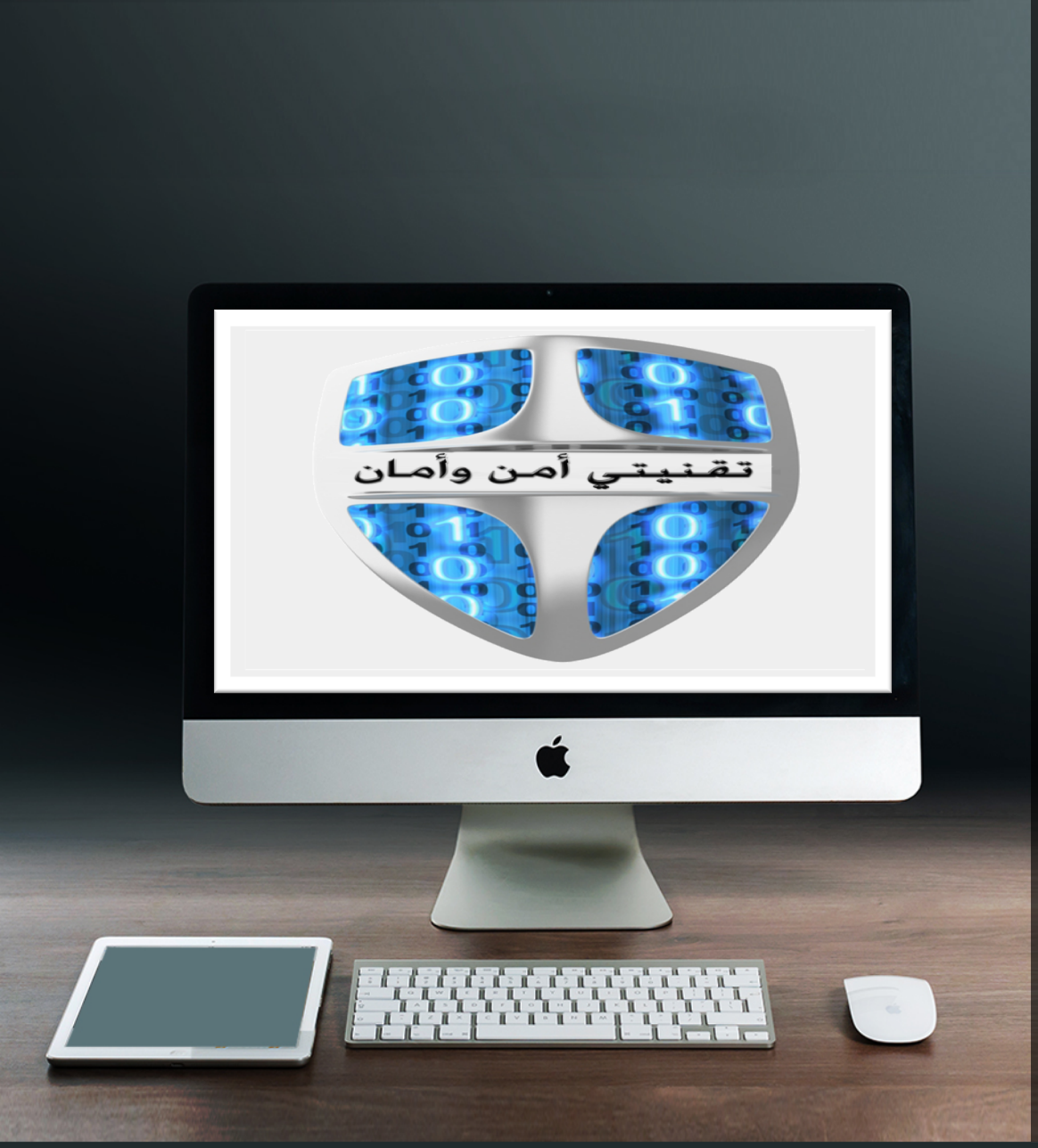


محاضرة بعنوان
(كيف أحمي خصوصيتي على الجوال)

المدربة
عواطف بنت احمد العوبثاني

مدرب معتمد في أكاديميات سيسكو للتدريب.
عضو مركز ماسترز البريطاني للتدريب والاستشارات

المدربة في سطور

- عواطف بنت أحمد العوبثاني.
- مدرب معتمد في أكاديميات سيسكو لتدريب الحاسب الآلي.
- عضو في مركز ماسترز البريطاني للتدريب والاستشارات.
- مهندسة حاسب آلي
- عدد سنوات الخبرة: 14سنة في مجال الـــــــــ (I T).

- **الشهادات العلمية**
- بكالريوس علم النفس العام من جامعة العلوم والتكنولوجيا.
- دبلوم تقنيات الشبكات معتمد من المؤسسة العامة للتدريب التقني والمهني
- كورس مكثف في CEH (certified ethical hacker)

- CCNA EXPLORATION: NETWORK FNDAMENTALS
- IT ESSENTIALS: PC HARDWARE AND SOFTWARE
- ICDL 2010

هدف اللقاء:

رفع مستوى الوعي التقني في أمن المعلومات لدى المستخدمين، ومعرفة المخاطر التي تواجههم على الشبكة العنكبوتية و كيفية تفادي هذه الأخطار والحماية منها.

