
بسم الله الرحمن الرحيم

وزارة التعليم
Ministry of Education

NCEPD

الأمن السيبراني

الهدف العام

التعرف على أساسيات الأمن السيبراني

واستراتيجياته.

الأهداف التفصيلية

أنواع الهجمات

عناصر أمن المعلومات

التصيد الإلكتروني

مفهوم الأمن السيبراني

البرمجيات الخبيثة

إحصائيات وأرقام في الأمن السيبراني

كلمات السر

مجالات ومخاطر الإنترنت

الأهداف التفصيلية

اختراقات عالمية

اختراقات محلية

العيون الخمسة

بعض أساليب الحماية من الاختراقات

قصة سفر الملفات

التشفير

إحصائيات وأرقام في الأمن السيبراني

جهود المملكة العربية السعودية في الأمن السيبراني

خطة البرنامج التدريبي

اليوم التدريبي	العنوان	الموضوع/الموضوعات	الهدف	الزمن
الأول	مقدمة في أساسيات الأمن السيبراني	مصطلحات وتعريفات الفرق بين امن المعلومات والأمن السيبراني أهداف الأمن السيبراني نظرة تاريخية عن أبرز الهجمات طرق الاختراق	التعرف على أشهر مصطلحات الأمن السيبراني. التفريق بن أمن المعلومات والأمن السيبراني التعرف على اهداف الأمن السيبراني الاطلاع على تاريخ الأمن السيبراني التعرف على بعض طرق الاختراق	٤ ساعات
الثاني	الجرائم المعلوماتية	الجرائم المعلوماتية أساليب الحماية من الهجوم السيبراني	التعرف على الجرائم المعلوماتية تطبيق بعض أساليب الحماية من الهجوم السيبراني	٤ ساعات
الثالث	البرامج الخبيثة	الفيروسات الديدان احصنة طروادة خبراء ومجرمي الأمن السيبراني	التعرف على أشهر البرمجيات الخبيثة وطرق عملها. التعرف على خبراء ومجرمي الأمن السيبراني ودور كل منهم.	٤ ساعات

خطة البرنامج التدريبي

اليوم التدريبي	الجلسة التدريبية	العنوان	الموضوع/الموضوعات	الهدف/ المحور	الزمن
الأول	الأولى	مقدمة في أساسيات الأمن السيبراني	مصطلحات وتعريفات الفرق بين امن المعلومات والأمن السيبراني أهداف الأمن السيبراني	التعرف على أشهر مصطلحات الأمن السيبراني. التفريق بن أمن المعلومات والأمن السيبراني التعرف على اهداف الأمن السيبراني	٩٠ دقيقة
		استراحة			٢٠ دقيقة
	الثانية	مقدمة في أساسيات الأمن السيبراني	نظرة تاريخية عن أبرز الهجمات	الاطلاع على تاريخ الأمن السيبراني	٦٠ دقيقة
		استراحة			١٠ دقائق
	الثالثة	مقدمة في أساسيات الأمن السيبراني	طرق الاختراق	التعرف على بعض طرق الاختراق	٦٠ دقيقة

الجلسة التدريبية الأولى

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١. ١ من كل ٣٦ جهاز معرض للاختراق بسبب تطبيقات غير موثوقة. المصدر: (Symantec)

٢. يتم برمجة ٣٠٠,٠٠٠ برمجية خبيثة يومياً. المصدر: (McAfee)

٣. كل ٣٩ ثانية، تحدث هجمة إلكترونية. المصدر: (security magazine)

٤. يتم سرقة ٧٥ سجل كل ثانية. المصدر: المصدر: (Breach Level Index)

٥. ٦٨% من الهاكرز يمكن هزيمتهم بالتشفير وطرق التحقق الثنائية. المصدر: (Thycotic)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

٦. ٩٢% من البرمجيات الخبيثة تصلك عبر البريد الإلكتروني. المصدر: CSO (Online)

٧. ١٢٤$ مليار دولار هو الإنفاق العالمي في الأمن السيبراني حالياً. المصدر: (Cybersecurityventures)

٨. فقط ٥% من بيانات الشركات هي فعلاً محمية. المصدر: (Varonis)

٩. تتجه ٨٣% من الشركات هذا العام الى التخزين السحابي. المصدر: (Forbes)

١٠. في المتوسط، تحدث ٢,٢٤٤ هجمة إلكترونية يومياً. المصدر: University of (Maryland)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١١. في عام ٢٠١٦، تم سرقة بيانات ٣,٥ مليار حساب من شركة Yahoo في أكبر عملية اختراق على الإطلاق. المصدر: (NY Times)

١٢. في ٢٠١٧، برمجية وناكري Wannacry الشهيرة اصابت أكثر من ٤٠٠,٠٠٠ جهاز في أكثر من ١٥٠ دولة حول العالم وبخسائر وصلت لـ ٤ مليار دولار. المصدر: Technology (Inquirer)

١٣. كلف هجوم Wannacry على مؤسسة الرعاية الصحية ببريطانيا (NHS) أكثر من ١٠٠ مليون دولار. المصدر: (Datto)

١٤. يبلغ متوسط هجوم الفدية على الشركات ١٣٣,٠٠٠$. المصدر: (SafeAtLast)

١٥. ٩٠% من برمجيات التحكم عن بعد التي يزرعها الهاكر في جهاز الضحية، يستخدمها في تعدين العملات الرقمية. المصدر: (CSO Online)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١٦. ستتوفر ٣,٦ مليون وظيفة في الأمن السيبراني بحلول عام ٢٠٢٣. المصدر: (Cybersecurityventures)

١٧. في ٢٠٢١، كلفت الجرائم الإلكترونية الشركات حول العالم مجموع ٦٠٠$ مليار دولار. المصدر: (McAfee)

١٨. في ٢٠٢١، ١٥% من الشركات في المملكة المتحدة فقدت السيطرة على شبكاتها لصالح الهاكر. المصدر: (Cyber Security Breaches Survey)

١٩. من بين ٥٢% من الخروقات التي تمت، ٢٨% منها كانت عبر برمجية خبيثة، و٣٢%-٣٤% تمت عبر الهندسة الإجتماعية والتلاعب الفكري بالضحية. المصدر: (Verizon)

٢٠. بحلول نهاية عام ٢٠٢٢، سيزيد العدد التقديري لكلمات المرور المستخدمة من قبل البشر والآلات في جميع أنحاء العالم إلى ٣٠٠ مليار. المصدر: (Cybersecurity Media)

(..تحذيقة..)

قبل أن نبدأ....

فضلا ادخل على الرابط التالي:

https://haveibeenpwned.com/

مصطلحات وتعريفات

السيبرانية

- مأخوذة من كلمة (سيبر) Cyber،وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.
- فالسيبرانية، تعني : (فضاء الانترنت)

تعريب مصطلح cyber security

المصطلح الأول: الأمن الحاسوبي.
المصطلح الثاني: الأمن الرقمي
المصطلح الثالث : الأمن السَّبْراني
المصطلح الرابع : الأمن المعلوماتي

الامن السيبراني

جهد مستمر لحماية أنظمة الشبكة المتصلة بالإنترنت لحماية جميع البيانات من الاستخدام غير المصرح به أو الذي يسبب الضرر

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.

الأمن السيبراني

هـــو المجـــال الجديـــد الخامـــس للحروب الحديثـــة بعد البر والبحر والجـــو والفضاء الحقيقي

وهو يمثل جميع شـــبكات الحاســـب الالي الموجودة حول العالم

ويشـــمل ذلك الاجهزة الالكترونية المرتبطة من خلال شـــبكة الالياف البصرية

والشـــبكات اللاســـلكية الفضاء السيبراني

ليس الإنترنت فقط وانما شبكات اخرى كثيرة متصلة

يتضح من هذا

الفضاء السيبراني مجال عملياتي يعتبر الميدان الخامس للحروب الحديثة بعد ميدان الحرب البرية والجوية والبحرية والفضائية

البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزء أساسي من الفضاء السيبراني

الفضاء السيبراني لايقتصر على شبكة الإنترنت فقط
وانما شبكات عالمية وخاصة أخرى مثل : gps / Acars / Swift / Gsm / pstn

الفضاء السيبراني

مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات.

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

الحرب السيبرانية (الرقمية)

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

الأمن السيبراني

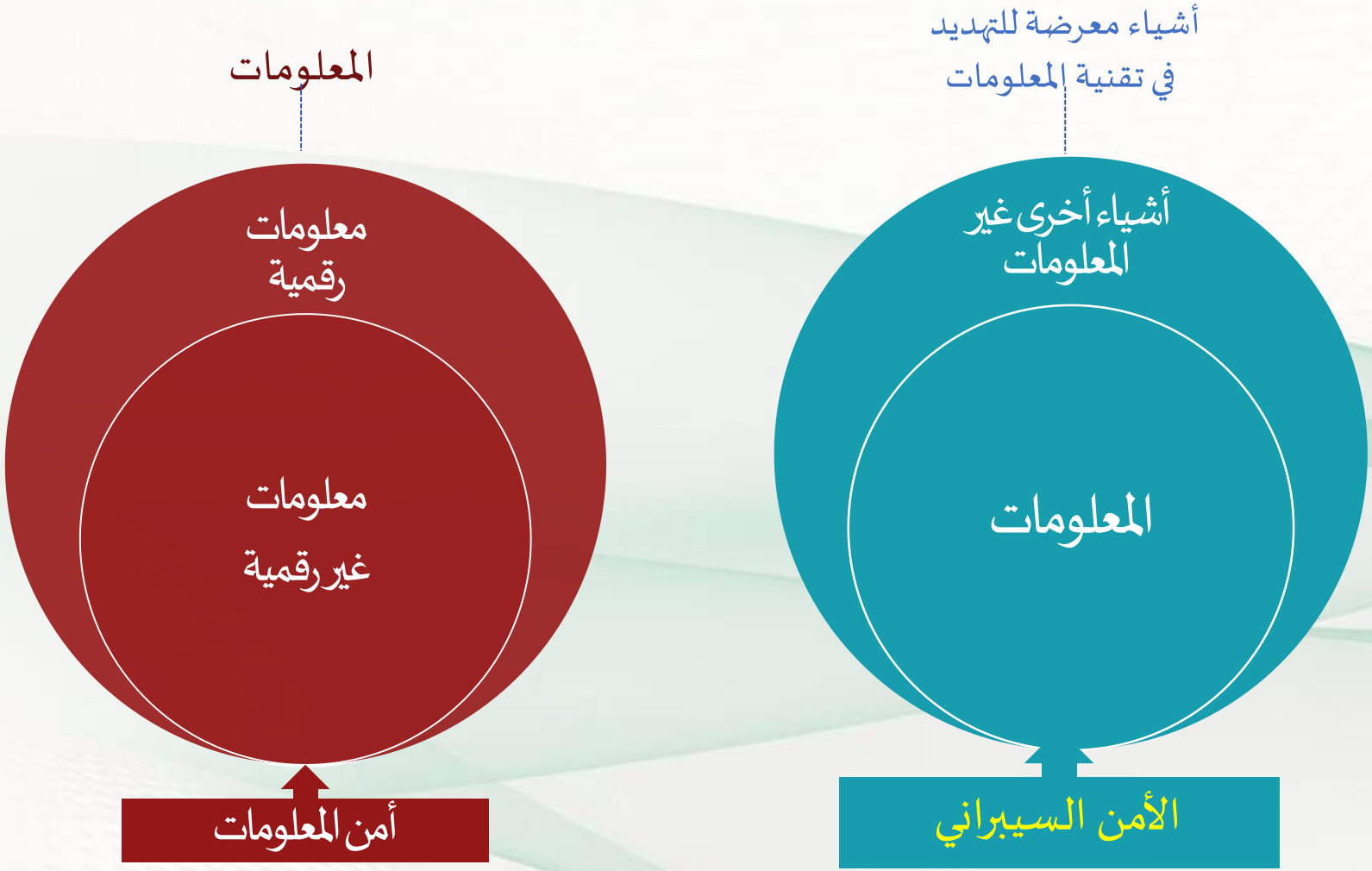
الفرق بين أمن المعلومات والأمن السيبراني

أمن المعلومات يهدف إلى:

