المملكة العربية السعودية
وزارة التعليم
الإدارة العامة للتعليم بمحافظة جدة
الشؤون التعليمية
إدارة التدريب والابتعاث (بنين)

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

وزارة التعليم
Ministry of Education

المركز الوطني
للتطوير المهني التعليمي

كلنا مسؤول

برنامج الأمن السيبراني

إعداد وتنفيذ

سهيل بن محمد أبو زهير

إدارة التدريب والابتعاث (بنين)
تعليم جدة

جائزة التعليم للتميز
EDUCATION EXCELLENCE AWARD

تاريخ التنفيذ ٠٢ ـ ٠٨ ـ ١٤٤١هـ

إدارة التدريب والابتعاث (بنين)
تعليم جدة

أهداف البرنامج

١- مفهوم الأمن السيبراني

٢- الأمن السيبراني وأمن المعلومات

٣- الاستراتيجية الوطنية للأمن السيبراني

٤- التهديدات والمخاطر والهندسة الاجتماعية

٥- حماية الأجهزة ووسائل التواصل

إدارة التدريب والابتعاث (بنين)
تعليم جدة

الهدف العام

التعرف على أساسيات الأمن السيبراني والاطلاع على الاستراتيجية الوطنية للأمن السيبراني

الأهداف التفصيلية

- التعرف على الفرق بين الأمن المعلوماتي والأمن السيبراني
- الاطلاع على بعض الجرائم السيبرانية
- التعرف على مفهوم الامن السيبراني
- التعرف على طرق التعامل مع الإساءة في مواقع التواصل الاجتماعي
- التعرف على مجالات ومخاطر استخدام الإنترنت
- الاطلاع على بعض الاحصائيات
- الوصول إلى أهداف الأمن السيبراني

محاور الدورة

الجلسة التدريبية الأولى
مفاهيم الأمن السيبراني

- التعريف بالمصطلحات
- الفضاء السيبراني
- الفرق بين الأمن المعلوماتي والأمن السيبراني
- الهدف من الأمن السيبراني

الجلسة التدريبية الثانية
تحقيق الأمن السيبراني

- تحقيق الأمن السيبراني الشامل
- لإنترنت أكثر أماناً
- كلمة المرور
- كيفية إنشاء كلمة مرور قوية يصعب اختراقها
- كيفية حماية الجهاز من الاختراق
- نصائح لحماية البيانات الشخصية أثناء تصفح الإنترنت

محاور الدورة

الجلسة التدريبية الثالثة
الإساءة في مواقع التواصل الاجتماعي

- استعادة السيطرة بعد الاختراق
- التعامل مع الإساءة في مواقع التواصل الاجتماعي
- سلوكي في الفضاء الإلكتروني يصنع تصورات الناس عني
- كيف أحافظ على حسابي في تويتر
- كيفية حماية الفيسبوك من الهكر
- كيف تحمي حسابك في "سناب شات"

الجلسة التدريبية الرابعة
الخصوصية في الفضاء الإلكتروني

- من أخطاء المستخدمين
- أساليب شهيرة في الاختراق وبعض نتائجها
- الخصوصية في الفضاء الإليكتروني
- أنواع الجرائم المعلوماتية
- طريقة التأكد من المواقع الموثوقة على الإنترنت
- كيف أعرف أن جهازي مخترق


الجلسة
الأولى

الجلسة التدريبية الأولى

مفاهيم الأمن السيبراني

التعريف بالمصطلحات

السبرانية

مأخوذة من كلمة (سيبر) Cyber
وتعني صفة لأي شيء مرتبط
بثقافة الحواسيب أو تقنية
المعلومات أو الواقع الافتراضي

الأمن السبراني

أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرّح به أو تغيير أو اختلاف قد يحدث

حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها

الأمن السيبراني

هو المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الالي الموجودة حول العالم ويشمل ذلك الاجهزة الالكترونية المرتبطة من خلال شبكة الالياف البصرية والشبكات اللاسلكية الفضاء السيبراني ليس الإنترنت فقط وانما شبكات اخرى كثيرة متصلة

الفضاء السيبراني

الفضاء السيبراني

مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة

استخدام الفضاء السيبراني للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي وحرمان العدو من تنفيذ نفس المقدرات

الجرائم السيبرانية

هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية.

الفرق بين الأمن المعلوماتي والأمن السيبراني

أمن المعلومات يهدف إلى:

حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل:

- يهدف إلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين
- يعنى بالوسائل الضرورية لاكتشاف وتوثيق وصد كل هذه التهديدات
- أمن المعلومات يشمل كل ما من شأنه حماية (المعلومة) التي قد تكون في نظام حاسوبي أو قد لا تكون كذلك
- أمن المعلومات المظلة الكبرى التي تغطي كل الأفرع الأخرى المرتبطة بحماية البيانات والمعلومات وتأمينها

فأمن المعلومات والأمن السيبراني هما مصطلحان متشابهان، لكنهما ليسا متطابقَين

أمن المعلومات بالتعريف هو أعم وأوسع من الأمن السيبراني

لعل التخصيص هنا بالتركيز على مجال الأمن السيبراني، بوصفه مجالًا من مجالات العلم، هو أمر مفيد جدًّا؛

فعلم الحاسب وعلم التشفير -مثلًا -اشتُقَّا أول ما اشتُقَّا من علم الرياضيات التطبيقية لأهميتهما، ثم ما لبثت هذه المجالات العلمية أن حلقت في فضاء العلم الرحب؛ لتتمدد، وتتوسع، وتخرج خارج الأطر العلمية لمجالها الأب. وهو الأمر ذاته لمجال الأمن السيبراني

الحرب الرقمية

هو سلاح استراتيجي بيد الحكومات والأفراد، لا سيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول.

نتذكر جميعًا الضجة الكبيرة التي أحدثها فيروس" شمعون" في المنطقة وخاصةً في المملكة العربية السعودية

الأمن السيبراني

الهدف من الأمن السيبراني

الهدف من الأمن السيبراني:

- ضمان توافر استمرارية عمل نظم المعلومات
- تعزيز حماية وسرية وخصوصية البيانات الشخصية
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة
- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة
- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال
- تعزيز حماية أنظمة تقنية المعلومات

الهدف من الأمن السيبراني:

- تعزيز حماية أنظمة تقنية المعلومات
- أن تكون المرجع الوطني للمملكة في شؤون تخصصها
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات
- مراعاة الأهمية الحيوية المتزايدة لتخصصها
- تعزيز حماية الشبكات

