجودا بشخصه. وقد أجريت تجربة في ثلاثة مستشفيات بالولايات المتحدة حيث ادعى الشخص الذي أجرى التجربة أنه طبيب، واتصل هاتفياً باثنتين وعشرين مكتباً من مكاتب المرضات بالمستشفيات الثلاثة، وفي كل مرة كان يطلب من المرضة التي ترد على مكالمته أن تصرف 20مللجراما من دواء معين لمريض معين موجود في الجناح الذي يشرف عليه مكتب المرضات الذي اتصل به الباحث. وفي هذه التجربة عدة أمور يجب أن يُنتبه إليها:

**أولاً:** إن المرضة لم يسبق لها رؤية الطبيب المزعوم، أو حتى الحديث إليه هاتفياً.

**ثانياً:** إن هذا الطبيب كان يعطيها الوصفة هاتفياً، بدلاً من الحضور شخصياً لإعطاء الوصفة كما تنص على ذلك قواعد العمل في المستشفيات التي أجريت التجارب فيها.

**ثالثاً:** إن العلاج الذي وصفه الطبيب المزعوم، لم يكن استخدامه مسموحاً به داخل ذلك الجناح.

**رابعاً:** إن الجرعة التي وصفها ذلك الطبيب كانت ضعف الحد الأقصى المسموح به في الأجنحة التي يسمح فيها بوصف ذلك الدواء.

ومع كل هذا فإن 95٪ من الممرضات التي جرى الاتصال بهن كن في طريقهن لتنفيذ طلبات الطبيب، لكن المراقبين المشاركين في التجربة أوقفوهن قبل تنفيذ ذلك.

## أسلوب انتحال الشخصية

وتعني تقمص إنسان ما شخصية إنسان آخر، وقد يكون هذا الآخر شخصاً حقيقياً أو متوهما. ومن الشخصيات التي يكثر انتحالها في مجال الهندسة الاجتماعية: شخصية فني صيانة معدات الحاسوب والشبكات، وعامل النظافة، والمدير، والسكرتير. كما يكثر انتحال شخصية طرف ثالث مخول من قبل الإدارة العليا في الشركة أو المؤسسة. ولتوضيح ذلك قد يحصل المهاجم على اسم المستخدم الخاص بالبريد الإلكتروني لمدير الشركة، وهذه مسألة سهلة لأن هذا الاسم ليس سرياً. بعدها يتصل المهاجم بأفراد مركز تقديم الدعم الفني بالشركة مقدماً نفسه على أنه سكرتير المدير، مدعياً أن المدير قد كلفه بالاتصال بهم ليطلب كلمة مرور جديدة، نظراً لأن المدير قد نسي كلمة المرور السابقة، وأنه يجب إصدار كلمة المرور الجديدة فوراً، لأن المدير لديه اجتماع بعد ساعة، ويرغب في مراجعة بعض الوثائق المهمة التي أرسلها أحد المشاركين في الاجتماع إليه عن طريق البريد الإلكتروني. وإذا كان المهاجم بارعاً في تقمص شخصية السكرتير فإن أفراد مركز تقديم الدعم الفني قد يصدرون كلمة مرور جديدة للمدير ويعطونها للمهاجم المنتحل شخصية سكرتير المدير، وبذا يستطيع المهاجم الدخول إلى البريد الخاص بمدير الشركة.

## قصة واقعية

أرسل المدرس أسئلة الواجب بالبريد الإلكتروني، وطلب إرسال الردود عليها بالبريد الإلكتروني، ووضع موعداً لا يقبل أي إجابات بعده. وقبيل حلول الموعد النهائي بساعتين وصل بريد إلكتروني إلى عدد من الطلاب من شخص تقمص شخصية مساعد مدرس المادة – وهو شخص حقيقي، غير أن كثيرا من الطلاب لا يعرفونه – يطلب من الطلاب أن يرسلوا إجابتهم إلى بريده واستخدم اسماً وهمياً. تبين بعد ذلك أن مرسل هذا البريد كان أحد طلاب المادة، لكنه لم يتمكن من حل بعض الأسئلة، وأراد أن يرى كيف حلها الطلبة الآخرون. ولفرط ذكاء المهاجم لم يرسل البريد إلى جميع الطلاب بل اكتفى بإرساله لبعضهم حتى لا يفتضح أمره.

هـذه إحـدى الطـرق المتقدمـة لكسـب ثقـة المستهدفين، ومـن ثـم الحصـول علـى المعلومات. وتقوم هذه الطريقة على اختلاق موقـف يُظهـر المهـاجم في صـورة صـاحـب سلطة إدارية أو فنية، فيتوجه إليه المستهدفون بالأسئلة ويطلبون منـه المسـاعدة ويتلقـون منه التعليمات. وقد ذكر بعض الباحثين[1] أن تنفيذ هذه الطريقة يمر بثلاث مراحل :

(1) افتعال الموقف.