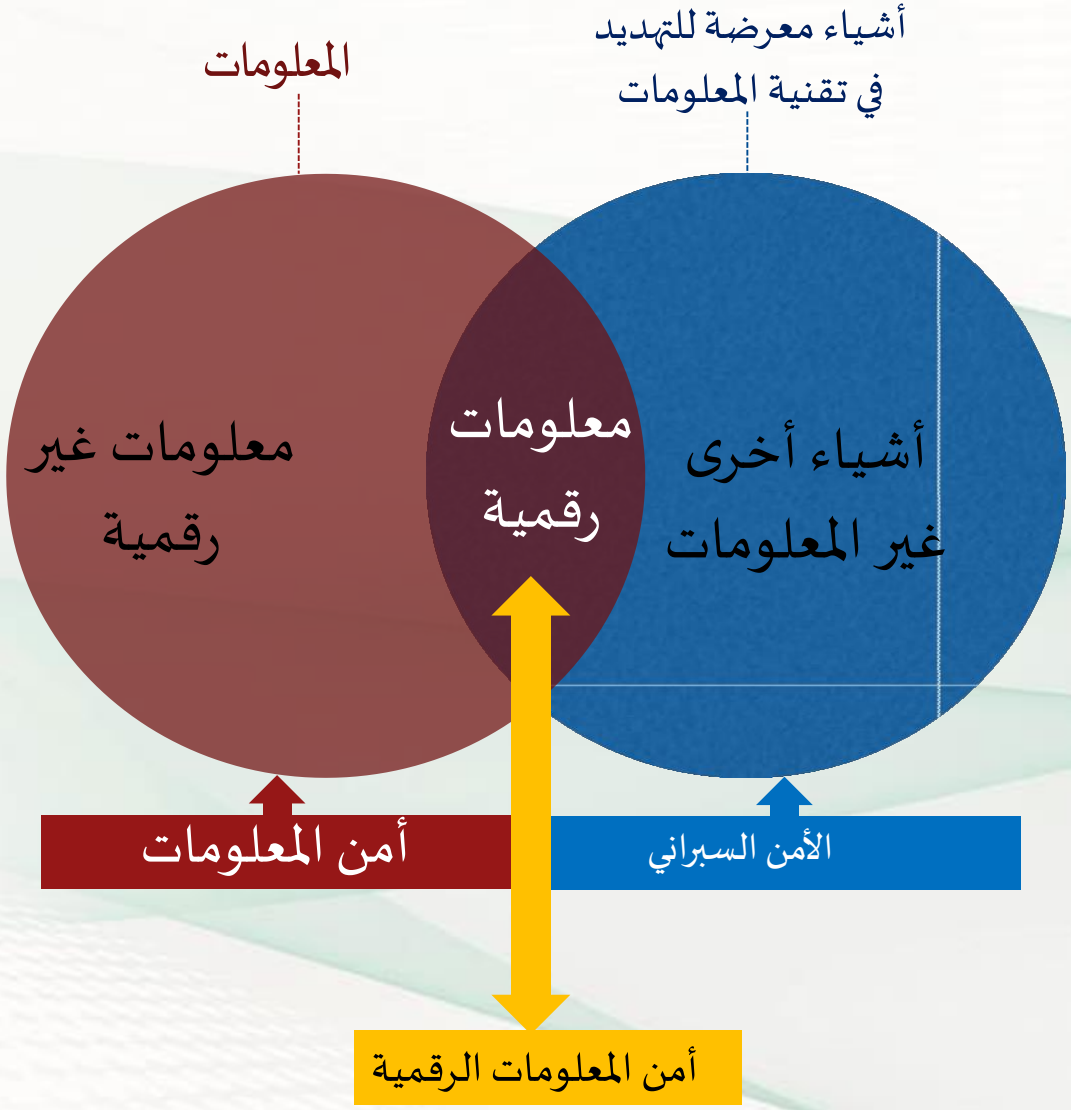
حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل:

- 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
- أمن المعلومات يهتم بمجالات ضخمة، كالتشفير، والتخزين، والتأمين الفيزيائي، والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر..

أمن المعلومات والأمن السيبراني



أمن المعلومات والأمن السيبراني



الفرق بين أمن المعلومات والأمن السيبراني

الأمن السيبراني يأخذ في عين الاعتبار أيضا حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها.

الأمن السيبراني يتعلق بتأمين الأشياء المعرضة للخطر من خلال تكنولوجيا المعلومات والاتصالات"	" أمن المعلومات هو كل شيء عن حماية المعلومات ، التي تركز بشكل عام على سرية وسلامة وتوافر المعلومات"

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

أمن المعلومات والأمن السيبراني

الأمن السيبراني

القدرة على الدفاع أو حماية الفضاء السيبراني (الالكتروني) من الهجمات السيبرانية.

أمن المعلومات

حماية نظم المعلومات والمعلومات من الوصول أو الاستخدام غير المصرح به أو التسريب أو التخريب أو التعديل أو التدمير وضمان توفير السرية والنزاهة والتوافر.

أهداف الأمن السيبراني

أهداف 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

يتبع أهداف 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

لماذا نحتاج الامن السيبراني؟

أهمية الأمن السيبراني

91٪ يقوم ممن يمتلكون أجهزة ذكية حول العالم بإتمام مُعاملات مالية أو عمليات شراء وتسوق عبر الإنترنت

%87 يستخدم من البشر المُتصلون بالإنترنت شبكات التواصل

25% يحتفظ من المُستخدمين بكلمات المرور الخاصة بحساباتهم الشخصية وحساباتهم البنكية على هواتفهم الذكية أو حاسباتهم

%65 تزايد نسبة من يحتفظون بصورهم الشخصية على هواتفهم الذكية أو أجهزتهم اللوحية

%72 نسبة من الاختراقات الإلكترونية ناجمة من الاخطاء البشرية

أهمية الأمن السيبراني

خسائر اقتصادية

متوسط تكلفة خرق البيانات في عام ٢٠٢١
يتجاوز ١٥٠ مليون دولار

في عام ٢٠٢١ تمكن المخترقون من سرقة نصف مليار من السجلات الشخصية

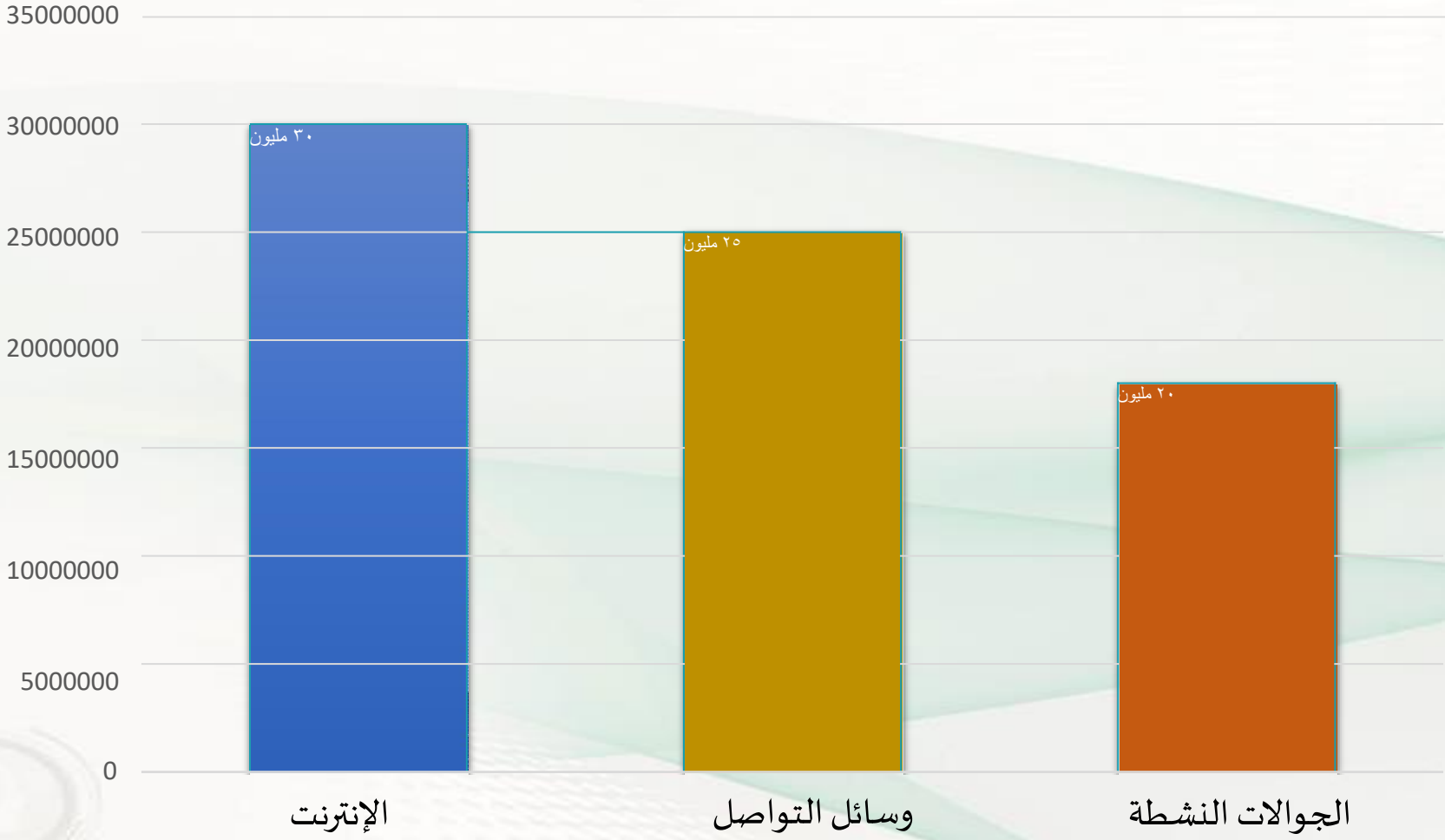
٧٦ مليار دولار من الأنشطة غير المشروعة تعتمد على بيتكوين

أهمية الأمن السيبراني

- وظائف الأمن السيبراني في جميع أنحاء العالم وصلت إلى ٣,٥ مليون عام ٢٠٢٢
- المتوقع أن يتم إنفاق ٦ تريليونات دولار تقريبًا على مستوى العالم على الأمن السيبراني بحلول عام ٢٠٢٣
- ٣٠٠ مليار دولار سوق الأمن السيبراني
- في عام ٢٠٢٢ هناك ما يقرب من ٢٠٠ مليار جهاز متصل
- أكثر من ٧٧ ٪ من المؤسسات ليس لديها خطة للاستجابة لحوادث الأمن السيبراني
- تستغرق معظم الشركات حوالي ٦ أشهر للكشف عن خرق البيانات ، حتى الشركات الكبرى
- تبلغ ميزانية الأمن السيبراني في الولايات المتحدة ١٤,٩٨ مليار دولار

إحصائية

عدد المستخدمين في ا لمملكة العربية السعودية



الجلسة التدريبية الثانية

اليوم الأول

الهجمات التي تحدث الآن في العالم

https://cybermap.kaspersky.com/

العيون الخمسة

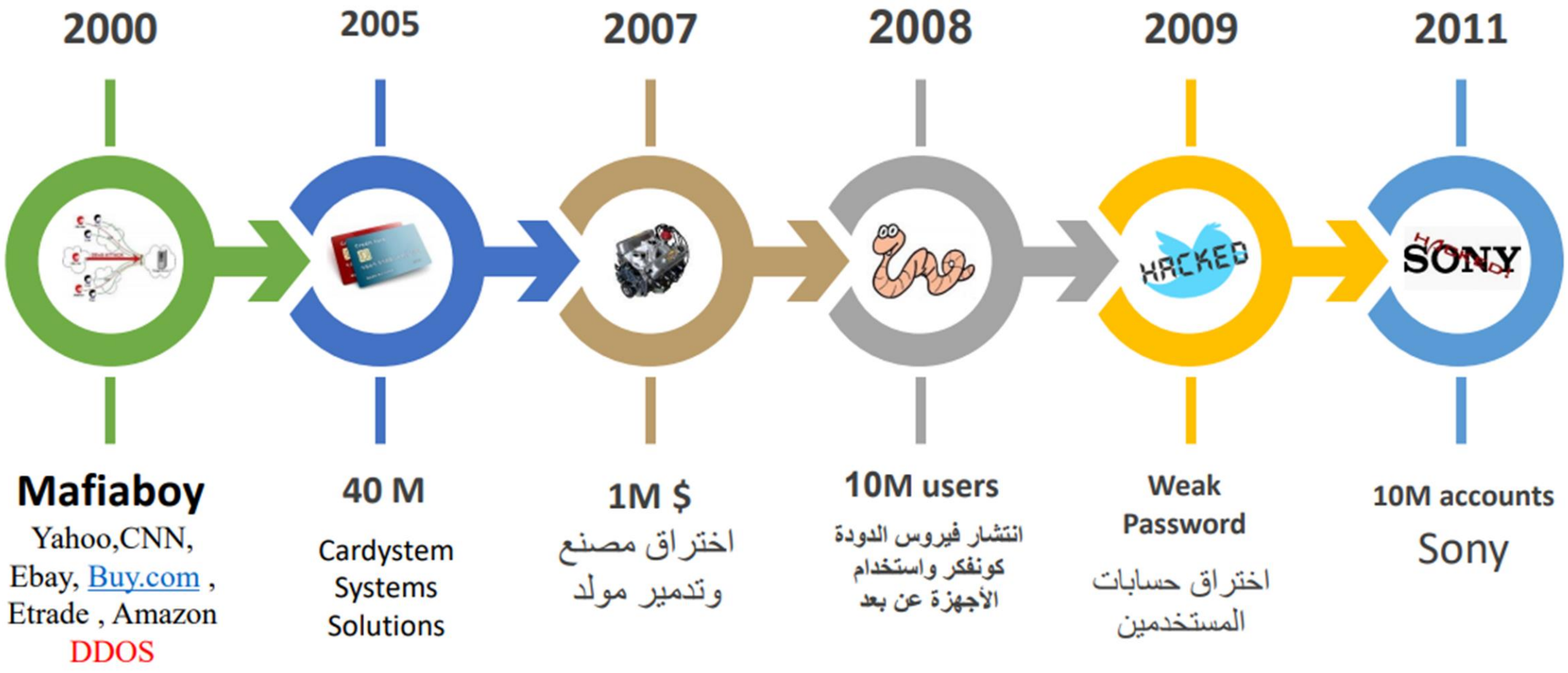
هو عبارة خمسة دول تراقب الانترنت (أمريكا – بريطانيا – استراليا – كندا – نيوزلندا)