الجلسة التدريبية الثانية

الأمن السيبراني

الأمن السيبراني

٢٥ بليون جهاز انترنت الأشياء متصل بالإنترنت في عام ٢٠٢٠ م

١. يتم حماية شبكات الاتصالات

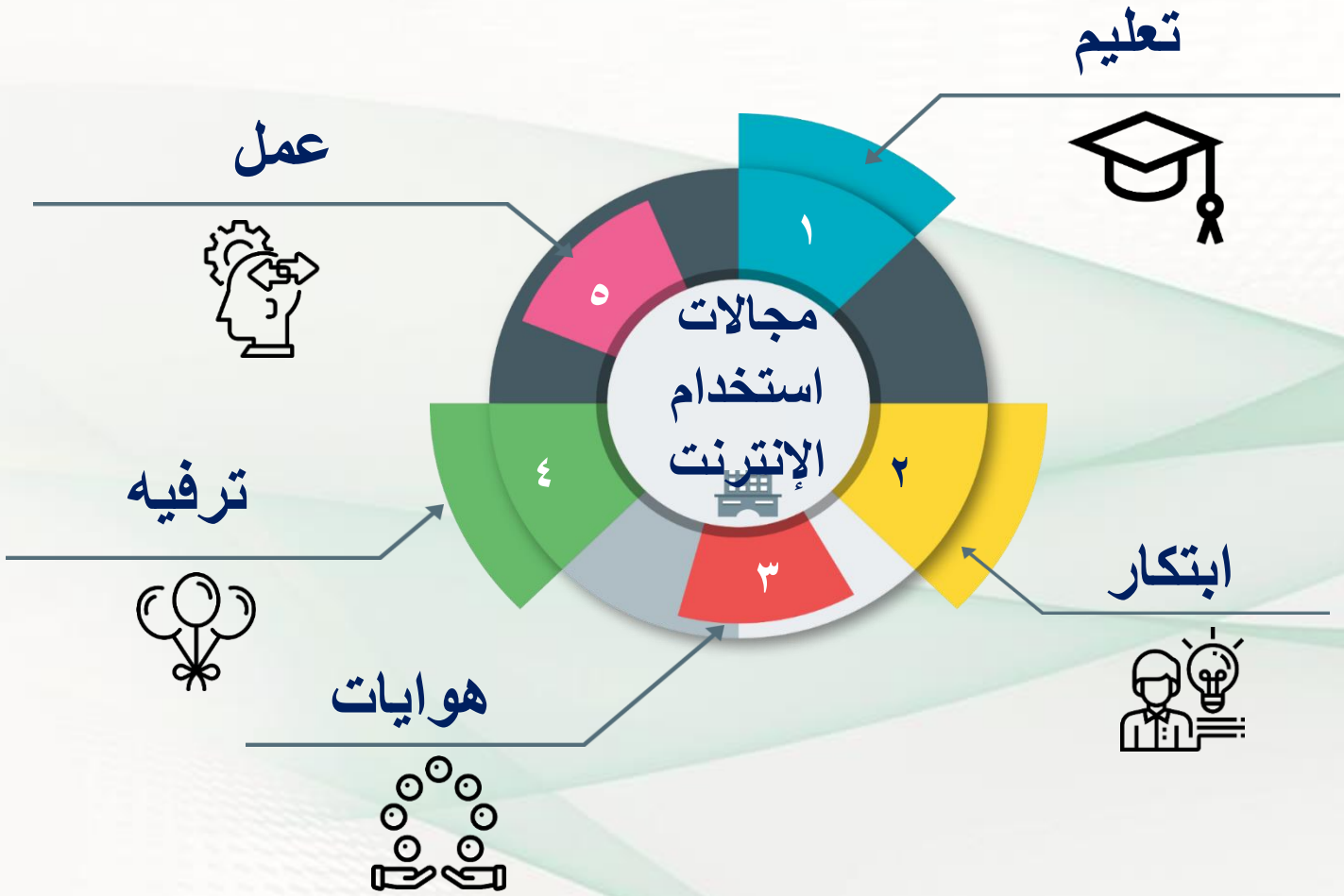
٢. شبكات المعلومات

٣. أنظمة الحواسيب ذات الاستخدام العام

٤. الانظمة المدمجة وما في حكمها

٢٦ مليون مستخدم للأنترنت في المملكة (٢٠١٧م)

زادت نسبة انتشار الأنترنت بمعدلات عالية خلال السنوات الماضية حيث ارتفعت من ٥٤٪ عام ٢٠١٢م إلى حوالي٨٢٪ في نهاية العام ٢٠١٧م


تعليم
عمل
ترفيه
ابتكار
هوايات
مجالات استخدام الإنترنت
١
٢
٣
٤
٥

أبرز مخاطر استخدام الإنترنت

- المحتوى الغير أخلاقي
- إدمان الإنترنت
- الابتزاز
- انتهاك الخصوصية
- الأضرار الصحية

لإنترنت أكثر أماناً

معرفة سُبل حماية خصوصية

معلوماتك وأجهزتك أثناء استخدامك

للإنترنت يقلل من احتمال تعرضها

لمخاطر الاستخدام غير المشروع،

والذي يلحق الضرر بك مادياً أو معنوياً

الجهاز الشخصي

محافظة منك على أمن جهازك وملفاتك الشخصية قم بالتالي

١ تركيب برامج مكافحة الفيروسات والحرص على تحديثها وفحص الجهاز بشكل دوري

٢ الحذر عند الاتصال بالشبكات اللاسلكية العامة

٣ المداومة على تحديث نظام التشغيل والتطبيقات

٤ الاحتفاظ بنسخة احتياطية

كلمة المرور

طرق اختيار كلمة المرور

- اختيار كلمة مرور قوية تحتوي على مجموعة من الاحرف والأرقام والرموز
- استخدام كلمة مرور مستقلة لكل حساب
- عدم اختيار كلمة مرور مبنية على معلومات شخصية
- عدم مشاركتها
- تغييرها بشكل دوري

حماية البريد الالكتروني

١
وضع كلمات مرور قوية وتفعيل التحقق الثنائي

٢
عدم فتح المرفقات من مصدر مجهول

٣
تفادي الوقوع ضحية للرسائل الاحتيالية

٤
تخصيص بريد خاص للاستخدامات الرسمية والهامة

كيفية إنشاء كلمة مرور

اشتراطات اختيار كلمة مرور قوية

١ يجب أن تتكون كلمة المرور من ٨ أحرف على الأقل، ويفضل استخدام اثنا عشر رمزا أو أكثر