المحاور الرئيسية

- مقدمة في عالم الاختراق
- أنظمة تشغيل الجوالات
- مخاطر تهدد أجهزة وتطبيقات الجوال

المحاور الرئيسية

- أشهر أساليب الاختراق.
- حماية الجوال والحد من الاختراقات والتسريبات
- كيف أحمي بياناتي Data security
- كيف احمي حساباتي الشخصية

مقدمة في عالم الاختراق

الاختراق

هناك الكثير من الناس ممّن يعانونَ من مشاكل يعود سببها إلى اختراق الأجهزة الخاصة بهم من قبل المتطفلين، الأمر الذي يجعل بياناتهم وملفاتهم معرضة للخطر والتسرب، لذا سوف نقوم في هذه الدورة بالحديث عن أهمّ الخطوات التي تمكن جميع المستخدمين من حماية أجهزتهم من الاختراق ومشاكله.

ما هو الاختراق؟ وماهي دوافعه ؟

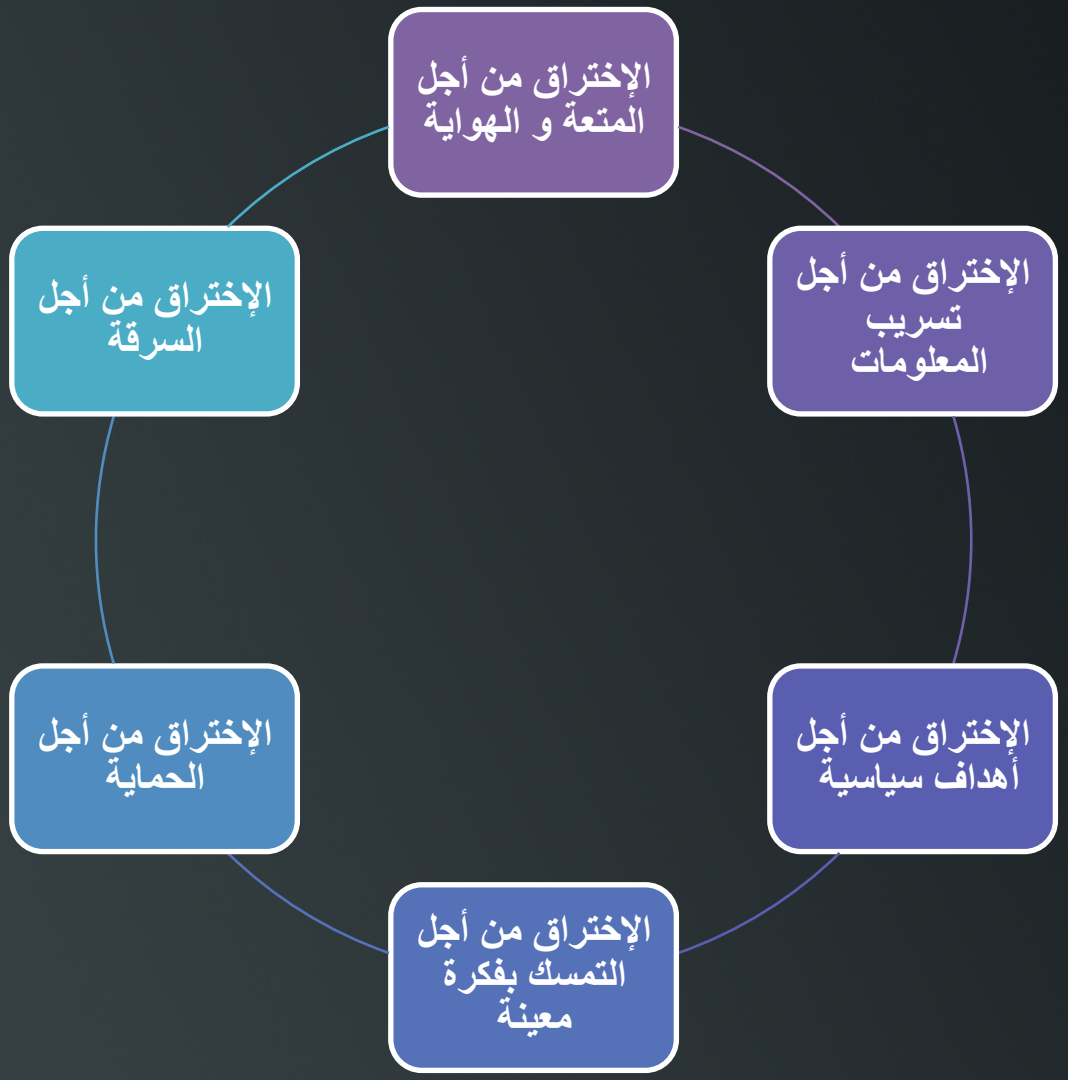
مقدمة في عالم الاختراق

اختراق الهواتف المحمولة

إنَّ ما يعنيه مُصطلح **الاختراق** في أمن المعلومات هو حدوث **تدخُّل خارجيّ** غير مَرغوب للجهاز أو النّظام، بحيث يستطيع المُخترِق أن يتحكَّم بكامل نظام الجهاز أو جزء منهُ، **أو إحداث تغيير في إعدادات فيه**، أو القُدرة على **الحصول على معلومات من داخل النّظام أو الجهاز** دون إذن الضّحيّة، وبدون مُخوِّلات