- تراقب الكابلات البحرية وتخزن البيانات وتحللها وتشاركها مع بعض
- جميع مواقع التواصل الاجتماعي (تويتر –فيس بوك – سناب ...الخ) تعطي بيانات للحكومة الالكترونية قانونيا واجباريا
- (فيديو – شات – ايميل – مكالمات الصوت – ملفات .. الخ جميع أنواع البيانات)

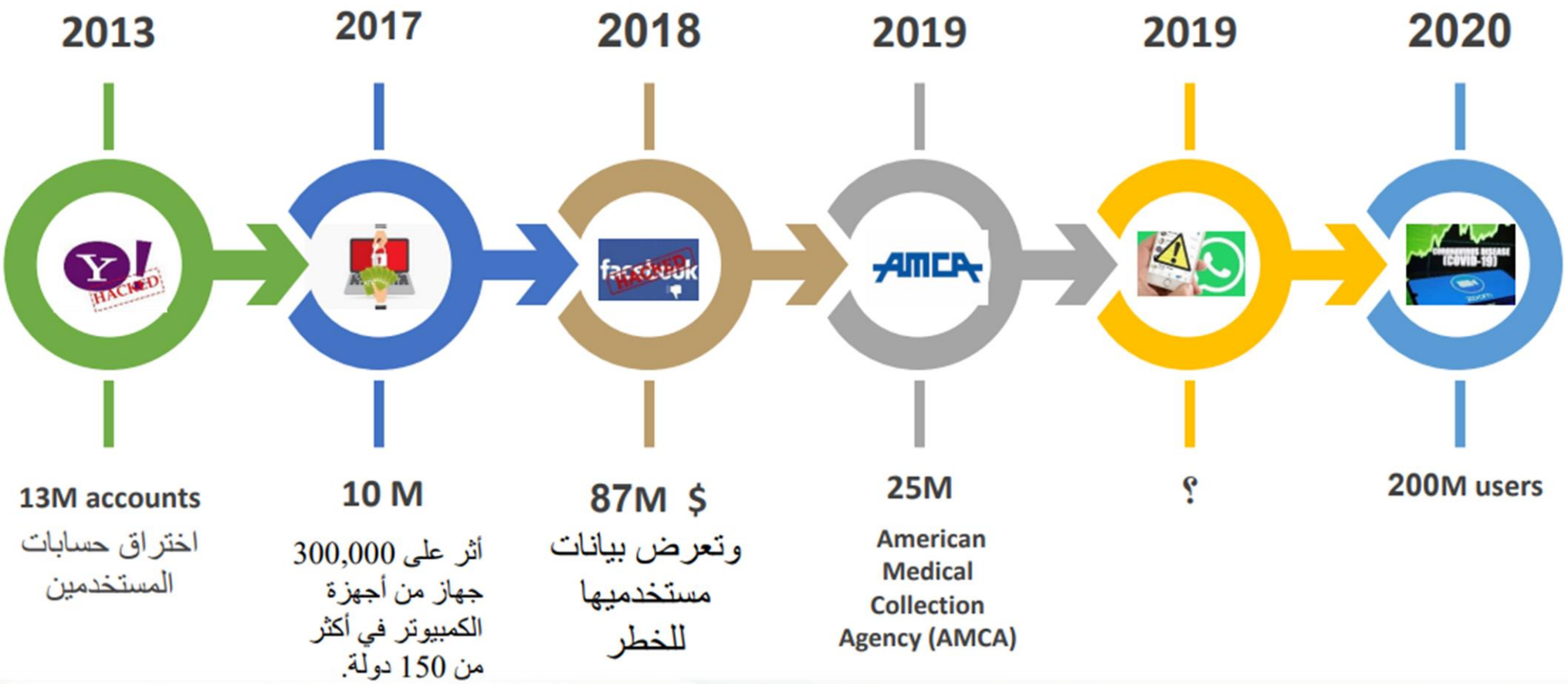
قصة سفر الملفات

نظرة تاريخية لأبرز الهجمات

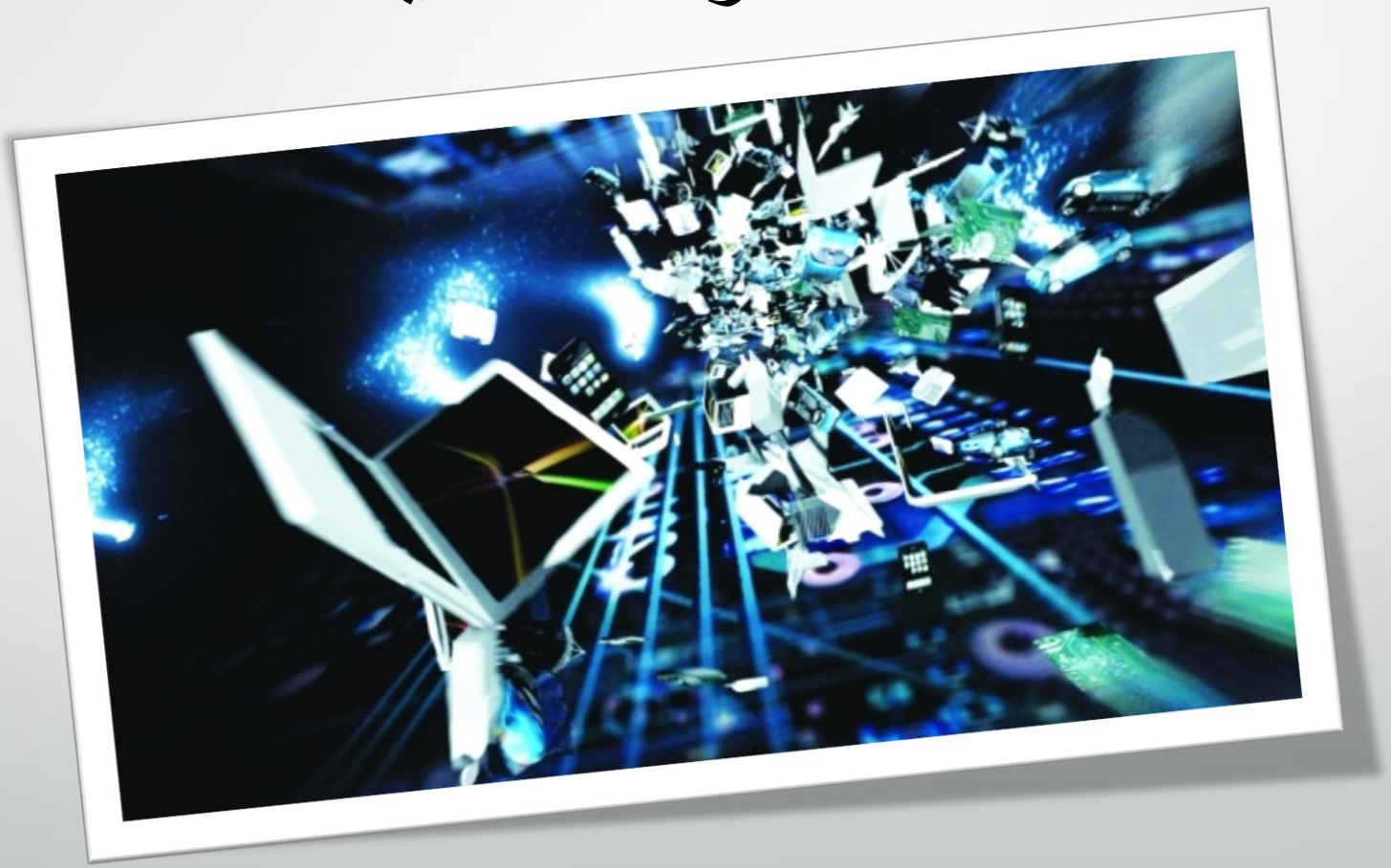
نظرة تاريخية



نظرة تاريخية



اختراقات عالمية

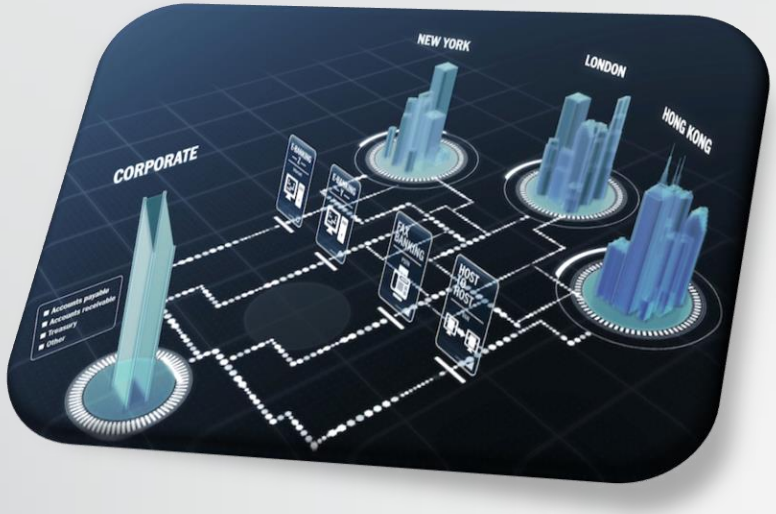


وكالة الأمن القومي الأمريكية

- وكالة تراقب الجميع (الانترنت) وهي أكبر وكالة تجسس إلكتروني وسايبري في العالم
- تحتوي على الكثير من المختصين في الامن السيبراني
- قامت مجموعة من القراصنة باختراق الوكالة وعرض الأدوات والملفات التي حصلوا عليها للبيع لمن يدفع أكثر.
- البيانات المسربة يصل حجمها إلى ١٠٠ غيغابايت وتتضمن معلومات تخص مشروع التجسس العسكري وتشمل البرامج الخبيثة المعدة للاختراقات أدوات وثغرات ...الخ

ياهو yahoo

- **موظف يدعى ريسيس رويز بشركة ياهو قام بسرقة معلومات عن نحو ٥٠٠ مليون مستخدم**
- رويز قام بالسطو على كلمات السر والدخول على أنظمة ياهو الداخلية لاختراق الحسابات الخاصة. وبعد دخوله على الحساب، قام المهندس بنسخ صور وفيديوهات وجدها على الحسابات الخاصة بدون إذن
- بعد دخوله حسابات الضحايا، أمكنه اختراق حساباتهم الأخرى على فيسبوك وآي كلاود ودروب بوكس وحسابات أخرى من أجل العثور على صور وفيديوهات خاصة.