٢ يجب أن تحتوي على أحرف كبيرة وصغيرة مثال a A

٣ يجب أن تحتوي على رقم على الأقل مثال 7

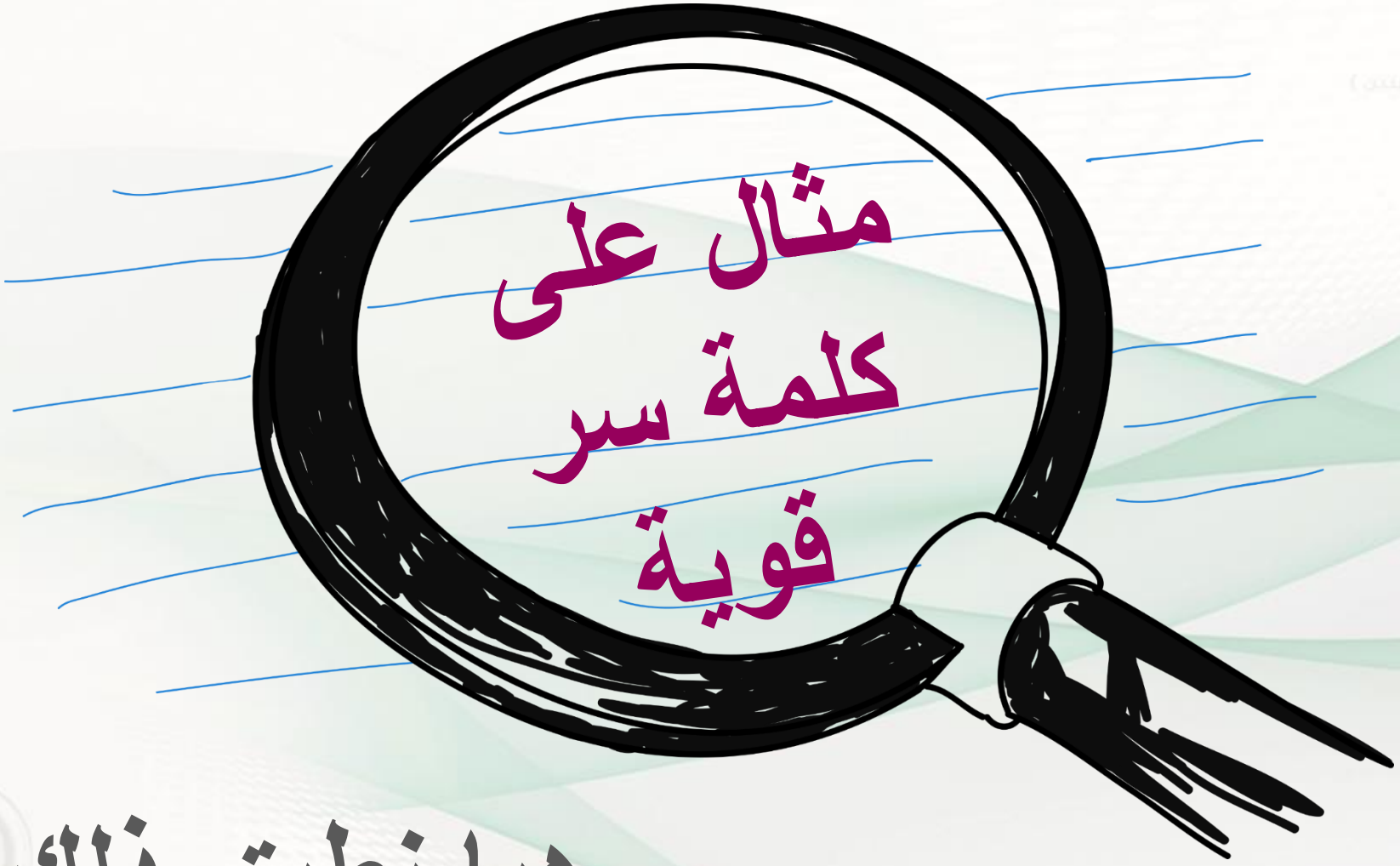
٤ أن تحتوي على أي من الرموز الخاصة الموجودة في لوحة المفاتيح مثال $ # &

ما هي الحروف / الرموز الخاصة في كلمة المرور؟

- يتم تحديد الرموز الخاصة المسموح باستخدامها في كلمة المرور طبقا لنوع البرنامج أو الموقع الذي يتم إنشاء كلمة السر فيه، فهناك بعض المواقع الإلكترونية التي تشترط رموز أو حروف محددة لاستخدامها في كلمة المرور

- هناك تطبيقات أخرى لا تشترط أي رموز محددة، وبالتالي فإن أي رمز يكون مسموح باستخدامه، ولذلك يجب مراعاة ذلك أثناء اختيار كلمة السر

- عادة ما تكون الرموز الخاصة مدمجة في لوحة المفاتيح (Keyboard) مع الأرقام، حيث تقوم بالضغط على زر NUM + Shift وهذا الرقم يكون من ٠ إلى ٩، أو يمكنك أن تعتبر أن أي رمز غير الحروف الإنجليزية Z-A والأرقام ٩-٠ هي من الحروف الخاصة



هيا نطبق ذلك

حماية الجهاز من الاختراق

تأمين البريد الإلكتروني

- يعتبر البريد الإلكتروني الشكل الرئيسي لتبادل المعلومات في الهواتف الذكية حالياً، وفي معظم الأوقات يكون مفعلاً على الشبكة، ممّا يجعل الشخص عرضةً للاحتيال الإلكتروني

- يقوم المخترقون في هذه العملية بالتنكر، لسحب المعلومات المهمة، والحساسة بالنسبة للمُخترق، ولمنع هذه الهجمات، يجب أن لا يقوم الشخص بفتح أيّ مرفقات، أو وصلات على شبكة الإنترنت

- الشركات الرسمية لا تقوم بطلب إكمال أيّ من النماذج المرفقة عن المعلومات الخاصة بالعميل، أو أن تقدم روابط مباشرة للتحميل مجاناً

- الشركات تطلب المعلومات من الموقع الخاص بها فقط، والحذر من الحسابات الوهمية، عن طريق التواصل مع الأصدقاء من خلال وسيلةٍ أخرى للتأكد من صحة الحساب

تعطيل خاصية المصادر المجهولة

يجب التأكد من تعطيل خاصية المصادر المجهولة على الجهاز عن طريق الذهاب إلى الإعدادات، ثمّ الأمان، ثمّ الذهاب إلى المصادر المجهولة وإغلاقها، وفي حال تنزيل إحدى التطبيقات أو البرامج المهمة على الجهاز، يمكن القيام بتشغيل الخاصية للتطبيق فقط، ثمّ إعادة إغلاقه بعد التنزيل

حذف الرسائل النصية

ينبغي حذف الرسائل النصية من المصادر المجهولة التي تطلب معلوماتٍ خاصة، وتجنب النقر على الروابط في الرسائل النصية، فبعض المخترقين يرسلون رسائل نصية قد تظهر أنّها من البنك الخاص أو أيّ مصدرٍ آخر موثوق، وفي حال الضغط على الرابط في الرسالة النصية

الحذر من شبكات الواي فاي المفتوحة

- ينبغي الدخول إلى الإنترنت من خلال الجهاز الخاص، وعن طريق شبكات واي فاي آمنة فقط، حيث إنّ شبكات الواي فاي غير الآمنة تسمح للمخترقين القريبين من التعرض للبيانات الشخصية عند الدخول إلى الإنترنت
- كما ينبغي عدم التسوق من الإنترنت أو القيام بالأمور المصرفية، باستخدام شبكات واي فاي عامة
- حيث إنّه يمكن للمخترقين أن يسرقوا رقم الحساب البنكي أو معلومات مالية أخرى، كما تحتوي الرسائل الفورية وتطبيقات الاتصال الأخرى على ثغرات، تمكن المخترقين من الوصول إلى البيانات الشخصية وسرقتها