ما هي أسباب الاختراق ودوافعه الخفية

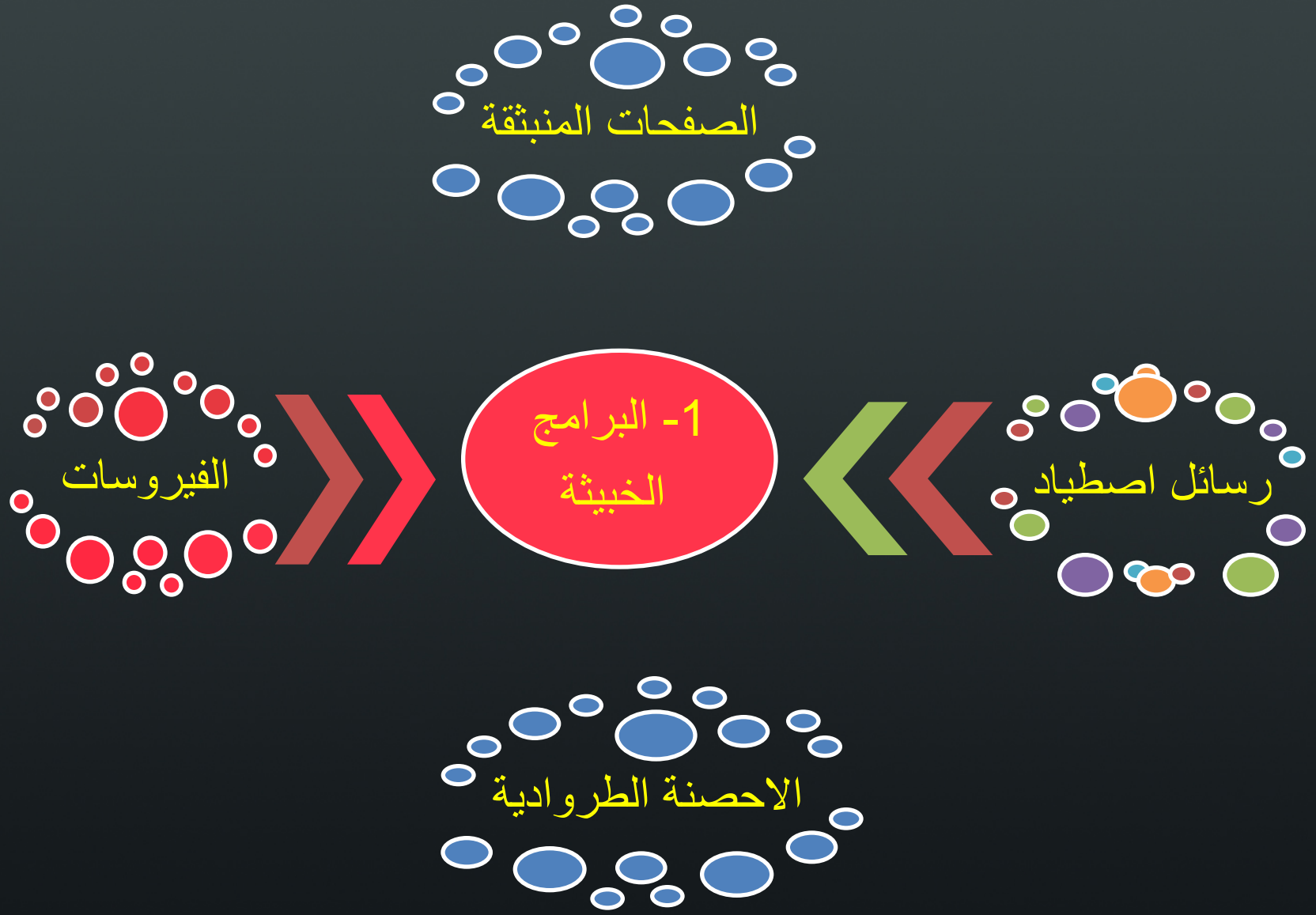
مقدمة في عالم الاختراق



أنظمة تشغيل الجوالات: Operating Systems

يتمتع نظاما التشغيل ios من آبل و android من قوقل بهيمنة مطلقة على أنظمة تشغيل الهواتف الذكية، حيث يمثلان ما نسبته 99.9% من السوق العالمية، وذلك وفقاً لتقديرات شركة أبحاث السوق قارتنر

ماهي مواطن الخطر أو نقاط الضعف في الجوال؟


الصفحات المنبثقة
الفيروسات
1- البرامج الخبيثة
رسائل اصطياد
الاحصنة الطروادية

تعريف البرامج الخبيثة: Malware

البرامج الخبيثة هي أي برنامج يكون كل مهامه أو أحدها عمل خبيث من تجسس وتخريب أو استتراف للموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي، وغيرها....)

مكان تواجد البرمجيات الخبيثة:

تختبئ البرمجيات الخبيثة داخل التطبيقات الأكثر شعبية.

البرامج الخبيثة

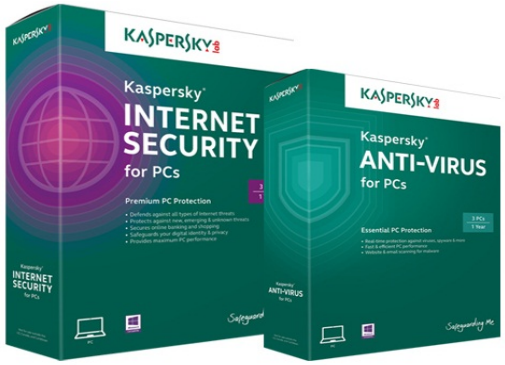
نوع البرنامج الخبيثة	تعريف البرنامج	النشاط التخريبي	الوقاية منه
الفايروسات	برنامج صغير مكتوب بأحد لغات الحاسب.	بطئ الجهاز كثرة التجميد	تثبيت برامج حماية والنسخ الاحتياطية
الاحصنة الطروادية	شفرة تزرع داخل البرامج ذات الشعبية	التجسس سرقة معلومات	برنامج الجدر النارية للتحكم بالمنافذ Firewall الغير آمنة، وبالتالي قطع الصلة بالمهاجم.
رسائل الاصطياد	يتم ارسال رسالة بريد الكتروني تبدو مفيدة لتسجيل بياناتك في موقع مفيد من خلال ارفاق الرابط	سرقة معلومات وبيانات شخصية وتحويلات مالية	تأكد من وجود القفل في صفحة الانترنت
الاعلانات المنبثقة	صفحات تظهر بدون امر فتحها	كثرة الصفحات الانبثاقية جهازك يحاول الاتصال بخط الهاتف بدون أمرك الجهاز يصبح بطيء صفحة البداية تتغير	برنامج مكافحة الفيروسات+ الجدر الحماية النارية