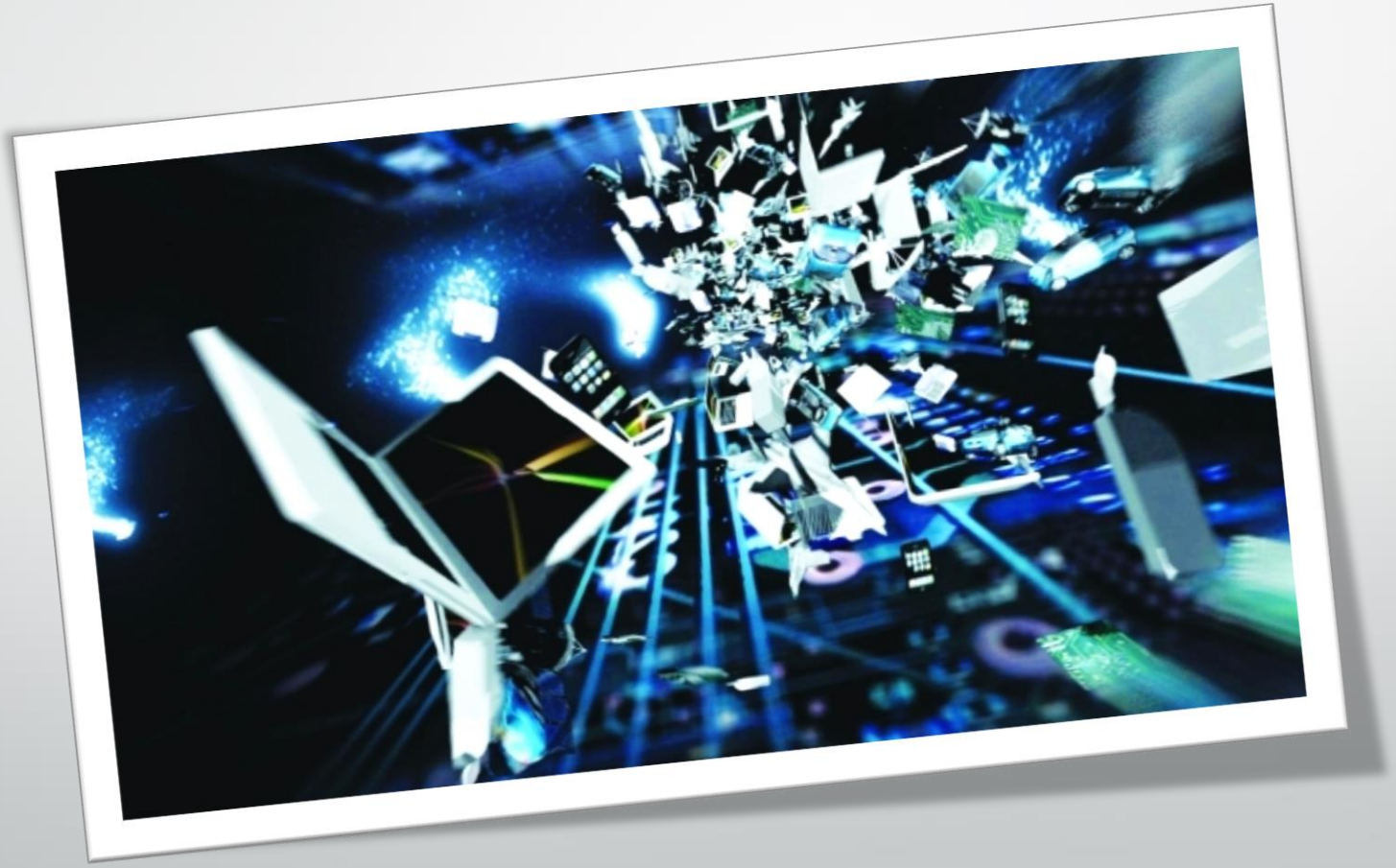
الشبكة swift المصرفية

- سويفت SWIFTهو نظام المراسلة المالية الذي يستخدم من قبل ١١ ألف بنك في جميع أنحاء العالم
- **تم اختراقها عدة مرات (في الفلبين وبانكوك وبنقلادش)**
- **سرقة البنك المركزي في بنقلادش بمحاولة تحويل ٩٥١ مليون وتم سرقة ٨١ مليون منها**

شركة سوني

- ٧٧ مليون أيميل تمت سرقته.
- ٢٥ مليون حساب لمستخدمي سوني تم تهكيرها.
- ١٠٧٠٠ لبطاقات الخصم .
- ١٢٧٠٠ بطاقة ائتمان.
- مراسلات سرية بين الموظفين
- أفلام كان من المفترض أن يبدأ عرضها تسربت على الانترنت
- انخفاض أسهم بورصة سوني بنسبة ٦,٦ بالمئة.
- خسائر تجاوزت ١٠٠ مليون دولار.

اختراقات محلية



Stc


Ransomware Virus strikes STC
STC
الاتصالات السعودية
إشارة إلى ما تم تداوله بخصوص فايروس WannaCry
فإن الشركة تود توضيح أن شبكاتها و انظمتها لم
تتأثر بحمد الله و بالتالي فإن ما ذكر في وسائل
الإعلام يخص بعض الأجهزة الشخصية التي سيتم
التعامل معها الآن من قبل الفرق الفنية
المتخصصة، و بالنسبة لتطبيق MySTC فلم
يتأثر أبداً و الحمد لله.
www.stc.com.sa
14 مايو 2017م

أرامكو

«أرامكو» وشركة هندية تقعان ضحية لأكبر جرائم الاحتيال الإلكتروني في مومباي

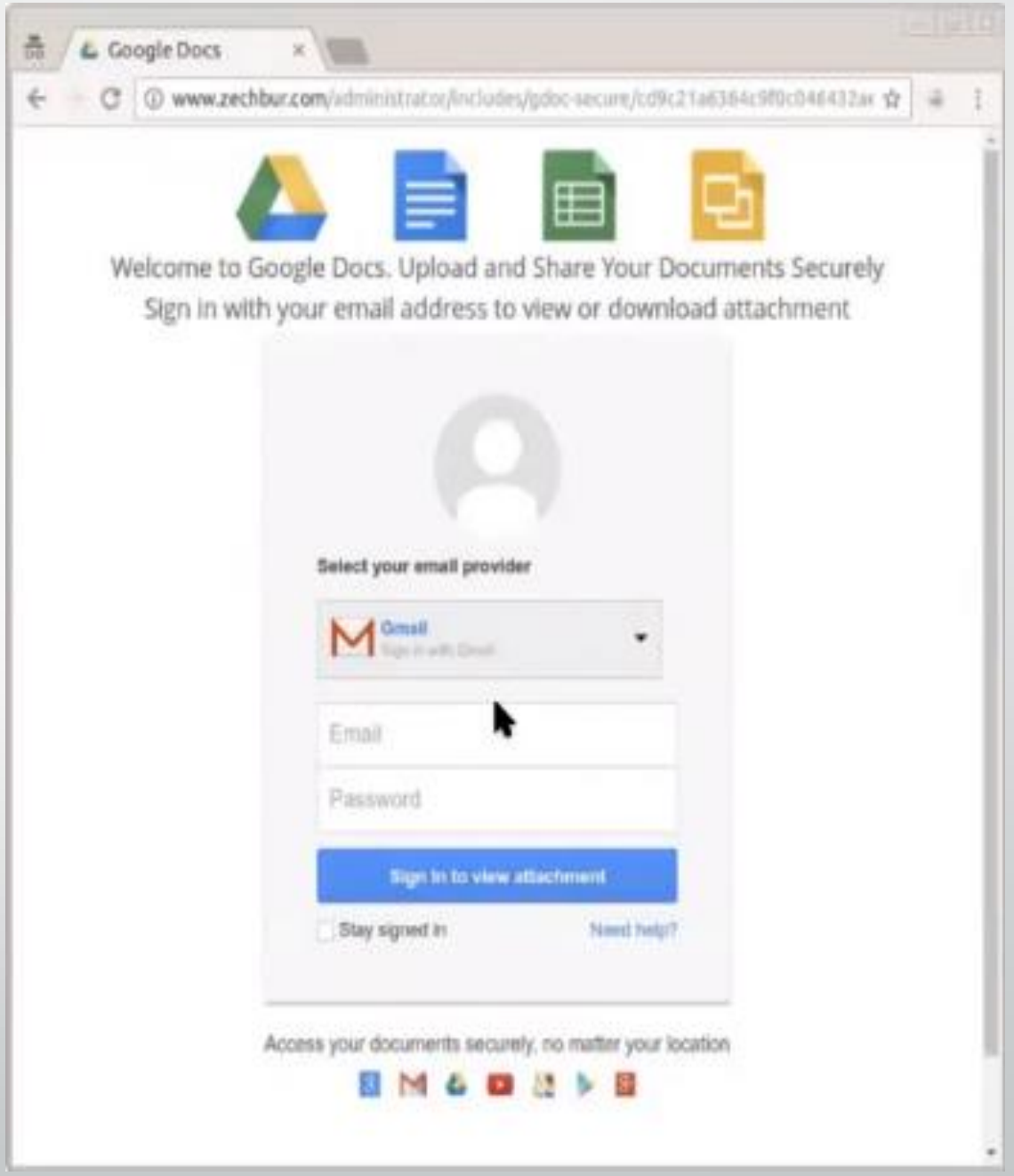
حجم الخسائر ٣٠ مليون دولار

*

البريد الإلكتروني للشركة الهندية

patel_dv@ongc.co.in

patel_dv@ognc.co.in



جامعة الملك فيصل

المتهم معترفاً في التحقيقات: نفعتهم.. ولم أضرّهم

اختراق جامعة.. وتعديل درجات 19 طالباً بالـ «Wi-Fi» !

عكاظ
مساحة إعلانية

أخبار | الأربعاء 18 ديسمبر 2019 02:51 | فاطمة آل دبيس (الرياض) -@fatimah_a_d | 410

طالبت النيابة العامة بسجن طالب 4 سنوات وتغريمه 3 ملايين ريال عقب تورطه في اختراق نظام جامعة الملك فيصل وتعديل درجات 19 طالباً إلى 199.

وعلمت «عكاظ» أن المتهم اعترف في التحقيقات بالدخول إلى موقع أجنبي مختص بتسريب البيانات، ما مكّنه من الاختراق والوصول إلى قاعدة بيانات جامعة الملك فيصل وعناوينها البريدية وأرقام سريه لمنسوبيها استخدمها في الوصول إلى

فضيحة جديدة.. موظفو «سناب شات» يتجسسون على المستخدمين!

محطة أخيرة | الاحد 26 مايو 2019 03:57 | «عكاظ» (دبي) @Okaz_online | 12370 مشاهدة

أفاد تقرير إخباري بأن عدداً من موظفي شركة سناب – المالكة لتطبيق التراسل المصور سناب شات – أساؤوا استخدام بعض الأدوات الخاصة بالشركة في التجسس على مستخدمي الخدمة.

إشترك بالنشرة الإلكترونية

أخبار شائعة

إذا كنت موجود في السعودية هذه المعلومات سترشدك
لتحقيق $32,000 في 10 أيام

News

نشر الهاكر "موكسي مارلينسبايك" تدوينة على موقعه الخاص على الإنترنت تظهر جزءا من المراسلات التي تمت بينه وبين الشركة، وقال إنه تلقى منذ أسبوع تقريبا رسالة من [redacted]، المدير التنفيذي لقسم أمن المعلومات والشبكات في شركة [redacted] لت عنوانا ملفتا وهو "حل لمراقبة بيانات مشفرة في شركة اتصالات"، مما أثار اهتمامه وأدى به لطلب المزيد من المعلومات حول المشروع على حد قوله، وأشار إلى أنه وبعد أسبوع من المراسلات علم أن شركة [redacted] تعمل على برنامج لاعتراض بيانات التطبيقات الخاصة بالأجهزة المحمولة مع اهتمام خاص بالتطبيقات التالية: "تويتر" و"فايبر"و"لاين"و"واتس آب"، ونشر مارلينسبايك المهارات والقدرات المطلوبة التي ينبغي أن تتوافر في الشخص الذي سيشارك في إيجاد حل لتنفيذ المشروع وهي القدرة على مراقبة وحجب بيانات التواصل عبر تطبيقات الأجهزة المحمولة .

https://www.traidnt.net/vb/images/img...13/05/2961.jpg

هل انا بعيد عن خطر الاختراق ؟

لماذا أنا من وسط الملايين ؟.