حماية البيانات الشخصية أثناء تصفح الإنترنت

اختيار شبكات افتراضية خاصة

توخي الحذر

تحديث البرامج المستخدمة

استخدام شبكات مشفرة

تثبيت متصفح المكونات الإضافية

تشغيل نمط التصفح الخاص

استعادة السيطرة بعد الاختراق

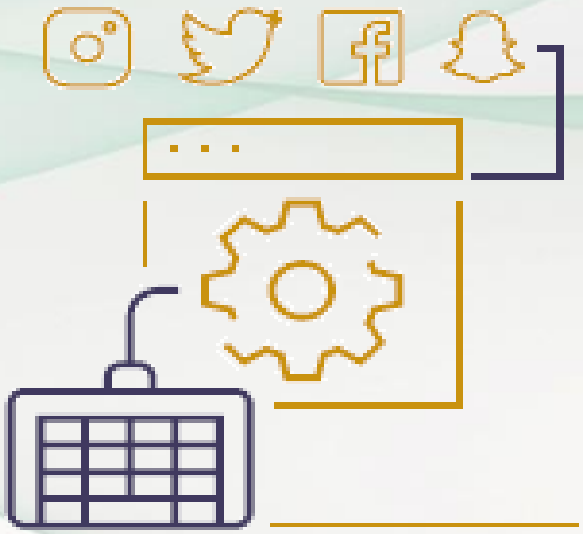
استعادة السيطرة بعد اختراق الجهاز الشخصي

١ فصل جهازك من الإنترنت ليُفصل الرابط بينك وبين المخترق

٢ إعادة تهيئة الجهاز

٣ تثبيت برامج حماية الفايروسات وإجراء فحص شامل للجهاز

٤ استعادة البيانات والمعلومات من النسخ الاحتياطية



استعادة السيطرة بعد اختراق الجهاز الشخصي

١ استعمال جهاز اخر للدخول إلى حساباتك الشخصية وتغيير كلمات المرور

٢ يمكن استعادته باستخدام خاصية نسيان كلمة المرور، ويمكنك في هذه الحالة الاستفادة من عنوان البريد الثانوي (الاحتياطي)

٣ في حال عدم تمكنك من استعادة حساب التواصل الاجتماعي أو البريد الالكتروني يجب التواصل مع الدعم الفني الخاص بالجهة الموفرة للحساب

الجلسة التدريبية الثالثة

التعامل مع مواقع التواصل الاجتماعي

التعامل مع
مواقع التواصل الاجتماعي

حماية حساب تويتر

- الحرص على عدم فتح الروابط التي تصل عن طريق رسائل البريد، لأنه في معظم الأحيان تكون هذه الروابط لاختراق الحساب، وسرقة البيانات الخاصة
- وضع كلمة سر قوية وصعبة، بحيث يصعب على أحد اختراقها
- استخدام مرحلة متقدمة من الحماية، عن طريق طلب رمز لتسجيل الدخول من أي متصفح جديد، بحيث تُرسل على شكل رسالة نصية إلى رقم الهاتف الخاص بنا
- الحرص على عدم مشاركة البيانات الخاصة مع الآخرين
- الحرص على تحديث متصفح الإنترنت والنظام المسؤول عن الموقع
- الانتباه من مختلف التطبيقات التي تتيح إمكانية الدخول إلى تويتر، والتأكد من أمانها وسلامتها

تأمين حساب تويتر

- الذهاب إلى قائمة الإعدادات، ثم الغاء خيار السماح للآخرين بالعثور علينا بواسطة البريد الإلكتروني
- إلغاء إمكانية العثور علينا عن طريق الموقع الجغرافي، وذلك لعدم تحديد مكاننا أثناء التغريد
- تحديد خصوصية التغريد، فلا يستطيع أي أحد قراءة التغريدات
- إدخال رقم الهاتف الخاص بنا، للاستفادة من خدمة الأمان المتقدمة التي لا تسمح بالدخول إلى الحساب إلا بعد إدخال الرمز الذي يصل إلى رقم الهاتف المدخل في الموقع
- إلغاء إمكانية العثور علينا عن طريق رقم الهاتف، وذلك بإزالة الصح الموجود على جانب الخيار

حماية حساب الفيسبوك

وضع كلمة سر قوية على الحساب؛ لأنّ ذلك سيصعب الأمر على المخترق من اختراق الحساب بسهولة، وسيضعف عنصر التخمين لديه

لذا من الأفضل الابتعاد عن وضع كلمات سر سهلة، أو يمكن تخمينها بسهولة كاسم العائلة، أو تاريخ الميلاد، أو تاريخ الزواج، وغير ذلك من المعلومات التي تبدو مألوفة

يجب أن تكون كلمة السر مكونة من ثماني خانات، تحتوي على أرقام، وحروف كبيرة، وصغيرة ورموز

التصفح الآمن

في العادة، لا نقوم بتفعيل خاصية التصفح الآمن في الفيس بوك، وهذه الخاصية موجودة بمسمى تشفير Https، وهذا يجعل القراصنة أو الهاكر يتمكنون من دخول الحساب، والاستيلاء عليه، أو التنصت على ما نقوم به من خلاله، لذا يجب علينا تسجيل الدخول من خلال رابط التشفير الآتي: https

تفعيل خاصية الدخول الآمن Https

ندخل إلى إعدادات الحساب العامة، نختار من بين الخيارات الموجودة خيار الأمان نحرك زر التفعيل لخاصية التصفح الآمن في الفيس بوك عبر اتصال آمن https، ثمّ نضغط أمر حفظ

خاصية إشعارات تسجيل الدخول

من خلال تفعيل هذه الخاصية يقوم فيس بوك بإعلامنا بدخول الهاكر، أو المخترق لحسابنا من خلال أجهزة غريبة لم نستخدمها سابقاً، وذلك من خلال رسالة نصية عبر الهاتف، أو البريد الإلكتروني

تفعيل خاصية إشعارات التسجيل

- ندخل إلى الإعدادات العامة للحساب
- نختار خيار الأمان، ثمّ نختار من بين الخيارات خاصية البريد الإلكتروني وخاصية الرسالة النصية، ثمّ نضغط أمر حفظ

الموافقات على تسجيل الدخول

- تستخدم هذه الخاصية لحماية الهاتف من الاختراق، وذلك من خلال تنبيه يصلنا عبر رسالة نصية على رقم الهاتف المسجل في فيس بوك، حيث تحمل هذه الرسالة رقم سري قوي نقوم بكتابته في الخانة المطلوبة للموافقة على تسجيل الدخول

الإبلاغ عن الإساءة

إذا كانت الشكوى
تتعلق بإزالة الإساءة
فيتم مخاطبة الموقع
المستضيف له

١ الإبلاغ عن الإساءة - تويتر

سياسة المحتوى
وشروط الاستخدام


المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع
السلوك العنيف والتهديدات
انتهاك الخصوصية
انتهاك حقوق النشر والملكية الفكرية
انتحال الشخصية
الإباحية
البرمجيات الخبيثة
الإساءة أو الرسائل المزعجة أو الترويج

٢ الإبلاغ عن الإساءة – سناب تشات ، انستغرام

سياسة المحتوى وشروط الاستخدام

أطلع بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن

- الموقع يشترط أن تبلغ من العمر ١٣ عاماً لتكون مؤهلًا لاستخدامه
- المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية



الإبلاغ

الإبلاغ عن الإساءات التي يتعرض لها المستخدمون، ومن ذلك

الإبلاغ عن الإساءة

كيفية التعامل مع إساءة الاستخدام في
بعض مواقع الشبكات الاجتماعية

الإبلاغ عن الإساءة - خدمة الترشيح

للإبلاغ عن المواقع والمواد التي تتنافى مع الدين والأنظمة الوطنية يمكن طلب حجبها من خلال القنوات التالية