طرق الوقاية من البرامج الخبيثة:

- استخدم برنامج مكافحة الفيروسات، وحدثه دورياً، ليتسنى للبرنامج التعرف على الفيروسات

موقع لمنظمة غير ربحية تقوم باختبار برامج المكافحات بشكل دوري
وتظهر أفضل عشرة برامج
https://www.av-test.org/en/antivirus/home-macos/

AVG



Norton by Symantec

Avira

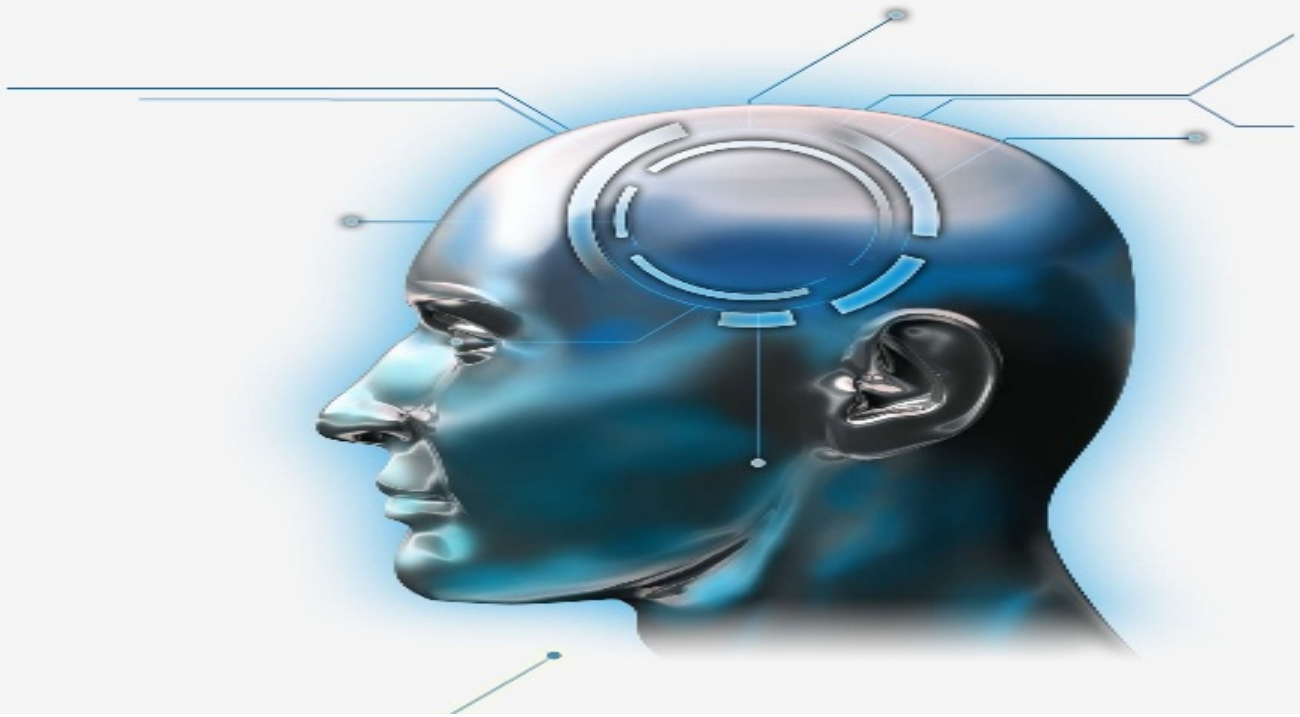
كيف انتقي تطبيقاتي من المتجر

استخدام تطبيقات بشكل أمن

- تجنب التطبيقات الجديدة
- تجنب التطبيقات التي لم يقم بتحميلها إلا عدد قليل من المستخدمين.
- تجنب تطبيقات التي لديها عدد قليل من التعليقات الايجابية.
- كما كلما مضى وقت طويل على وجود التطبيق في المتجر كلما كان من الارجح انه موثوق به.
- اذا توقفت عن استخدام تطبيق معين قمِ بإزالته من جهازك .
- الصلاحيات: كثير من التطبيقات تسأل عن رصد مواقعك الجغرافي في حالة الموافقة من الممكن ان يتم رصد تحركاتك ومن الممكن تباع هذ المعلومات لآخرين.
- تحديث التطبيقات: تحديث تلقائي وأتأكد أن كل التطبيقات تم تحديثها

أشهر أساليب الاختراق: Social engineering

الهندسة الاجتماعية



أشهر أساليب الاختراق

مفهوم الهندسة الاجتماعية

عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس
يقومون بعمل ما أو يفصحون عن معلومات سرية وشخصية.