(2) إبـراز المهـاجم نفسـه علـى أنـه الشـخص ذو المعرفـة أو الصـلاحية اللازمـة للتعامل مع الموقف.

(3) تقديم المساعدة.

ولتوضيح المسألة نضرب المثال التـــالي: يقوم المهاجم بتخريب متعمد لشبكة المعلومات في أحد مكاتب الشركة مثلاً فتنقطع الخدمة عن بعض أو كل الموظفين، وهذه مرحلة افتعال الموقف. و يجب أن لا يظن أحد أن القيام بمثل هذا التخريب أمر صعب، فكل ما يُحتاج إليه هو سحب الكيبل الموصل بين المقسم وباقي الشبكة، وغالبا ما يكون هذا المقسم في مكان عام يمكن لأي شخص الوصول إليه. ووسط هذه المعمعة يظهر المهاجم بصورة المنقذ، فيقدم نفسه على أنه أحد أعضاء فريق الدعم الفني وأنه سيقوم بإنقاذ ما يمكن إنقاذه، وتأتي بعد هذا المرحلة الثالثة وهي مرحلة تقديم المساعدة إذ أن الموظفين سيتوجهون إليه بالأسئلة عما إذا كانوا سيفقدون الوثائق التي كانوا يعملون عليها لحظة انقطاع الشبكة، وهل يحتاجون إلى تغيير كلمة المرور وكيف يمكن معاودة الاتصال بالشبكة وهلم جرا. وهنا يستطيع المهاجم الحصول على المعلومات التي يريدها، وإذا كان المهاجم ذكياً فإنه سيقوم بإصلاح الشبكة بسرعة قبل أن ينتبه لانقطاعها أعضاء الدعم الفني الحقيقيون، وإذا أفلح في فعل ذلك فسيكون قد نجح في اختراق نظام معلومات الشركة دون أن يشعر بذلك أحد.


## الخلاصة

الهندسة الاجتماعية هي إعمال الحيل النفسية لخداع مستخدمي الحاسوب للوصول إلى المعلومات المخزنة فيها، وهي أسهل الأساليب و أكثرها فعالية لأنها تهاجم العنصر البشري الذي هو أضعف نقطة في منظومة حماية المعلومات، و لذا يجب أن تكون على رأس قائمة المعنيين بحماية المعلومات.

**طرق الحماية من الهندسة الاجتماعية:**

**وضع قوانين للحماية الأمنية للمنظمة:** تقوم المنظمة بالتوضيح للعاملين فيها قوانين الحماية الأمنية المتبعة والتي على العاملين تطبيقها.

على سبيل المثال: يقدم الدعم الفني المساعدة ضمن أمور معرفة ومحددة مسبقاً.

**وضع حماية أمنية لمبنى المنظمة:** يمنع دخول الأشخاص غير العاملين في المنظمة.

و تحدد الزيارات في حدود الأعمال بمعرفة سابقة لحراس الأمن في المنظمة وتحت مراقبة منهم.

**التحكم بالمكالمات الهاتفية:** وذلك بوضع نظام امني للمكالمات مع قدرة على التحكم في من يستطيع مكالمة من.

منع المكالمات الخاصة وحضر المكالمات الدولية وبعيدة المدى إلا للضرورة وبإذن المسئول عن المكالمات.

عدم إظهار مدخل للخط الهاتفي للمنظمة لتجنب استخدام الهاتف من قبل شخص خارج المنظمة.

**التعليم والتدريب:** تثقيف الموظفين داخل المنظمة بمجال أمن المعلومات والاختراقات التي من الممكن حصولها.

تدريب الموظفين في مركز الدعم الفني وتثقيفهم على مستوى جيد من الناحية الأمنية وتوضيح أساليب المهاجمين وتدريسها لهم.

تدريبهم على عدم إعطاء معلومات ذات سرية عالية إلا بعد التأكد من هوية الشخص ووفقاً للحد المسموح بيه.

تدريبهم على كيفية رفض إعطاء المعلومات عند عدم الإمكانية بأسلوب لبق.

إستراتيجية التصرف في المواقف الحرجة: بأن يكون هناك إستراتيجية محددة تضعها المنظمة تمكن الموظف من التصرف إذا طلب منه معلومات سرية تحت ضغط ما.

**إتلاف المستندات والأجهزة غير المستخدمة:** وضع أجهزة لإتلاف الورق داخل المنظمة كي لا يمكن استخدام المعلومات التي تحويها سواء كانت معلومات حساسة أو كلمات سر للدخول للنظام ونحو ذلك.

إتلاف أجهزة الكمبيوتر القديمة كي لا تستعمل باستخراج معلومات سرية منها.