البحث في متاجر
الآيفون والأندرويد

www.filter.sa

block@internet.gove.sa

٠١١ - ٤٦١٩٤٨٥

الإبلاغ عن الإساءة - تطبيق خدمة الترشيح

خطوات طلب حجب أو رفع حجب المواقع الإلكترونية من خلال تطبيق (ترشيح . السعودية)

سلوكي في الفضاء الإلكتروني يصنع


١
المعرفات الشخصية على وسائل التواصل
٢
الأشخاص الذين يتابعونني
٣
المواقع والقنوات التي أشترك فيها
٤
الأجهزة الشخصية التي أستخدمها
٥
الأشخاص الذين أتابعهم

كيف أكون انطباع إيجابي عن نفسي في الفضاء الإلكتروني

المواقع والقنوات التي أشترك فيها

من خلال القنوات المشترك فيها يتحدد الانطباع العام حولك، فكن على حذر من القنوات المشبوهة أو الكيانات الوهمية والغير موثوقة، مثل

الجلسة التدريبية الرابعة

الخصوصية في الفضاء الإلكتروني

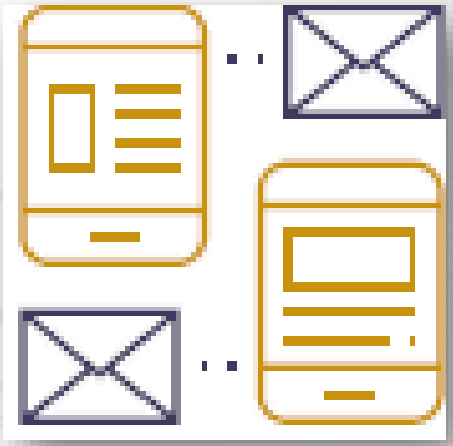
طرق الاختراق


أساليب شهيرة
في الاختراق
١
الاصطياد الإلكتروني
٢
الهندسة الاجتماعية
٣
ملفات طروادة
٤
انتحال الشخصية
٥
الابتزاز الإلكتروني

١ سهولة الوقوع في فخ الاصطياد

٢ تتبع الروابط بدون تدقيق

- يجب التأكد من مصدر الرابط
- لا تقم بفتح روابط تصلك إلى بريدك لزيارة مواقع البنوك
- قم بتهجئة العنوان قبل فتحه
- عدم الوثوق بأي شخص مجهول في الفضاء الإلكتروني
- احذر مواقع التصويتات التي تنتشر من فترة لأخرى



٣ الاسترسال في تتبع الروابط

١ يجب أن يكون هناك ثقافة تجاهل الإعلانات

٢ كثير من البرمجيات الخبيثة تتسلل عن طريق الإعلانات

٤ تحميل البرامج غير الموثوقة

١ تأكد من تحميل البرامج من المتجر الرسمي سواء أندرويد أو أبل

٢ لا تثق بأي دعاية لأي برنامج إلا بعد قراءة التعليقات وتقييم المستخدمين له

٣ حمل ما تحتاج إليه فقط حدث البرامج والتطبيقات من حين لآخر

٤ كما أن هناك اصطياد في المواقع فهناك اصطياد في التطبيقات والفكرة واحدة (سرقة بياناتك)

٥ أخطاء في إدارة كلمات المرور

١ كلمة المرور (سرية لك وحدك)

٢ يجب أن تكون كلمة المرور معقدة بشكل كاف يمنع برامج التخمين من اكتشافها

٣ نوع كلمات المرور ولا تجعلها متطابقة

٤ لا تكتب كلمة المرور مطلقا قريبا من جهازك أو في جيبك

٥ تجنب كلمات المرور المرتبطة بمناسبة معروفة لديك

أنواع الجرائم المعلوماتية

جرائم الاعتداء على الحياة الخاصة

١

المقصود من الحياة الخاصة

ما يقوم به الشخص ولا يرتضي أن يطلع عليه الغير، واعتاد الناس على أن هذا الحق من الخصوصية للشخص

السب والشتم عبر الانترنت

الشتم وهو كل قبيح اعتاد الناس قبحه وسوؤه فتجد بعض المتعاملين بشبكات المعلومات العالمية، يستسهل السب للآخرين وذلك راجع للأسباب التالية

المتعاملين بالإنترنت لا تحدهم حدود جغرافية فنجد الشاتم من بلد والمشتوم من آخر الأمر الذي يأمن معه من الملاحقة القضائية

أن غالب من يرتكب ذلك يختفي وراء أسباب وهمية فيأمن العقوبة في زعمه

٣ إفشاء الأسرار

عن طريق الحاسب يمكن الاعتداء على خصوصيات الأفراد وإفشاء أسرارهم وذلك باستعمال بيانات شخصية حقيقية بدون ترخيص أو إفشاء أسرار بصورة غير قانونية وإساءة استعمالها أو عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عملية جمع ومعالجة ونشر البيانات الشخصية

٤ الابتزاز والتهديد

تهديد الجاني المجني عليه إما بنشر أخباره أو صورة أو معلومات صحيحة ولكن لا يرغب المجني عليه لسبب ما ظهورها للآخرين وإما يهدده بنشر صور أو أخبار أو معلومات غير صحيحة ويقوم بطلب مقابل حتى لا ينشرها سواء كان هذا المقابل مادي أو علاقة غير مشروعة

الابتزاز والتهديد

كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين

الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه

يتضح من النص مجرد فعل التهديد أو الابتزاز كاف لإقامة هذه الجريمة

قد جرم النظام هذا التهديد والابتزاز المعلوماتي حيث نصت المادة الثالثة الفقرة الثانية

جريمة التنصت

من يرتكب جريمة التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو التقاطه أو اعتراضه

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين

جريمة التنصت

أشكال التنصت المعلوماتي

استخدام برنامج في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى جهاز المعتدى عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغرية يزورها المعتدى عليه

استخدام برنامج المحادثة، فيقوم المجرم بإغراء الضحية بأن هذا البرنامج يحتوي على ألعاب مثيرة أو غير ذلك فيقوم الضحية باستقبال الملف

جرائم إساءة استخدام الهواتف النقالة

هذا النوع من الجرائم له العديد من الآثار الاجتماعية والنفسية على مستوى الأفراد، نظراً لما تدخله في نفوس الأفراد من الخوف في الوقوع كضحايا لهذا النوع من الجرائم ولقد ظهرت العديد من المشاكل في المجتمع السعودي نتيجة للاستخدام السيء للجوال

نصت الفقرة الرابعة من المادة الثالثة على أنه

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال او بإحدى العقوبتين

٧ التشهير بالأشخاص

أصبحت هذه الجريمة من أبرز الجرائم الواقعة في الانترنت بل هناك مواقع صممت لأجل التشهير بالأشخاص والتسميع بهم