أشهر أساليب الاختراق: الهندسة الاجتماعية

موضوع الهندسة الاجتماعية هي فقط اللعب على الإنسان وكسب الثقة بشكل مخادع، ويمتد لأكثر من طريقة لا يمكن تخيلها، فمثلا قد يقوم المخترق بالبحث في المهملات للعثور على اي من المعلومات واستغلالها ضد الضحية.

أمامي علبة من الأقلام، كم قلم متوفر داخل هذه العلبة:

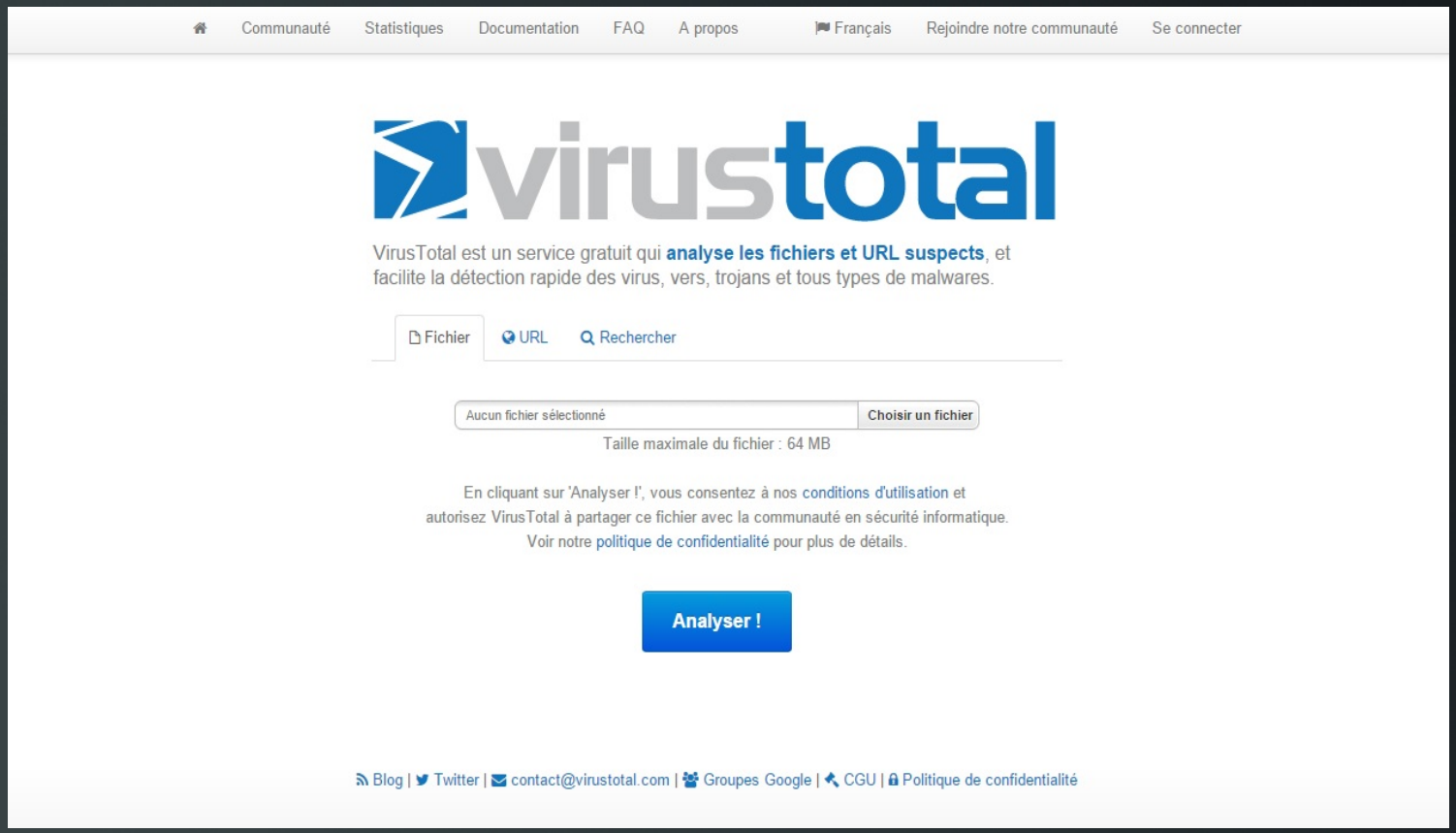
- لا يوجد علبة في الأصل
- خمسة أقلام
- لا أدري
- يجب التحقق
- بين الـ 20 والـ 30

- التحقق من صحة الرابط

https://www.google.com

فايروس توتال - VirusTotal

موقع لفحص الروابط والتطبيقات المقرصنة



احذر من تسمية شبكتك باسمك الصريح أو تثبيت برامج الواي فاي المفتوح

برامج التنصت على الشبكات وكشف مسمياتها

الحذر من شبكات الواي فاي العامة (النقاط الساخنة)

يوجد اتصال انترنت مجاني في مول أو فندق هل تقوم بالاتصال به ؟

احد أهم طرق اختراق الجوال بمجرد الاتصال بشبكة مفتوحه قد تتسبب في فقدان واختراق حساباتك

المحور الخامس: حماية الجوال والحد من الاختراقات والتسريبات

وضع عدة طبقات حماية على الجوال وهي كالتالي:

- استخدام متصفح آمن
- تحديث تطبيقات الجوال باستمرار
- تحديث نظام تشغيل الجوال باستمرار
- تثبيت مكافح فايروسات أصلي وتحديثه
- تركيب الجدار الناري Firewall