هل يوجد أمان في الانترنت ؟

الجلسة التدريبية الثالثة

اليوم الأول

طرق الاختراق

معرفة سُبل حماية خصوصية
معلوماتك وأجهزتك أثناء استخدامك
للإنترنت يقلل من احتمال تعرضها
لمخاطر الاستخدام غير المشروع،
والذي يلحق الضرر بك ماديا أو معنويا

نشاط ١-١

نشاط وعي التصيد

https://bit.ly/2yv7qq5


الاصطياد الإلكتروني
1
الابتزاز الإلكتروني
5
أساليب شهيرة
في الاختراق
2
الهندسة الاجتماعية
4
انتحال الشخصية
3
أحصنة طروادة

ماهي الهندسة الاجتماعية ؟

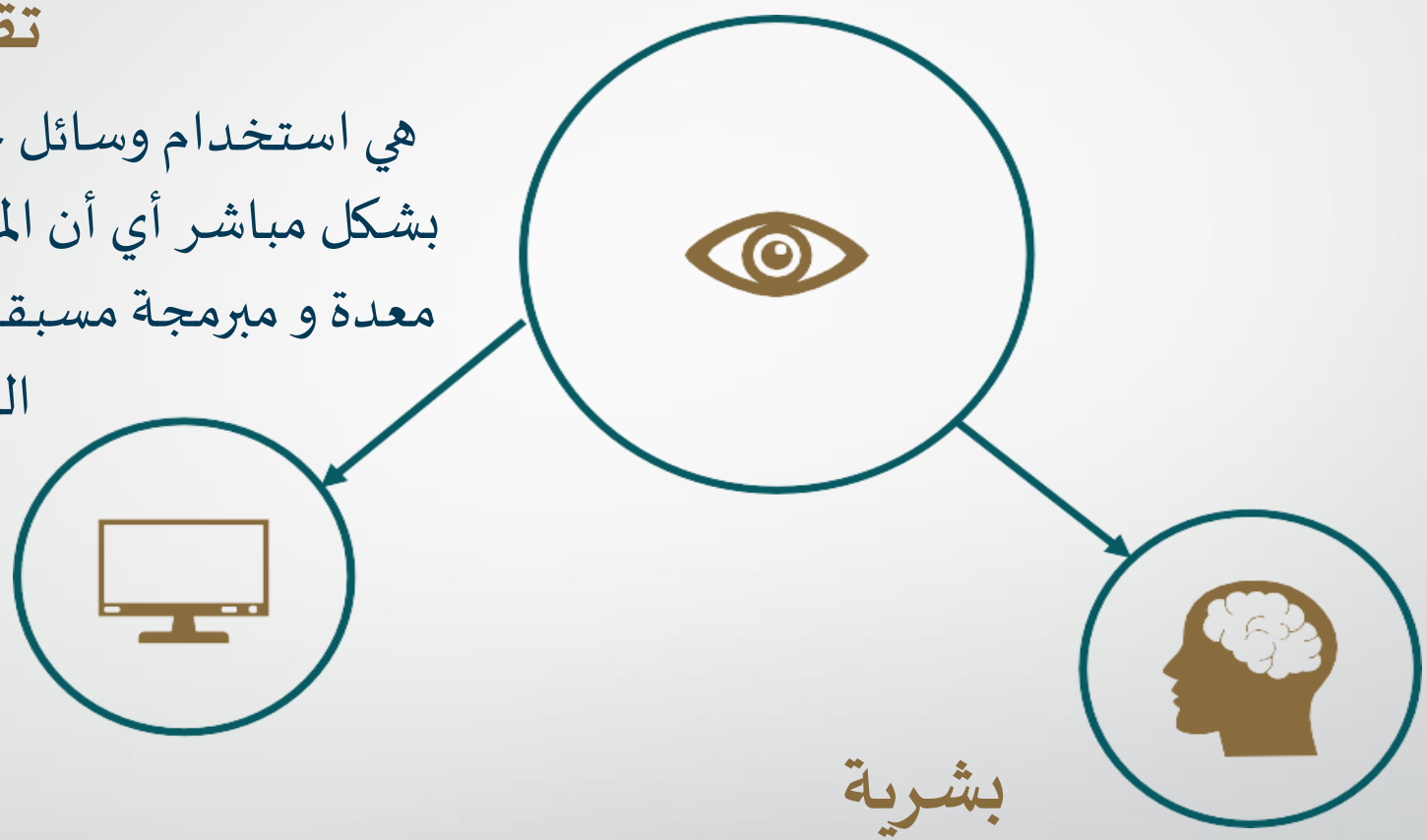
هي فن التلاعب بالبشر وخداعهم بهدف الحصول على البيانات لكشف معلوماتهم أو حساباتهم السرية دون علمهم وذلك باستهداف نقاط الضعف البشرية.

أهداف الهندسة الاجتماعية :

أنواع الهندسة الاجتماعية :

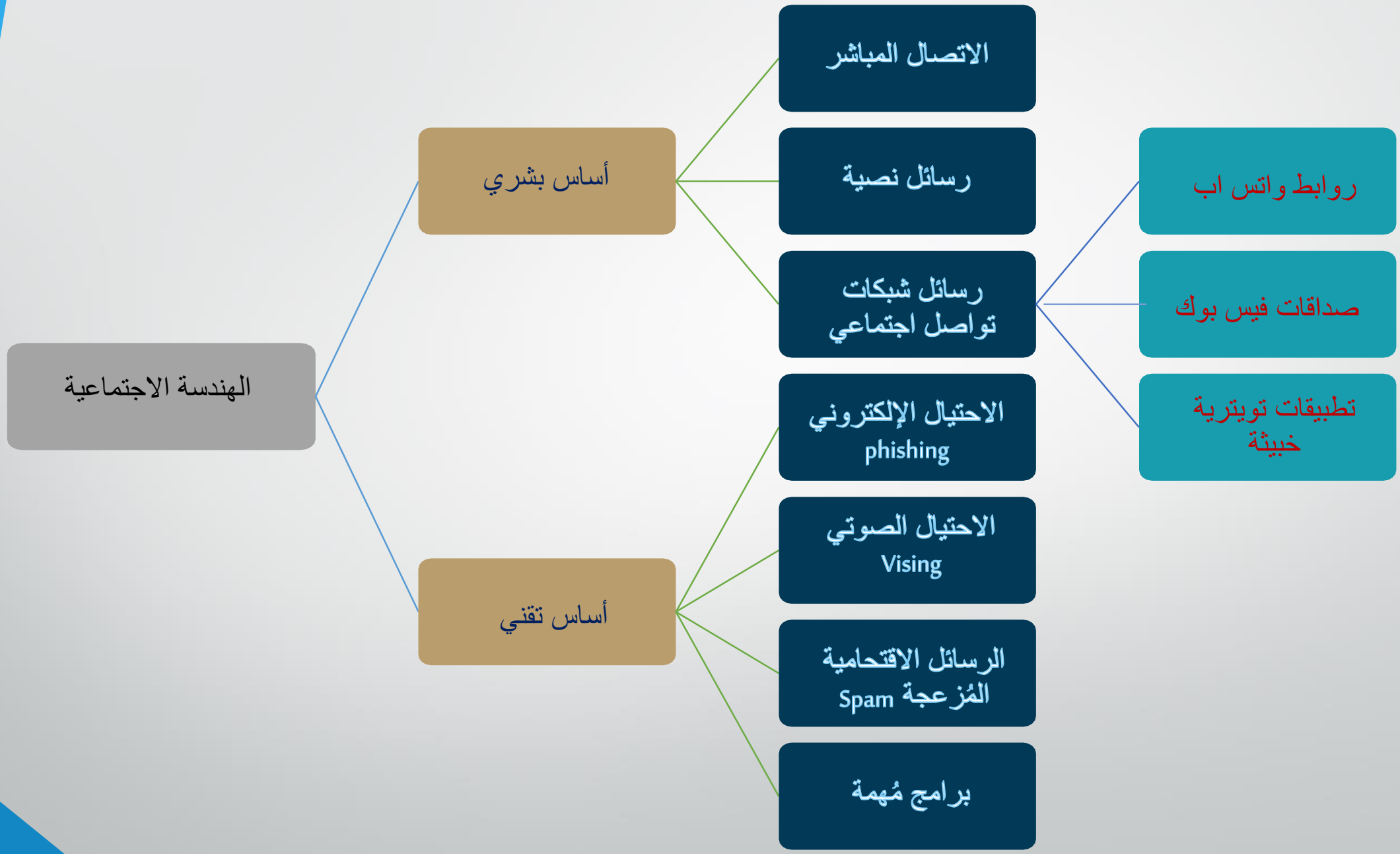
تقنية

هي استخدام وسائل خداعية تعتمد على التقنية بشكل مباشر أي أن المهاجم يستخدم أدوات تقنية معدة و مبرمجة مسبقا تمكنه من سحب معلومات الضحية.



بشرية

هي استخدام الأساليب والمهارات البشرية دون الاعتماد على التقنية ، وهذا لا يعني عدم استخدام أي وسيلة تقنية في هذا النوع .


الهندسة الاجتماعية
أساس بشري
أساس تقني
الاتصال المباشر
رسائل نصية
رسائل شبكات تواصل اجتماعي
روابط واتس اب
صداقات فيس بوك
تطبيقات تويترية خبيثة
الاحتيال الإلكتروني phishing
الاحتيال الصوتي Vising
الرسائل الاقتحامية المُزعجة Spam
برامج مُهمة

البيانات التي يمكن خسارتها ..

البيانات التي يمكن خسارتها ..

