مقدمة في الأمن السيبراني

الجزء الرابع: طرق الحماية

أ. د. أسامة حسام الدين

مارس 2018

المحتوى العام

- الجزء الأول: المستخدم.
- الجزء الثاني: القراصنة.
- الجزء الثالث: الهجمات.
- **الجزء الرابع: طرق الحماية.**

طرق الحماية

حماية الأجهزة الشخصية

- قم دائما بتشغيل الجدار الناريFirewall
- قم بتثبيت مكافح للفيروسات Anti-Virusومكافح لبرامج التجسس Anti-Spyware

عرض كيفية إدارة الجدار الناري ومكافح الفيروسات

حماية شبكة الواي فاي

- يجب ان تقوم بتغيير معرف الخدمة الافتراضي SSIDوكلمة السر الافتراضية
- يجب أن يتم تغيير كلمة السر الخاصة بلوحة التحكم، تيقن أن القراصنة يدركون جيدا المعلومات الافتراضية للشبكات اللاسلكية لذا يجب تغييره
- يجب تفعيل خدمة الاتصال المشفر وذلك بتفعيل خوارزمية WPA2 للتشفير
- واختياريا ممكن إعداد الموجه لكيلا يقوم ببث معرف الخدمة لذا فإن معرف الشبكة اللاسلكية لا يظهر على أجهزة الأشخاص المتجولون قريبا من الشبكة
- بالنسبة للشبكات اللاسلكية في الأماكن العامة استخدم خدمات "الشبكة الافتراضية الخاصة Virtual Private Network "أو VPN والتي ترسل البيانات في أنفاق بتغليفها وتشفيرها فلا يستطيع المهاجمين الوصول إلى البيانات

عرض كيفية عمل الخطوات في الأعلى

كلمات السر | برامج إدارة كلمات المرور

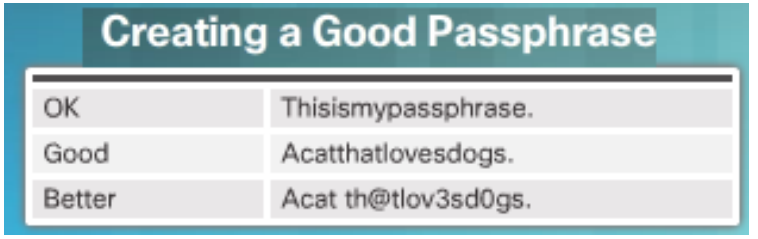
- من المحتمل أن يكون لديك أكثر من حساب على الإنترنت، وكل حساب يجب ان يكون له كلمة سر منفصلة .وهذا كثير من كلمات السر لا يمكن حفظها كلها
- استخدام نفس كلمة السر في كل حسابات الإنترنت بمثابة عمل مفتاح واحد لكل الكنوز
- برنامج إدارة كلمات السر الموقع https://lastpass.com/
- ويوجد أيضا بعض المواقع التي تقترح عليك كلمات سر مثل http://passwordsgenerator.net/ .

كيفية استخدام برنامج lastpass

كلمات السر | نصائح هامة عند اختيارها

- لا تستخدم كلمات القواميس بأي لغة ككلمة سر
- لا تستخدم كلمات القاموس المبعثرة أو ناقصة الأحرف.
- لا تستخدم كلمات متعلقة بالحاسب، ككلمة "ويندوز" أو "سيستم" أو اسم المستخدم
- استخدم الحروف الخاصة مثل ! @ # $ % ^ & * ( ) إن أمكن.
- استخدم كلمات سر بطول ثمانية أحرف ويفضل أطول. يعرض الشكل أمثلة على الاستخدام الأمثل لكلمات السر