كيف أحمي بياناتي Data security

حماية البيانات الشخصية

كيف أحمي بياناتي

Data security

1- حماية المعلومات الشخصية عن طريق التشفير

الارقام- عناوين- الصور الخاصة – قاعدة بيانات مالية....الخ

الدخول على الإعدادات ثم التخزين ثم اختيار تخزين ذاكرة الهاتف ثم تفعيل التشفير في أسفل الخيارات

2- حماية الخصوصية عن طريق إخفاء البيانات

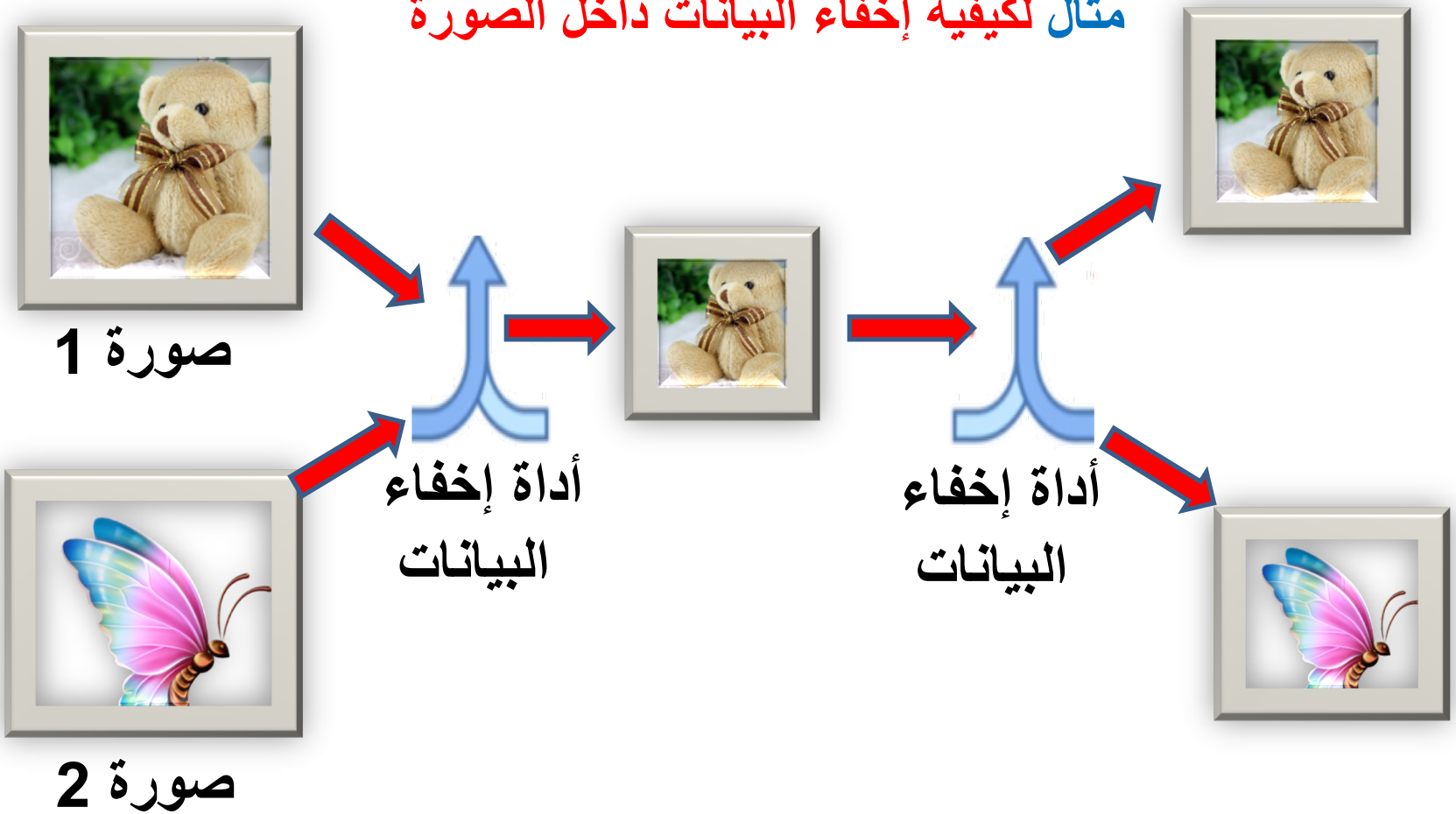
علم إخفاء البيانات (Steganography)