الاستيلاء والاحتيال المعلوماتي

إساءة استخدام الحاسبات الآلية والتلاعب في نظام المعالجة الالكترونية للبيانات والمعلومات للحصول بغير حق على الأموال أو الخدمات والاستيلاء عليها للمجرم فعليا على مال منقول أو سند أو توقيع هذا السند

يكون الاستيلاء لغيره بأن يسهل للغير الحصول على تلك الأموال بتزويده ببرامج مثلا تسهل تلك الجريمة

السطو على أموال البنوك

يتم ذلك عن طريق استخدام الجاني الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية وتحويل الأموال من تلك الحسابات الخاصة بالعملاء الى حسابات أخرى

تحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها وإتلافها

تقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جداً من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال

السطو على أموال البنوك

الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق ماليه للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات يعاقب بالسجن مدة لا تزيد على ثلاث سنوات بغرامة لا تزيد على مليوني ريال او بإحدى هاتين العقوبتين

قد جرمت هذه الافعال كما في المادة الرابعة الفقرة الثانية

الانتحال والتغرير

الانتحال على صورتين

١ انتحال شخصية فردية

بسبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية

الانتحال والتغرير

الانتحال على صورتين

انتحال شخصية المواقع

يكون باختراق حاجز أمني وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور

الانتحال والتغرير

فيما يخص التغرير فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة حيث يوهم المجرمون ضحايا هذا النوع برغبتهم في تكوين صداقة على الانترنت وقد تتطور إلى التقاء مادي بين الطرفين

نصت المادة الرابعة الفقرة الأولى

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات بغرامة لأتزيد على مليوني ريال بإحدى هاتين العقوبتين

التحريض على الجريمة المعلوماتية

نصت المادة التاسعة من النظام على أنه

يعاقب كل من حرض غيره أو ساعده أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام إذا وقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق

قد جعل المنظم العقوبة على التحريض في الجرائم المعلوماتية مماثلة لعقوبة الفاعل الأصلي للجريمة بل في حال عدم فعل الجاني المعلوماتي وثبت التحريض عليها

بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية

١ الجريمة المعلوماتية الأخلاقية والاتجار بالبشر والاتجار بالمخدرات

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الاتية:

- إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار في الجنس البشري أو تسهيل التعامل به
- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها
- إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرائق تعاطيها

الجريمة المعلوماتية الأمنية

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات

- الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني

الجريمة المعلوماتية الأمنية

نجد أن الفقرة الأولى

- تجرم انشاء موقع لمنظمات إرهابية وقد أصبح الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة المتلاحقة في العصر الحديث
- تحبذ الجماعات الإرهابية من خلال الانترنت انضمام عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر فتعلن الجماعات الإرهابية عبر مواقعها على الانترنت عن حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب مستخدمة في ذلك الجانب الديني.

الجريمة المعلوماتية الأمنية

ما قررته الفقرة الثانية

- التي نصت على الدخول غير المشروع والذي ينصرف معناه ليشمل الافعال كافة التي تسمح بالدخول إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها أو الخدمات التي يقدمها عن مجرد لدخول إلى نظام الحاسب الآلي

- يرتبط مفهوم عدم مشروعية الدخول بمعرفة من له الحق في الدخول إلى نظام الحاسب الآلي ومن ليس له هذا الحق ويدخل في عدم المشروعية حالة دخول العاملين في الجهة التي يوجد بها نظام الحاسب الآلي متجاوزا الصلاحيات الممنوحة له

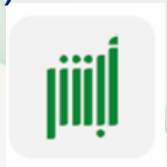
تطبيق كلنا أمن
على الأجهزة الذكية

الشرطة حسب
الاختصاص لمكاني

البريد الإلكتروني
info.cybercrime@moisp.gov
.sa

الاتصال على
الرقم ٩٨٩

البوابة الإلكترونية
لوزارة الداخلية (ابشر)



مرحلة المحاكمة الجزائية تحال الدعوى بعد استكمال مرحلة التحقيق بدعوى عامة تقوم النيابة العامة بالترافع فيها امام المحكمة الجزائية مطالبة بتطبيق المواد الواردة في نظام مكافحة الجرائم المعلوماتية

الاحالة الى النيابة العامة وفي النيابة العامة دوائر متخصصة في التحقيق في الجرائم المعلوماتية تسمى بدوائر المال تقوم هذه الدوائر باستجواب المتهم والتحقيق معه في الجريمة المنسوبة اليه

المواقع الموثوقة على الإنترنت

كثيراً ما يجد المستخدم بعض الخدمات المدفوعة على الإنترنت مثل فك قفل أجهزة "آي فون" على سبيل المثال أو غيرها من الخدمات، إلا أن وثوقيه الموقع قد تكون غير معروفة ومُحيّرة بعض الشيء للمستخدم

لذا يمكن التوجه إلى موقع "http://www.webutation.net" الذي يعطي للمستخدم درجة وثوقيه الموقع وسمعته على الإنترنت اعتماداً على الكثير من أدوات الحماية المتوفرة على الإنترنت

بعد الدخول إلى الموقع، يقوم المستخدم بكتابة رابط الموقع الذي يرغب بالتأكد منه، لتظهر له درجة وتوقيته وسمعته وبعض التعليقات التي تركها المستخدمين

http://www.webutation.net

جهازي مخترق

تثبيت برامج جديدة

يعد تثبيت برامج جديدة على الجهاز من العلامات التي تدلّ على أنّ الجهاز مخترق (مهكر)، وبشكل خاص في حال كان الجهاز مُستخدم من قبل شخص واحد، ومن العلامات التي تشير إلى تثبيت برامج جديدة تلقّي نظام التشغيل التحديثات التي شملت الملفات أو البرامج الجديدة

تواجد حسابات مُستخدمين غير معروفة

يتم التحقق من ذلك من خلال التوجّه إلى لوحة التحكم لفتح القائمة ثم الضغط على خيار حسابات المستخدمين (بالإنجليزية: user accounts)، أو من خلال قائمة ابدأ وكتابة الأمر (cmd)، والضغط على إدخال (بالإنجليزية: enter) لفتح موجّه الأوامر، ثم إدخال (بالإنجليزية: net user) والضغط على إدخال مرةً أخرى

تغيير كلمات المرور عبر الإنترنت

يُغيّر المخترقون في بعض الأحيان وبعد اختراق أي حساب عبر الإنترنت كلمات المرور لحساب أو أكثر، ممّا يؤدّي إلى منع تسجيل الدخول إلى الحساب؛ لذلك يُنصح باستخدام ميّزة إعادة تعيين كلمة المرور عند نسيانها، أو الاتصال بالشركة التي تقدّم الخدمة لإعادة

بعض العلامات التي تدل على اختراق الجهاز، ومنها

١. إلغاء تثبيت أو تعطيل برامج مكافحة الفيروسات؛ بسبب قيام المخترق بتعطيل هذه البرامج بهدف مساعدته على إخفاء أيّ تحذيرات قد تظهر على الجهاز

٢. إجراء الجهاز عدّة نشاطات من تلقاء نفسه، مثل تحرك مؤشر الماوس وحده

٣. تغيير كلمة مرور الجهاز: يدلّ تغيير كلمة المرور لتسجيل الدخول إلى الجهاز من تلقاء نفسها على اختراق الجهاز