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now



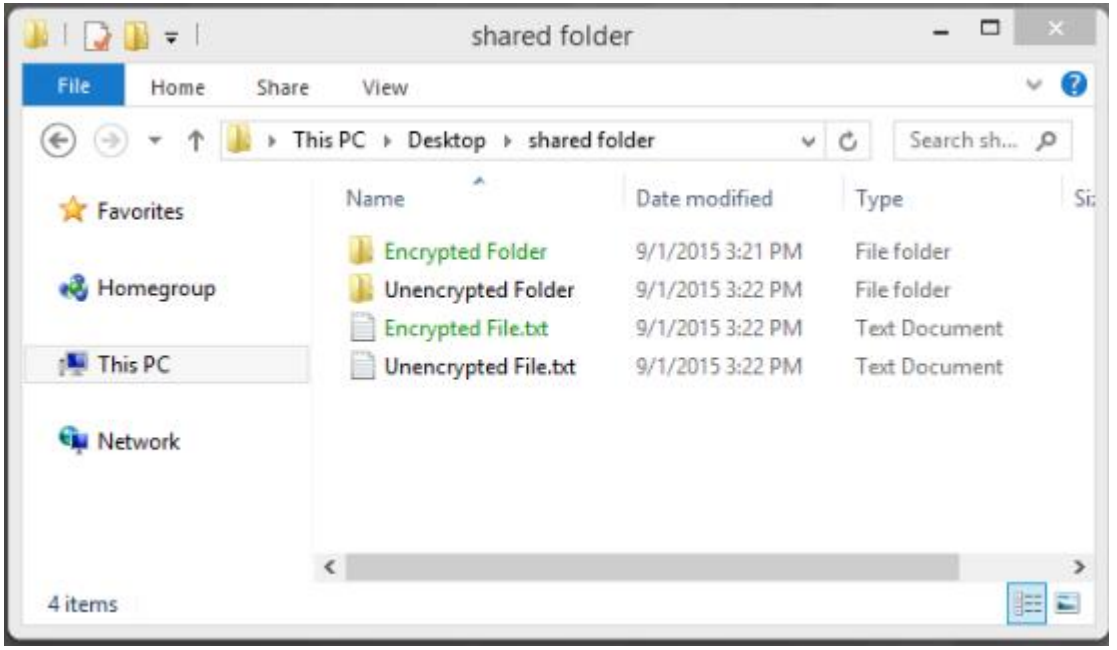
استخدم عبارات السر

حماية البيانات | البيانات الثابتة

.قم بتشفير بياناتك :استخدم البرامج المتاحة على الإنترنت

.احتفظ بنسخة احتياطية من البيانات :من الأمثلة على التخزين في السحب، Dropbox.com, Google Drive, OneDrive, Meaga

.قم بالتخلص من بياناتك كليا :لمنع استرجاع الملفات المحذوفة من آثارها المغناطيسية، يجب استخدام برامج متخصصة في ذلك مثل برنامج SDeleteلبرامج النوافذ والذي يمكنه حذف الملفات السرية بشكل كامل. وبرنامج Shredفي لينكس وكلمة Shredتعني التمزيق .وبرنامج Secure Empty Trashفي نظام التشغيل ماك.



حماية البيانات | البيانات المتنقلة

.لا تشارك كثيرا على شبكات التواصل الاجتماعي:

فلا تشارك مثلا تاريخ ميلادك، عنوان بريدك الإلكتروني، أو رقم تليفونك لا تكمل ملفك الشخصي الموجود على مواقع التواصل الاجتماعي (Profile) قم بإعطاء أقل معلومات ممكن.
تأكد دائما من أن الأشخاص الذي يطلعون على أنشطتك ومحادثاتك هم أشخاص تعرفهم، وهم فعليا من تريد أن يتابعوك

.خصوصية البريد الإلكتروني:

عندما ترسل بريدا الكترونيا فأنت كمن يرسل بطاقة بريدية أو بطاقة معايدة أو بطاقة دعوة للزفاف. حيث يتم تراسلها في صورتها الحقيقية كنص عادي

كيفية استخدام التصفح الآمن

القضايا القانونية والأخلاقية

- قد تتعجب أن **القوانين والسياسات والأخلاقيات** من أهم العوامل لعمل حماية من الهجمات
- سيفكر القراصنة ألف مرة إذا علموا عاقبة ما يفعلون.

القضايا القانونية

من الناحية الشخصية فإنك لن تسلم من الاحتكاك بقانون الأمن السيبراني حتى إن كنت لا تعمل في شركة أو موجود في أي مؤسسة من الممكن أن تحاول أن تتسلل إلى جهاز جيرانك أو الدخول على شبكة عامة والعبث ببيانات من يتصلون بها.

.هناك مقولة قديمة تقول " فقط لأنه يمكن لا يعني أنه يجب " مترجمة من المثل الإنجليزي Just because you can doesn’t mean you should