١- الوصول للجهة المستهدفة

الموقع
الموظفين
نبذة عن الجهة

٢- اختيار ضحية معينة

البحث عن الضحية الضعيفة والمترددة

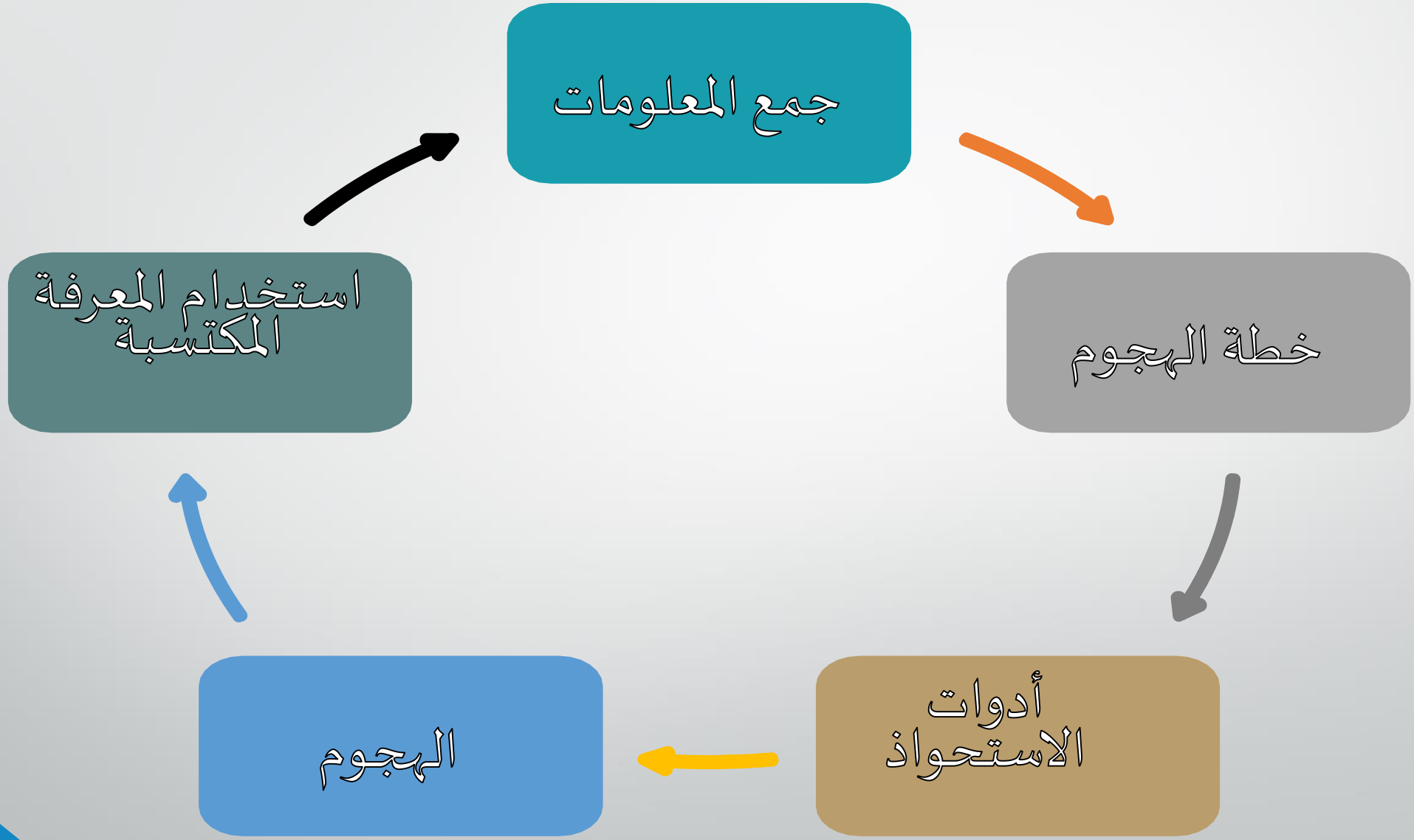
٣- بناء علاقة

بناء علاقة بها ثقة متبادلة

٤- استغلال العلاقة

استغلال
العلاقة
لجمع البيانات
الحساسة

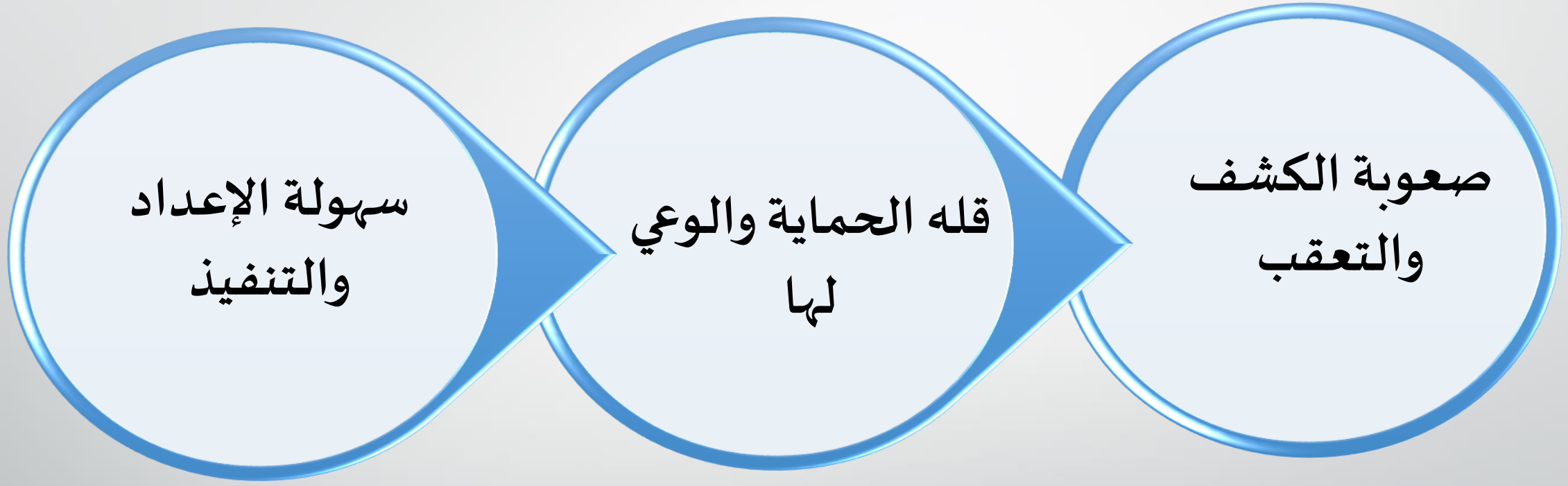
مراحل الهندسة الاجتماعية



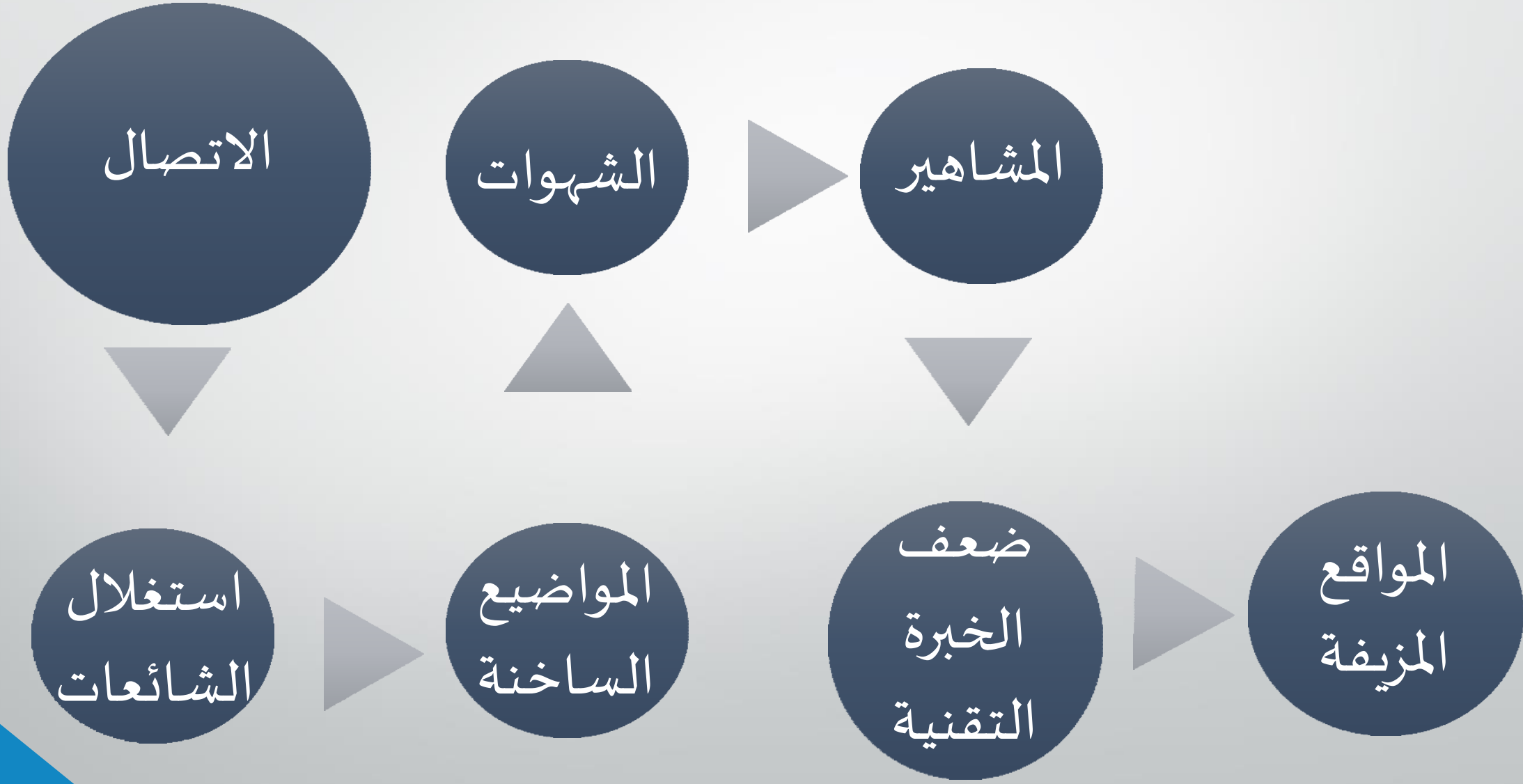
الأساليب المتبعة في الهندسة الاجتماعية :

- الإقناع عن طريق استغلال عواطف الضحية
- استغلال الشائعات (الرسائل الكاذبة)
- المكالمات من مجهولين لتسجيل المعلومات
- انتحال الشخصية
- اصطياد كلمات السر
- البحث في المهملات
- استغلال ضعف الخبرة التقنية للضحية (فتح الملفات الغير آمنة)