٤. زيادة نشاط الشبكة: تدلّ زيادة نشاط الشبكة، وتباطؤ سرعة الإنترنت على الاتصال بالجهاز عن بُعد

عزل الجهاز

تثبيت التحديثات
الجديدة على الجهاز

إزالة القرص الصلب

نسخ الملفات المهمّة

استخدام برامج
لمكافحة التجسس

إعادة تحميل نظام التشغيل
من الوسائط الموثوق فيها

التدريب خيار أصيل ..
وليس حل بديل

hail4321

Suhail_asiri

Moooj

suhail1972

hail4321

0505757427

hail4321

hail4321@hotmail.com

hail4321@gmail.com

Suhail Abu Zuhair

تأكد من إيقاف نظام تحديد المواقع على كاميرا الهاتف الذكي

لا تفعل خاصية حفظ اسم المستخدم وكلمات المرور لتسجيل الدخول التلقائي للمواقع والتطبيقات

اختر كلمات مرور يصعب تخمينها وتذكر تغييرها بانتظام

تأكد من استخدام كلمات مرور مختلفة لحسابات التواصل الاجتماعي

احذف بياناتك الشخصية على حساب التواصل الاجتماعي الذي توقفت عن استخدامه وقم بإلغائه

اجهزتك من سرقه المعلومات

ضع جدار ناري للحماية

قم بتحديث برامج التصفح وانظمة التشغيل بشكل مستمر

ضع برامج لمكافحة الفيروسات

قم بازالة الملفات المؤقتة

تنجنب تحميل الملفات من المواقع الغير موثوقه

توخى الحذر عند فتح الرسائل مجهولة المصدر

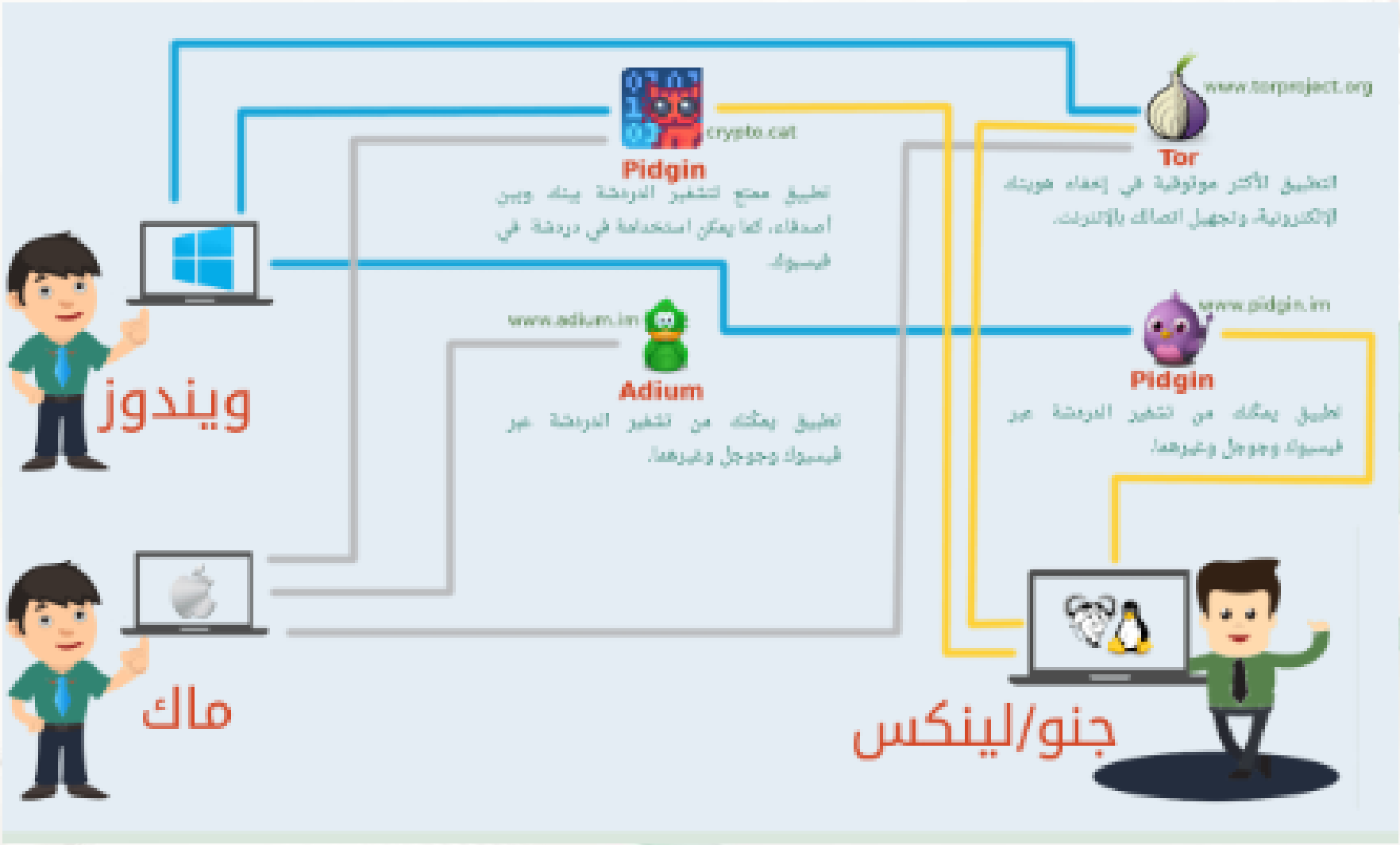
استخدم كلمة مرور معقدة وطويلة

استخدم متصفح امن

قم بتشفير جهاز الراوتر

احم خصوصيتك الرقمية

مجموعة تطبيقات للهواتف المحمولة تعمل على أنظمة التشغيل Android و iOS، ومجموعة برمجيات تعمل على أنظمة التشغيل؛ ويندوز ، وجنو/لينكس، وماك.


www.torproject.org
Tor
التطبيق الأكثر موثوقية في إخفاء هويتك الإلكترونية وتجهيل اتصالك بالإنترنت.
crypto.cat
Pidgin
تطبيق ممتع لتشفير الدردشة بينك وبين أصدقاء، كما يمكن استخدامه في دردشة في فيسبوك.
www.adium.im
Adium
تطبيق يمكنك من تشفير الدردشة عبر فيسبوك وجوجل وغيرهما.
www.pidgin.im
Pidgin
تطبيق يمكنك من تشفير الدردشة عبر فيسبوك وجوجل وغيرهما.
ويندوز
ماك
جنو/لينكس