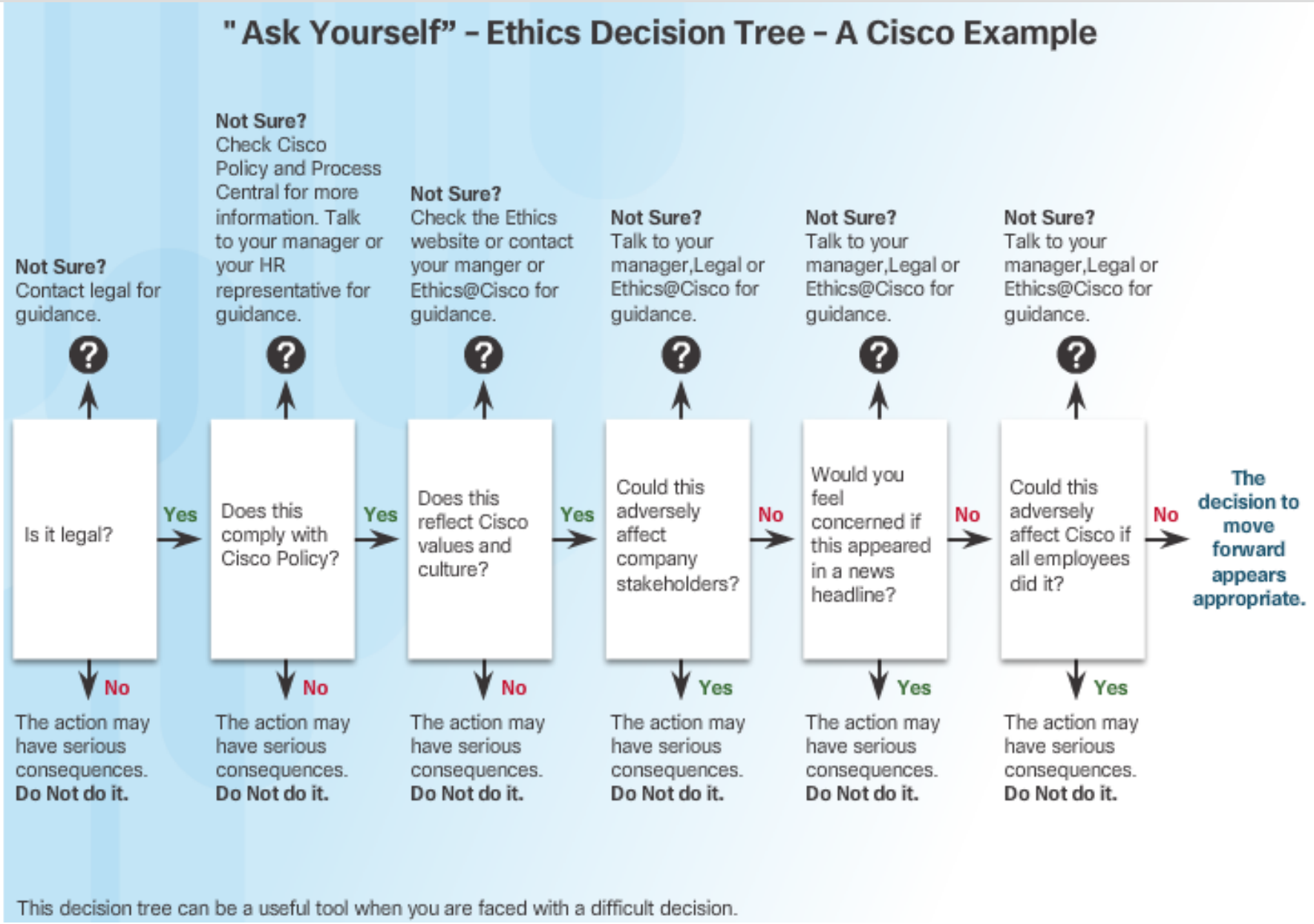
.وكن على وعي بأن القراصنة غالبا ما يتركون أثرا خلفهم يمكن تتبعه للوصول اليهم.

من الناحية المؤسسية فإن كثيرا من الأقطار يضعون قوانين للأمن السيبراني مثلا قوانين خاصة بالبنية الشبكية للمؤسسة وخصوصية الفرد والمؤسسة

. بعض الأحيان قد يفقدك مخالفة القانون السيبراني وظيفتك. أو ان تعاقبك الشركة بالفصل أو الغرامة وأحيانا السجن.

.الحل الأمثل في حالة مواجهة موقف أمني لا تعرف إن كان قانونيا أم، افترض عدم قانونيته وأسأل بعدها المتخصصون في القانون داخل الشركة.

ماذا أفعل لمواجهة موقف أمنى غريب



نظام مكافحة الجرائم المعلوماتيه بالمملكة

.تقدمه هيئة الاتصالات وتقنية المعلومات.

.عبارة عن مستند يحتوى على القوانين التي تحكم استخدام الموارد والوصول إليها بدون تصريح

.تعاقب بالسجن وبالغرامة في حالة المخالفة

.يمكن الاطلاع على نظام مكافحة الجرائم المعلوماتيه على الرابط

http://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

المادة الثالثة:

يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح- أو التقاطه أو اعتراضه.