لماذا تنجح الهندسة الاجتماعية



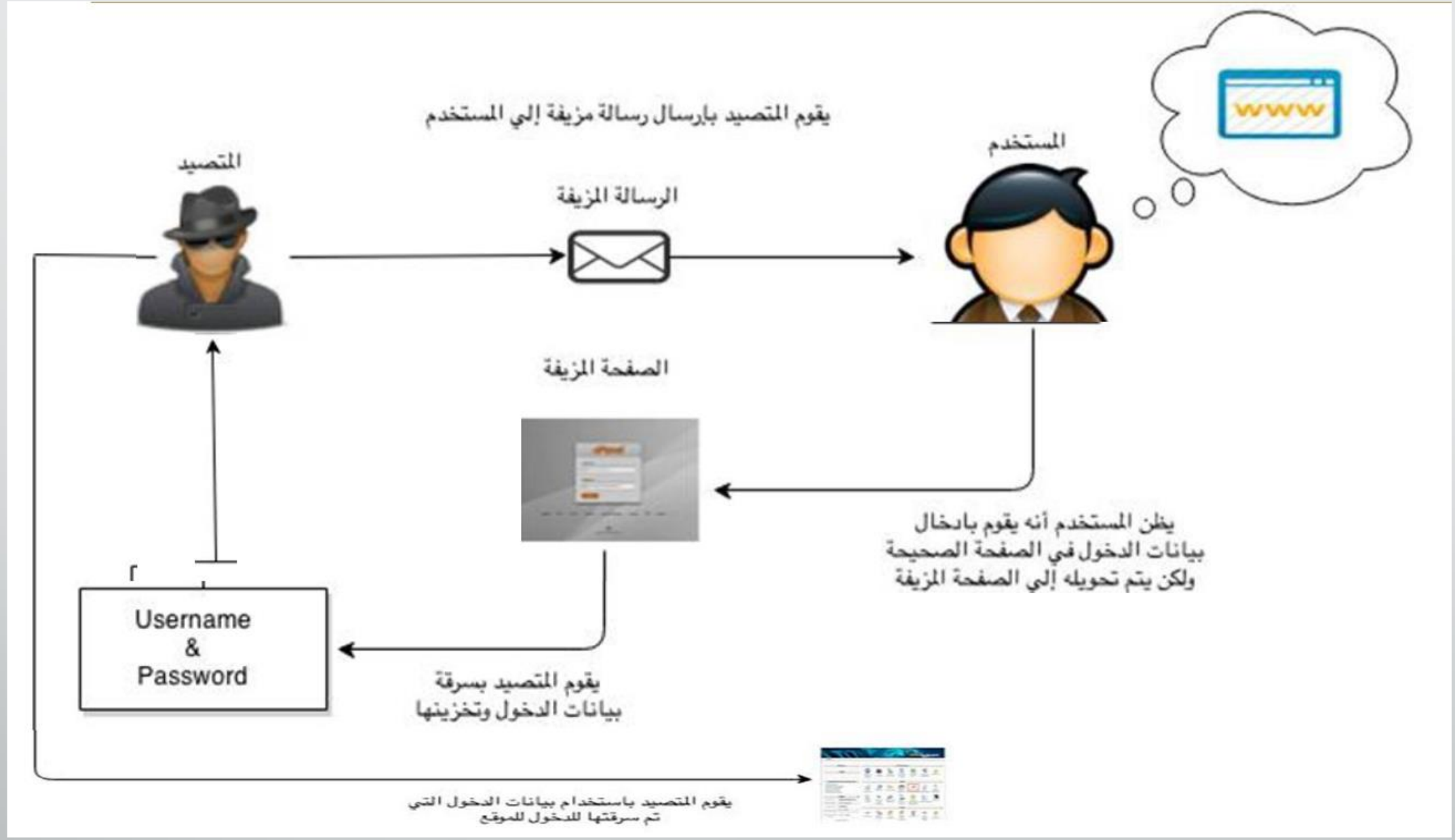
لماذا تنجح الهندسة الاجتماعية

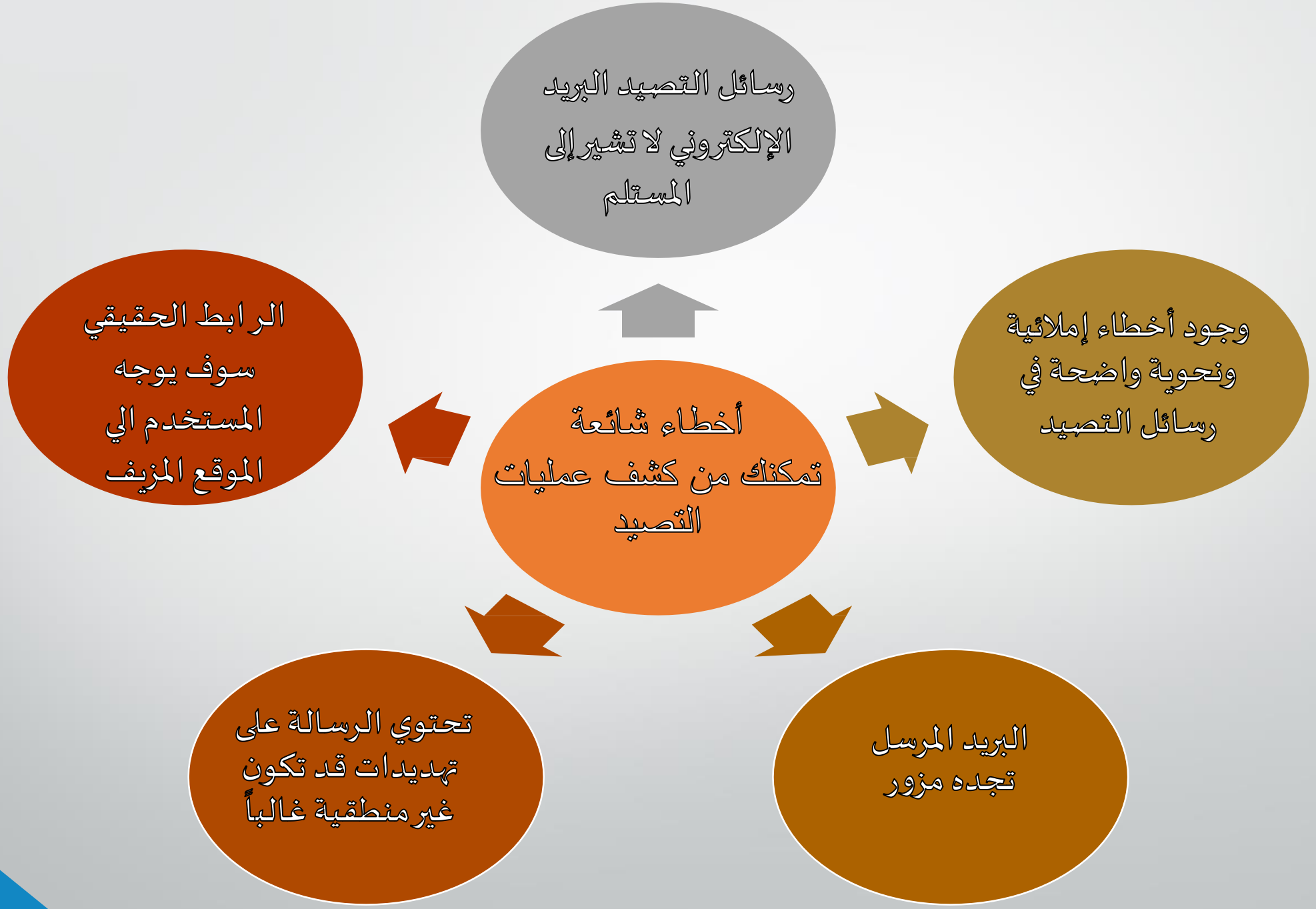


التصيد؟

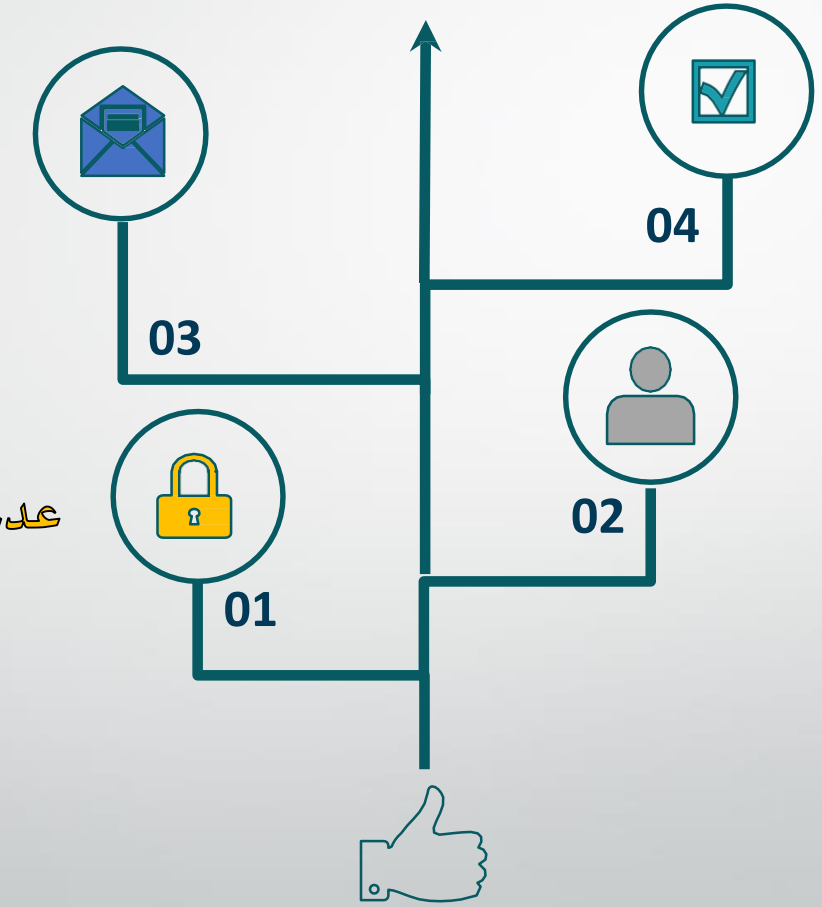
التصيد الإلكتروني هو نوع من أنواع الجرائم الإلكترونية الأكثر انتشارا.


الاصطياد
الإلكتروني
استغلال وسائل تقنية
المعلومات لمحاولة خداع
الضحية للكشف
عن معلوماته السرية
الهندسة الاجتماعية


يقوم المتصيد بإرسال رسالة مزيفة إلي المستخدم
المتصيد
الرسالة المزيفة
المستخدم
www
الصفحة المزيفة
يظن المستخدم أنه يقوم بادخال
بيانات الدخول في الصفحة الصحيحة
ولكن يتم تحويله إلي الصفحة المزيفة
Username
&
Password
يقوم المتصيد بسرقة
بيانات الدخول وتخزينها
يقوم المتصيد باستخدام بيانات الدخول التي
تم سرقتها للدخول للموقع


رسائل التصيد البريد الإلكتروني لا تشير إلى المستلم
وجود أخطاء إملائية ونحوية واضحة في رسائل التصيد
الرابط الحقيقي سوف يوجه المستخدم الي الموقع المزيف
أخطاء شائعة تمكنك من كشف عمليات التصيد
البريد المرسل تجده مزور
تحتوي الرسالة على تهديدات قد تكون غير منطقية غالباً

طرق الوقاية من الوقوع ضحية للهندسة الاجتماعية



الوقاية من الوقوع ضحية للهندسة الاجتماعية:

تأمين المشاركة	لا تقم بمُشاركة أي معلومات خاصة بك
التحقق من هوية المرسل أو المتصل	تحقق دائما من هوية الأشخاص الذين يتصلون بك
المرفقات	لا تقم بفتح أو تحميل أي مُرفق إلكتروني أو فيديو أو صورمن في وسائل التواصل وصلتك من أشخاص غير معروفين
تأمين الأجهزة	تأمين الأجهزة الشخصية واستخدام برامج قوية لمُكافحة الفيروسات
تفعيل التحقق بخطوتين في برامج التوصل	قم بتفعيل التحقق بخطوتين في الواتس اب وتويتر وغيرها من وسائل التواصل الاجتماعي

نشاط٢-١ لبعض طرق جمع البيانات بطريقة غير مباشرة

- https://www.whois.net رواق – منصة زائر

نشاط ٢-٢ لبعض طرق جمع البيانات بطريقة غير مباشرة

- https://tineye.com/
- مصابين كورونا في إيطاليا

نشاط ٢-٣ لبعض طرق جمع البيانات بطريقة غير مباشرة

- http://exif.regex.info/exif.cgi معلومات الصورة

21.406094,39.891042

نشاط ٢-٤ لبعض طرق جمع البيانات بطريقة غير مباشرة

- https://www.google.com.sa/imghp?hl=ar&tab=wi&ogbl

البحث عن بيانات بالصورة

اليوم الأول

ملخص اليوم التدريبي الأول

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

وزارة التعليم
Ministry of Education

NCEPD

الأمن السيبراني

خطة البرنامج التدريبي

اليوم التدريبي	الجلسة التدريبية	العنوان	الموضوع/الموضوعات	الهدف/ المحور	الزمن
الثاني	الأولى	الجرائم المعلوماتية	الجرائم المعلوماتية	التعرف على الجرائم المعلوماتية	٩٠ دقيقة
	استراحة				٢٠ دقيقة
	الثانية	الجرائم المعلوماتية	الجرائم المعلوماتية	تطبيق بعض أساليب الهجوم السيبراني	٦٠ دقيقة
	استراحة				١٠ دقائق
	الثالثة	الجرائم المعلوماتية	أساليب الحماية من الهجوم السيبراني	تطبيق بعض أساليب الحماية من الهجوم السيبراني	٦٠ دقيقة

الثانية

اليوم

الجلسة التدريبية الأولى

تحذيقة

اختبار وعي التصيد

http://www.phishingaware.com/quizScript.html

الجرائم المعلوماتية

جرائم الاعتداء على الحياة الخاصة

المقصود من الحياة الخاصة

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

٢

السب والشتم عبر الانترنت

الشتم وهوكل 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

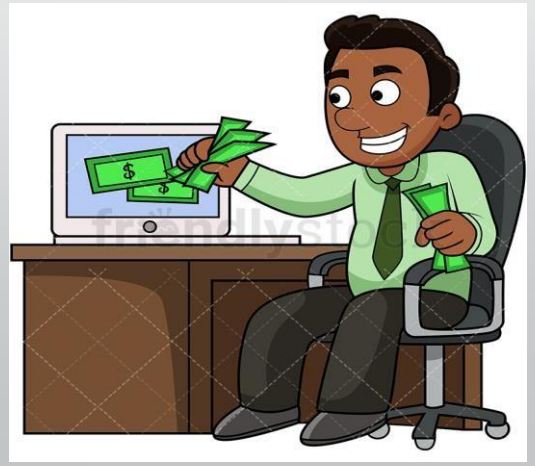
إفشاء الأسرار

عن طريق الحاسب يمكن الاعتداء على خصوصيات الأفراد و إفشاء 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

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

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

كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية

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

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 مو اقع 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

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 بغيرحق على الأموال أو الخدمات والاستيلاء عليها للمجرم فعليا على مال منقول أوسند أو توقيع هذا السند

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

الاستيلاء والاحتيال المعلوماتي

له طرق متعددة كأن يوهم المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح ، فيسلم المال للجاني بطريقة معلوماتي أو من خلال تصرف الجاني في المال وقد يتخذ اسم أو صفة كاذبة تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الالكتروني للأموال وذلك من خلال اتصل بالمجيني عليه عن طريق الشبكة أو بتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب والاحتيال عليه فيسلمه المنظام المال .

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات

او بغرامة لا تزيد على مليوني ريال

او بإحدى هاتين العقوبتين

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 إلى حسابات أخرى

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

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

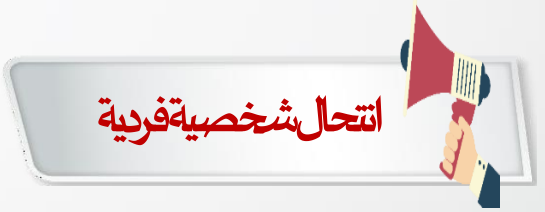
السطو على أموال البنوك

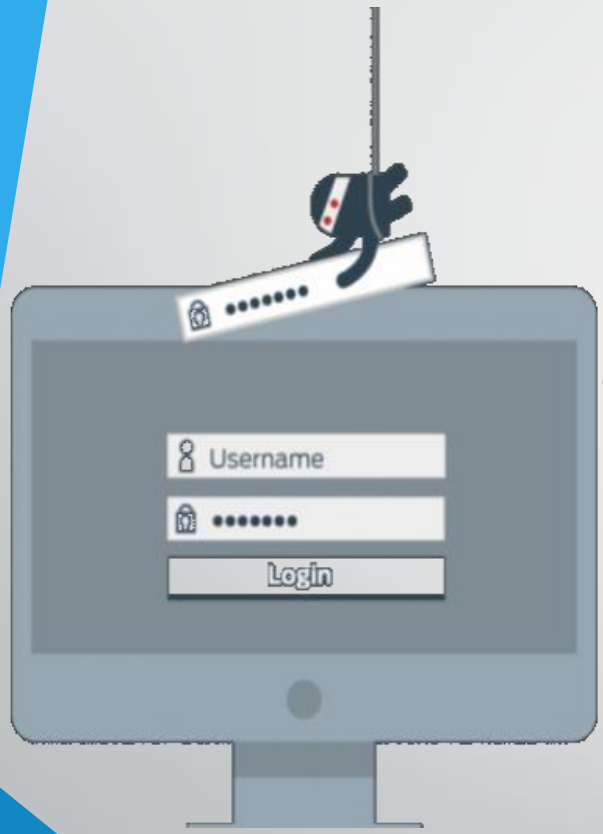
قد جرمت هذه الافعال كما في المادة الرابعة الفقرة الثانية

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

الانتحال والتغرير

الانتحال على صورتين





بسبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم

الانتحال والتغرير

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

نصت المادة الرابعة الفقرة الأولى

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين

التحريض على الجريمة المعلوماتية

نصت المادة التاسعة من النظام على أنه

يعاقب كل من حرض غيره أوساعده أواتفق معه على ارتكاب أي من الجرائم المنصوص عليهافي هذا النظام إذا وقعت الجريمة بناء على هذا التحريض أوالمساعدة أوالاتفاق

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

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 تزي على خمسة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا 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
- تحبذ الجماعات الإرهابية من خلال الانترنت انضمام عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية

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

تزامن
TAZAMUN

أدوات الإبلاغ عن الجريمة المعلوماتية

الشرطة حسب
الاختصاص المكاني

تطبيق كلنا أمن على
الأجهزة الذكية

هيئة الامر بالمعروف والنهي عن
المنكر عن طريق الهاتف المجاني
1909 أو الموقع الإلكتروني
www.pv.gov.sa

الاتصال على
الرقم 989

البوابة الإلكترونية
لوزارة الداخلية (أبشر)

البريد الإلكتروني
info.cybercrime@moisp.gov.sa

الثانوي اليوم

الجلسة التدريبية الثانية

الانترنت لا ينسى !!