كيف تحفظ
١٠٠٠٠٠٠ كلمة مرور بسهولة
أجعل لنفسك قاعدة ترجع إليها عند اختيار كلمات المرور الخاصة بحساباتك الإلكترونية
مثلاً، سنستخدم القانون التالي كقاعدة عامة لإنشاء كلمة مرور طولها ١٠ أحرف
١ الحرف الاول والثاني من اسم المستخدم ahmad
٢ علامة "&" (مكررة مرتان)
٣ الحرف الاول والثاني من اسم الموقع (أحرف صغيرة)
٤ عدد أحرف اسم الموقع (مكررة مرتان)
٥ الحرف الاول والثاني من اسم الموقع (أحرف كبيرة)
ah&&tw77TW
إذاً كلمة المرور في تويتر twitter.com
ah&&mo33MO
و كلمة المرور في أبشر mol.gov.sa كالتالي
بعض المواقع مثل البنوك تمنع استخدام بعض الرموز مثل $ و الأقواس فيُنصح إنشاء قاعدة ملائمة.
يمكنك ابتكار قاعدة خاصة بك بطرق مختلفة وسهلة الحفظ وملائمة، مثلاً: أول حرف وأخر حرف، ثم أول حرف مكرر، ثم علامتان #^، ثم نوع النطاق com أو net، ..... إلخ
فائدة هذه الطريقة
سهلة التذكر
لن تحتاج إلى تكرار نفس كلمة المرور لكل حساب ولا لكتابتها.
يصعب استنتاج القاعدة الأساسية
حتى لو تم كشف كلمة المرور باختراق الحساب فإنه يصعب استنتاج هذه القاعدة.
صعبة التخمين
لن يكون بمقدور المخترق تخمينها ولا تستطيع أدوات كشف كلمات المرور تخمينها.

خطوات لحماية شبكة الانترنت المنزلية من الاختراق

احرص على استخدام كابل " الإيثرنت" عند تسجيل الدخول لصفحة الراوتر و إعداده

قم بتغيير اسم المستخدم و كلمة المرور الافتراضية واجعل كلمة المرور قوية

قم بتغيير اسم الشبكة الافتراضي

قم بتغيير وضع مصادقة الـ Wireless الى "WPA / WPA2"

قم بتغيير تشفير الـ Wireless الى "AES & TKIP"

قم بتفعيل الجدار الناري (Firewall)

قم بتعطيل خدمة الـ WPS وخدمة الـ UPnP

قم بتحديث الـ Firmware الخاص بالراوتر الى اخر اصدار

اذا كان مستخدمين الشبكة محدودين فقم بوضع فلتر القائمة البيضاء لعناوين الـ MAC Address بحيث لا يستطيع اي ان يرتبط بالشبكة مالم يكن عنوان الـ MAC الخاص به في القائمة حتى ولو تمكن من الحصول على كلمة مرور الشبكة

من المهم جداً القيام بحماية الشبكة المنزلية من الاختراقات و الهجمات للحرص على امن الاجهزة المرتبطة بالشبكة

IN 60 SECONDS v2

710 COMPUTERS SOLD

232 COMPUTERS GOT INFECTED BY MALWARE

2,6 MILLION CD'S

1,820 TB OF DATA CREATED

450 Windows 7 CDs SOLD

12 WEBSITES GOT HACKED

416 ATTEMPTS

redbox

1,400 DISCS ARE RENTED ON ONLINE MOVIE RENTAL SERVICE

180+ BY MOBILE

ebay

555 OF THEM WITH intel

81 iPad SOLD

925 iPhone 4 S SOLD

ebay

950+ PURCHASES ON

$10,000 BY MOBILE

PayPal

$219,000 OF TOTAL PAYMENTS

11 XBOX 360 CONSOLES SOLD

1,100 ACRES OF LAND FARMED IN FARMVILLE

18 amazon.com kindle fire

103 BlackBerry SOLD

11 MILLION CONVERSATIONS ON INSTANT MESSENGERS

38 tons E-WASTE GENERATED

4,000 USB DEVICES SOLD

2,500 INK CARTRIDGES SOLD

2,100 foursquare CHECK-INS

$ 75,000 ADDED TO Google REVENUES

2 MILLION INTERNET USERS WATCHED PORN ONLINE

compiled & designed by:
GO-Globe.com


44,000,000
MESSAGES PROCESSED
486,000
PHOTOS
26
NEW REVIEWS
POSTED ON YELP
120
NEW ACCOUNTS
OPENED ON
LINKEDIN
MORE THAN
140
SUBMISSIONS
ON REDDIT
MORE THAN
2,315,000
SEARCHES
3,125,000
243,055
MORE THAN
21,000,000
MESSAGES SENT
70,000
VIDEO MESSAGES
SHARED
Share
MORE THAN
3,000,000
ITEMS ARE
SHARED
MORE THAN
18,000
MATCHES MADE
MORE THAN
195,000
MINUTES OF AUDIO CHATTING
ON WECHAT
972,000
DAILY SWIPES
ON TINDER
IN
60
SECONDS
GO-Globe
CUSTOM WEB DEVELOPMENT
MORE THAN
69,500
HOURS OF
VIDEO WATCHED
ON NETFLIX
NETFLIX
MORE THAN
150,000,000
E-MAILS ARE SENT
MORE THAN
48,000
APPS DOWNLOADED
ON IPHONE
MORE THAN
95,000
APPS DOWNLOADED
ON ANDROID
YouTube
MORE THAN
430,000
TWEETS SENT
MORE THAN
2,700,000
VIDEO VIEWS AND
139,000 HOURS
OF VIDEO WATCHED
MORE THAN
39,300
HOURS OF MUSIC
LISTENED
AROUND
56,000
PHOTOS
UPLOADED
9,800
ARTICLES PINNED
ON PINTEREST
MORE THAN
280,000
SNAPS SENT
ON SNAPCHAT
MORE THAN
100
NEW DOMAINS
REGISTERED
14 NEW
SONGS ADDED
ON SPOTIFY
MORE THAN
300 HOURS
OF VIDEO ARE UPLOADED

ثلث مستخدمى الانترنت ينامون فقط

٥ - ٦ ساعات

طوال الليل

نصف الساعات التى تقضيها فى المشى طوال اليوم تقضيها ناظرا الى شاشة هاتفك

جميع اضطرابات النوم تقريبا بسبب

استخدام الانترنت

قبل النوم

٤٦%

يشاهدون التليفزيون قبل الانترنت على

هواتفهم الذكية

٢٠%

ينتظرون قبل النوم دائما للبدء فى ارسال الرسائل النصية للاصدقاء والاحباب

٧٠%

منا لدية تليفزيون داخل غرفة نومه بالمقارنة بـ

٥٧%

منذ عشرة سنوات


٥٢%
ينتظرون رسائل نصية جديدة قبل النوم واثناء النوم ايضا
ازدياد اضطرابات النوم بعد ظهور الهواتف عام
١٩٧٣
SAMSUNG
٦٠%
يستخدمون اجهزتهم اللوحية قبل النوم
٥١%
يتفقدون رسائلهم باستمرار قبل النوم
تقليل عدد ساعات النوم بعد ظهور الرسائل النصية عام
١٩٨٢
٤١% يقرأون الكتب قبل النوم
٧٠%
يذهبون الى مواقع التواصل الاجتماعى قبل النوم لتحديث حالتهم وتفقد الجديد من الاصدقاء
٧٩%
يتفقدون ماهو جديد على الويب باستمرار قبل الذهاب للنوم
٢٢%
يستخدمون أجهزتهم المحمولة قبل النوم
١٦%
ينامون بشكل سئ وقد لا ينامون بسبب تفقد وارسال الايميلات قبل النوم