2- حماية الخصوصية عن طريق إخفاء البيانات

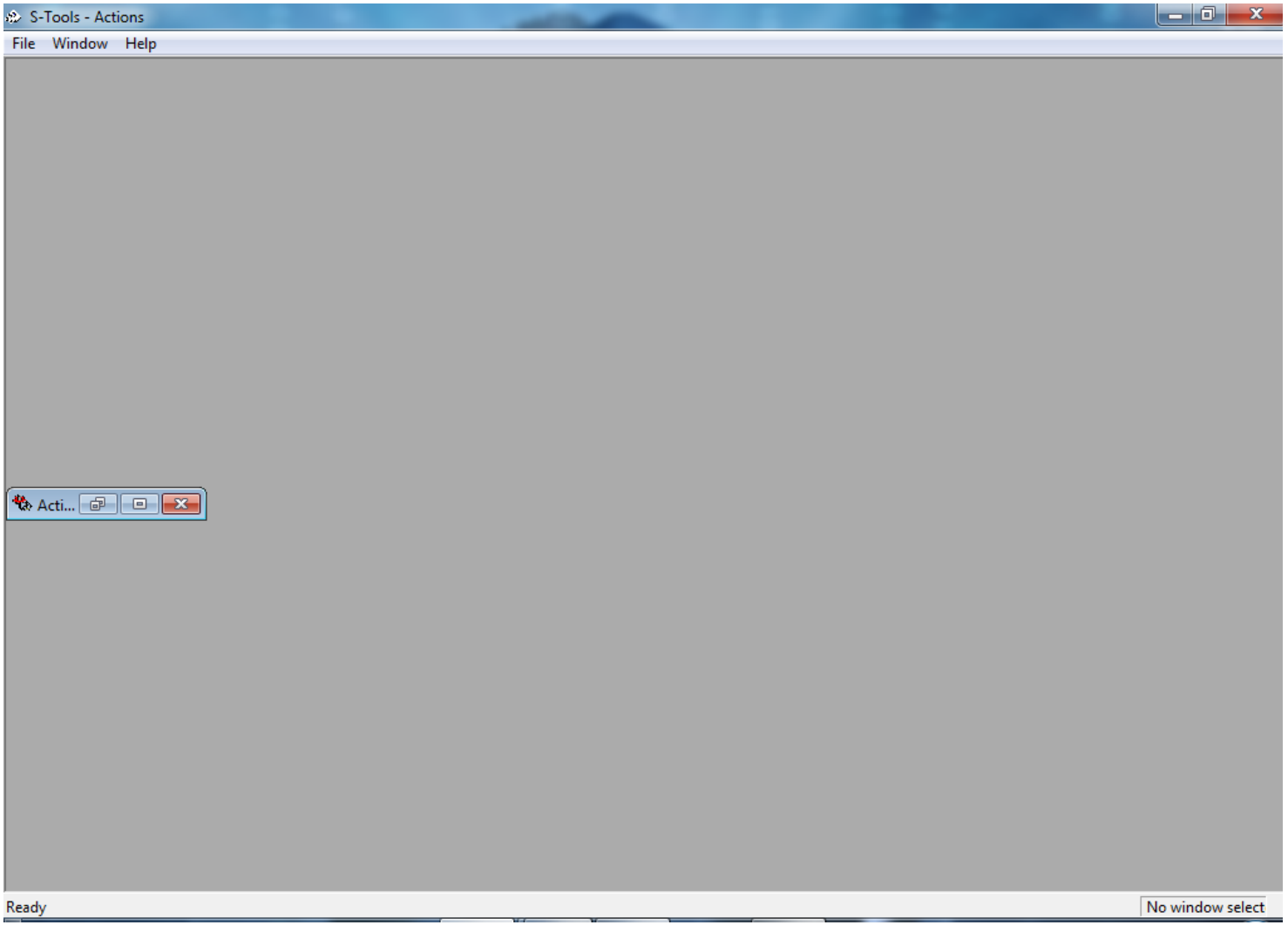

طريقة اخفاء الملفات داخل صوره


Q3_Financial_Pla
nuls
SOW-T187.docx
SOW-T327.pptx
SOW-T189.docx
SOW-T320.pptx

مثال لكيفية إخفاء البيانات داخل الصورة



أداة الإخفاء الشهيرة
S-TOOLS



3- الحماية من التعقب أثناء تصفح الانترنت

التصفح الآمن من خلال تفعيل ميزة التصفح الشبح (التخفي)

عند استخدام علامات التبويب□□□□□ □□ □□، لا يتم حفظ بيانات الاستعراض (مثل ملفا ت
تعريف الارتباط، أو السجل أو الملفات المؤقتة) على الكمبيوتر عند الانتهاء، يحذف متصفح الإنترنت البيانات المؤقتة من الكمبيوتر الخاص بك بعد غلق كل علامات التبويب □□□□ □□ □□□

خطوات التصفح الآمن (التخفي)

الذهاب إلى قائمة إعدادات المتصفح
ثم النقر على خيار نافذة جديدة
للتصفح الخفي

3- الحماية من التعقب أثناء تصفح الانترنت

موقع يجمع معلوماتي وتنقلاتي على الانترنت:My Activity.google.com

3- وضع كلمة مرور قوية للجهاز

P@$$W0RD

****

تجربة مدى قوة كلمة المرور : http://www.passwordmeter.com/

كلمات المرور الضعيفة

password12345
123456 123456789 abc123
DEFAULT 12345678
1234567 qwerty

- الارقام فقط
- الاحرف فقط
- الأسم الشخصي
- تاريخ الميلاد
- رقم الهاتف - الجوال
- اسم الأم او الاب او العائلة

كلمات المرور القوية

4ET%1ge6 ✓

1234 ✗

- أرقام وأحرف وعلامات مثل !@#$%^&*

عند توقف جهازي الموبايل عن العمل فالطريقة الصحيحة للتخلص منه:

أن أقوم بحذف بياناتي بشكل

نهائي (إعادة ضبط المصنع)

إذا توقفت من استخدام حساباتي،

لابد من حذف الحساب نهائياً وليس

فقط الخروج من الحساب.