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه ، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

تمرين اختبار أمان التصفح عبر الإنترنت

قم بالإجابة على الأسئلة التالية بإخلاص، وقم بحساب النقاط الإجمالية التي حصلت عليها بتجميع نقاط كل سؤال

1. ما هي نوعية المعلومات التي تشاركها عبر مواقع التواصل الاجتماعي

- كل شيء، فأنا أعتمد على مواقع التواصل الاجتماعي في التواصل مع الأصدقاء والعائلة (3نقطة)
- الأخبار والمقالات التي اقرأها (2نقطة)
- أعرف جيدا ما الذي أشاركه ومع من أشاركه (1نقطة)
- لا شيء، فأنا لا استخدم مواقع التواصل الاجتماعي.(0نقطة)

2. عندما تفتح حساب في أحد المواقع على الإنترنت

- أستخدم نفس كلمة السر التي استخدمتها في مواقع أخرى ليسهل علي تذكرها (3

تمرين اختبار أمان التصفح عبر الإنترنت

3عندما تستقبل رسالة بريد إلكتروني تحتوى على روابط لمواقع خارجية

- لا تضغط على الرابط أبدا، لأنك لا تفتح الروابط بداخل الرسائل الإلكترونية بالأساس (0نقطة)
- تضغط على الرابط لأن خادم الويب يقوم بفحص رسائل البريد الإلكتروني ويتأكد من خلوها من البرمجيات الخبيثة (3نقطة)
- تضغط على الرابط فقط في حالة ورود الرسالة من شخص تعرفه (2نقطة)
- قبل النقر بزر الفأرة على الرابط، تقوم بإيقاف مؤشر الفأرة فوق الرابط حتى تظهر معلومات عن الموقع الذي يشير إليه (1نقطة)

4.ظهرت فجأة نافذه تقول إن جهازك به بعض البرمجيات الخبيثة التي تحتاج إلى إزالة وتطلب انزال برنامج مكافحة للتعامل مع تلك البرمجيات الخبيثة وإزالتها.

- تقوم على الفور بإنزال البرنامج لحماية جهازك (3نقطة(
- تقوم بإيقاف مؤشر الفأرة فوق النافذة المنبثقة لتتأكد من الرابط الذي ستحولك عليه (3نقطة)
- تقوم بتجاهل الرسالة، وتتأكد من انك لم تنقر على النافذة وأنه لا يوجد أي برامج تم إنزالها دون طلبك (0نقطة)

تمرين اختبار أمان التصفح عبر الإنترنت

5. عندما تتصفح موقع بنك أو موقع شراء باستخدام بطاقة الائتمان

- تقوم بإدخال بيانات الدخول على الفور (3نقطة)
- تقوم بالتأكد من الرابط وأنه رابط موقع البنك أو موقع الشراء الذي تريده (0نقطة)
- أنت لا تستخدم البنوك عبر الإنترنت أو أي مواقع أخرى للعمليات المالية (0نقطة)

6. سمعت عن برنامج وتريد تجربته، وقمت بالبحث عنه عبر الإنترنت حتى وجدت نسخة تجريبية منه على موقع إلكتروني غير مشهور،

- تقوم بإنزال البرنامج وتشغيله (3نقطة)
- تقوم بالبحث عن معلومات عن البرنامج والشركة المصنعة له قبل تحميله (1نقطة)
- لا تقوم بتحميل أو تثبيت البرنامج (0نقطة)

تمرين اختبار أمان التصفح عبر الإنترنت

7. وجدت ذاكرة فلاش USB أثناء ذهابك للعمل

- تقوم بأخذها وتركيبها في جهازك لفحص محتوياتها (3نقاط)
- تقوم بأخذها وتوصيلها بجهازك بغرض إزالة محتوياتها (3نقاط)
- تقم بأخذها وتوصيلها بجهازك بغرض مسحها بمكافح الفيروسات حتى تتمكن من استعمالها لنقل ملفاتك الشخصية (3نقاط)
- تتجاهلها (0نقطة)

8. كنت في حاجة ملحة للإنترنت ووجدت نقطة لاسلكية لشبكة واي فاي مفتوحة بلا كلمة سر

- تتصل بها وتتصفح الإنترنت (3نقطة)
- لا تتصل بها وتنتظر حتى تصل إلى نقطة اتصال موثوقة (0نقطة)
- تتصل بها وتنشئ اتصال خاص (VPN) عبر خادم VPN موثوق قبل أن تستخدمها في تصفح الإنترنت.

النتيجة

الآن وبعد إجابتك على الأسئلة والاحتفاظ بمجموع النقاط التي حصلت عليها .قم بتقييم نفسك، فالأرقام المرتفعة تعني أنك غير آمن عند تصفح الإنترنت .يمكن معرفة نتيجة سلوكك من خلال إجمالي النقاط كالتالي:

إذا كان الإجمالي : 0فأنت آمن عبر الإنترنت

إذا كان الإجمالي :0-3فأنت آمن إلى حد ما يجب أن تغير من سلوكك عبر الإنترنت حتى تحصل على الأمان الكافي

إذا كان الإجمالي :3-17فأنت تتصفح بشكل غير آمن على الإنترنت وأنت عرضة للقرصنة

18فما فوق :أنت غير آمن على الإطلاق، وسيتم الاستيلاء على بياناتك

سؤال ؟