إذا انسرق جوالك فهذه أهم خطوتين تقوم بها مباشرة:

1- تتبع مكان جوالك عبر الصفحة التالية:

الآيفون:

https://t.co/G9yqAWPpqB

الاندرويد:

https://t.co/dAIn0db8Pg

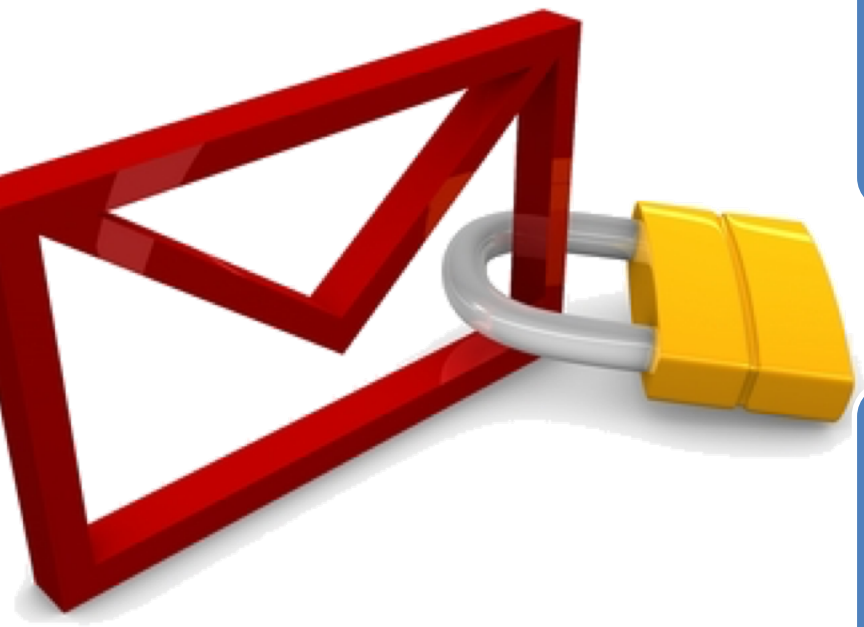
ثم بلغ الشرطة

2- اتصل بشركة الاتصالات وأعطهم رقم IMEI للجهاز ليتم حجبه "لاستخراجه اتصل على (*#06#)

المحور السابع: كيف أحمي حساباتي من السرقة (الإيميل - الواتساب - برامج السوشيال ميديا)

المحور السابع: كيف أحمي حساباتي من السرقة
(الإيميل - الواتساب - برامج السوشيال ميديا)

طريقة حماية الإيميل



- الحماية من الفيروسات
- عدم فتح إيميل مجهول
- كلمة مرور قوية
- الدخول من الأجهزة الموثوقة
- التحقق بوسيلة اتصال (التحقق الثنائي 2FA)

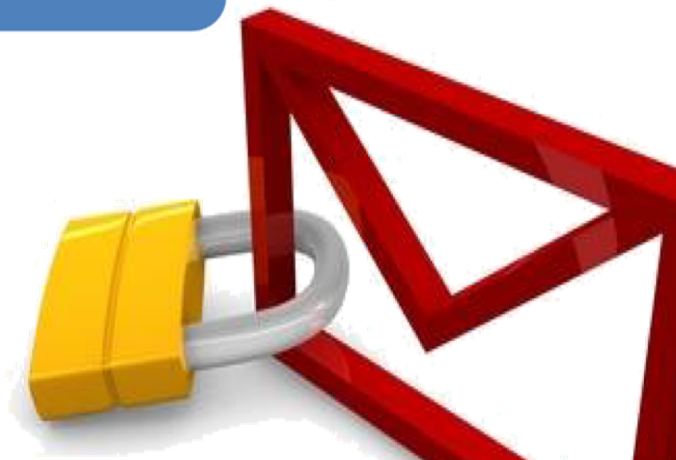
المحور السابع: كيف أحمي حساباتي من السرقة (الإيميل - الواتساب - برامج السوشيال ميديا)

التحقق الثنائي من خلال تطبيق المصادقة

google Authenticator

التحقق بوسيلة اتصال (التحقق الثنائي 2FA) من خلال تطبيقات المصادقة ومن أشهرها تطبيق

Google Authenticator



تطبيق عملي لحماية البريد الالكتروني

المحور السابع: كيف أحمي حساباتي من السرقة (الإيميل - الواتساب - برامج السوشيال ميديا)

طريقة حماية الواتساب

- الحماية من الفيروسات
- عدم ترك جهازي في مكان عام
- عدم فتح أي رابط مجهول
- تحديث البرنامج باستمرار
- وضع كلمة مرور قوية للتطبيقات
- التحقق بوسيلة اتصال (التحقق الثنائي 2FA)

المحور السابع: كيف أحمي حساباتي من السرقة (الإيميل - الواتساب - برامج السوشيال ميديا)

طريقة حماية برامج السوشيال ميديا

- الحماية من الفيروسات
- عدم ترك جهازي في مكان عام
- عدم فتح أي رابط مجهول
- تحديث البرنامج باستمرار
- وضع كلمة مرور قوية للتطبيقات
- التحقق بوسيلة اتصال (التحقق الثنائي 2FA)

الملخص و أهم التنبيهات

- **** احمي اجهزتك بكلمة سر
- تحميل برنامج مضاد للفيروسات
- الحذر في استعمال الواي فاي العمومي
- قم بتحديث جهازك بشكل مستمر

تطبيقات تهمك

XRAY: برنامج يكشف لك الثغرات بجوالك ويقوم بغلقها مباشرة مهم جداً للحماية.

Active password: برنامج مهم لفتح جهاز الحاسوب بدون كلمة مرور يتم تثبيت البرنامج على فلاشة وادخالها بالجهاز وقت بدء التشغيل

شكراً لحسن إنصاتكم
كفارة المجلس

إعداد وتقديم
عواطف بنت أحمد العوبثاني

للتواصل وطلب الاستشارة:

 Awatefahmad

 Awatef Ahmed

 @hemmam555

 awatef1430@gmail.com

 @informationSecurity1