نشاط ٣-١ هل تحذف البيانات

- قم بالدخول للرابط التالي النسخة المخبأة

https://www.google.com/

نشاط ٣-٢ هل تحذف البيانات

- قم بالدخول للرابط التالي أرشيف المواقع

https://archive.org/

(/http://te3p.com/)

نشاط ٣-٣ هل تحذف البيانات

- قم بالدخول للرابط التالي ولاحظ سجلك في قوقل
https://myactivity.google.com/more-activity

هل انا بعيد عن خطر الاختراق ؟

لماذا انا من وسط الملايين ؟.

أي شيء تبحث عنه ستجد إعلانات تظهر لك

هل يوجد أمان كامل في الانترنت

ما الحل

انت للبيع

أساليب الحماية

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

التحديثات


windows
update


Windows Update
تم إيقاف التحديثات مؤقتًا
لن يتم تحديث جهازك أثناء إيقاف التحديثات مؤقتًا.
سيتم استئناف التحديثات في ٤١/٠٩/٠٦
استئناف التحديثات
تشغيل
إيقاف التحديثات مؤقتًا لـ ٧ يومًا (أيام) إضافية
يمكنك الانتقال إلى الخيارات المتقدمة لتغيير مدة الإيقاف المؤقت
تغيير الساعات النشطة
٠٥:٠٠ م 08:00 ص الآن إلى
عرض محفوظات التحديثات
عرض التحديثات المثبتة على جهازك
خيارات متقدمة
المزيد من عناصر التحكم في التحديث والإعدادات
الصفحة الرئيسية
العثور على إعداد
التحديث والأمان
Windows Update
تحسين التسليم
أمن Windows
النسخ الاحتياطي
استكشاف الأخطاء وإصلاحها
استرداد
التنشيط
البحث عن جهازي
للمطوّرين
برنامج Windows Insider

برامج الحماية (الانتي فايروس)

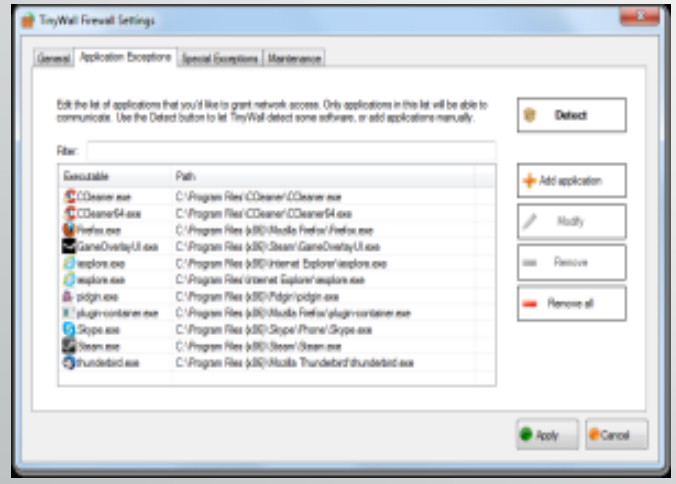
AVG AVIRA eset
VIPRE KASPERSKY PANDA SECURITY
TOTAL DEFENSE pc tools McAfee An Intel Company
LAVASOFT Dr.WEB TREND MICRO

ما الأفضل

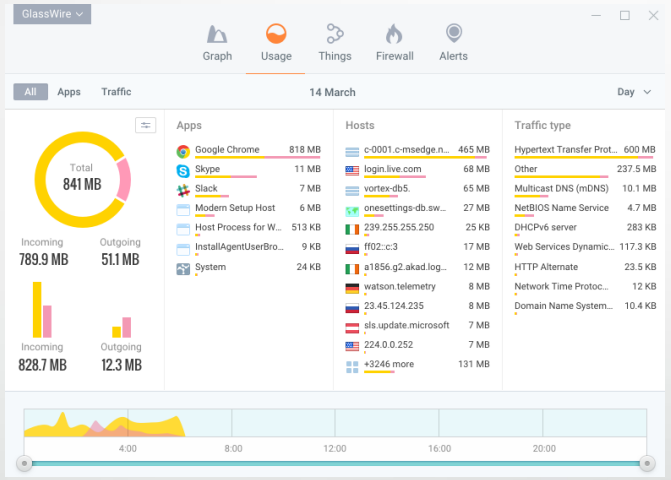
https://www.av-test.org/en/

الجدار الناري

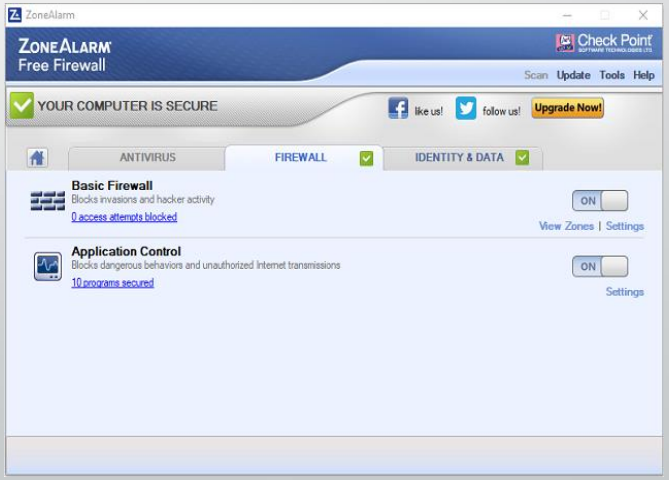
برنامج على جهاز الحاسوب الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة



https://tinywall.pados.hu/



https://www.glasswire.com/



https://www.zonealarm.com/software/free-firewall

الملفات و المنافذ

https://nmap.org/

NirSoft

https://www.nirsoft.net/

فحص المنافذ في جهازك ومن تواصل معها

https://directorymonitor.com/

لمراقبة جميع التغييرات التي تكون في أي مجلد
يعطي تنبيهات ما الذي حدث داخل المجلد ، سواء كان
حذف ملفات او إنشاء ملفات

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

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

طرق اختيار كلمة المرور

1. يجب أن تتكون كلمة المرورمن ٨ أحرف على الأقل ، ويفضل استخدام اثنا عشررمزا أو أكثر
2. يجب أن تحتوي على أحرف كبيرة وصغيرة مثال a A
3. يجب أن تحتوي على رقم على الأقل مثال 7
4. أن تحتوي على أي من الرموزالخاصة الموجودة في لوحة المفاتيح مثال $ # &

لتجعل من اختراق رقمك السري مستحيلاً بإذن الله! استخدم طريقة "الأنماط الابداعية"، والتي تصعّب من كلمات المرور الخاصة بك وتجعلها متنوعة من حساب ومنصة لأخرى، وتصعب عليك نسيانها، لأنك ستحفظ نمط وليس كلمة مرور معينة! وهذه الطريقة من أفضل طرق توليد كلمات المرور الصعبة لحساباتك. الشرح:

كوّن رقمك السري من الأنماط الإبداعية ليكون صعب الاختراق

إعداد:
عبدالعزيز الحمادي
@Abdulaziz_Hmadi

مثال النمط الأول

AlahmadSalihah1410Twitter#

اسم العائلة + اسم والدتك + تاريخ مميز لك + اسم الخدمة التي تستخدمها + علامة ترقيم

مثال النمط الثاني

AbAh0123Snap@

الحرفين الأولى من اسمك + من اسم والدك + آخر ٤ أرقام من جوالك + اسم الخدمة + علامة ترقيم

مثال النمط الثالث

Twitter#2022AzizRiyadh

اسم الخدمة + علامة ترقيم + تاريخ مميز لك + اسمك + مدينتك

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.

- 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 A -Z والأرقام ٩ - ٠ هي من الحروف الخاصة

نشاط ٣-٤

اعرف ماذا يوجد بجهازك

- كلمات السر المحفوظة
- سجلك في المتصفح (history)
- المتصفح الخفي

هيا نطبق

نشاط ٣-٥

اختبر قوة كلمة المرور لديك..

- كلمات المرور https://howsecureismypassword.net/

نشاط ٣-٦

ابحث عن اسمك (NIKNAME) المحجوز في مواقع التواصل في الانترنت..

- الاسم المحجوز https://namechk.com/

مثال: tnumeih_rab

طرق اختيار كلمة المرور

- يعتبر البريد الإلكتروني الشكل الرئيسي لتبادل المعلومات في الهواتف الذكية حاليا ، وفي معظم الأوقات يكون مفعلا على الشبكة، ممّا يجعل الشخص عرضة 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 روابط 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

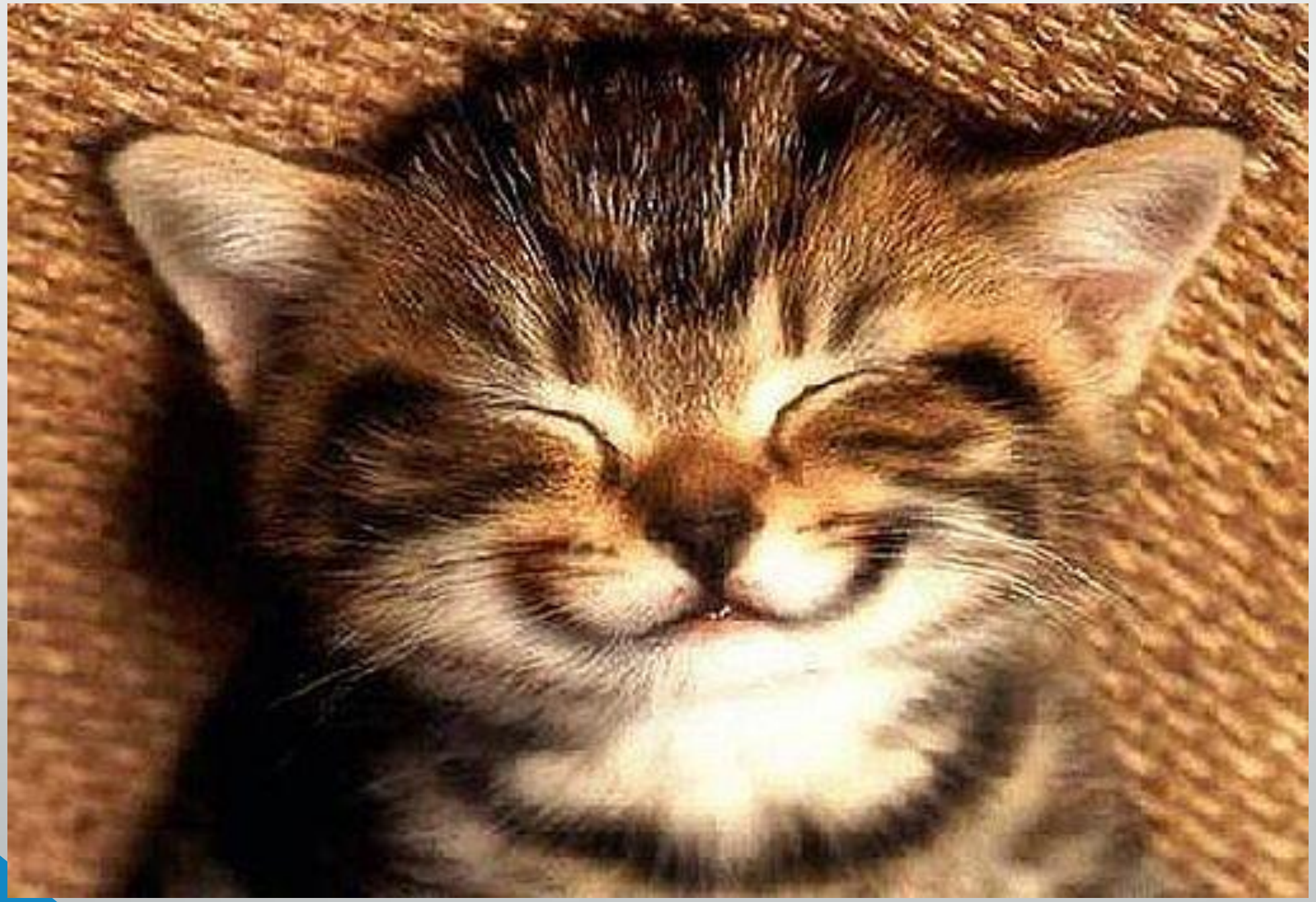
ينبغي حذف الرسائل النصية من المصادر المجهولة التي تطلب معلوماتٍ خاصة، وتجنب النقر على الروابط في الرسائل النصية، فبعض المخترقين يرسلون رسائل نصية قد تظهر أنّها من البنك الخاص أو أيّ مصدرٍ آخر موثوق، وفي حال الضغط على الرابط في الرسالة النصية

الحذر من شبكات الواي فاي المفتوحة

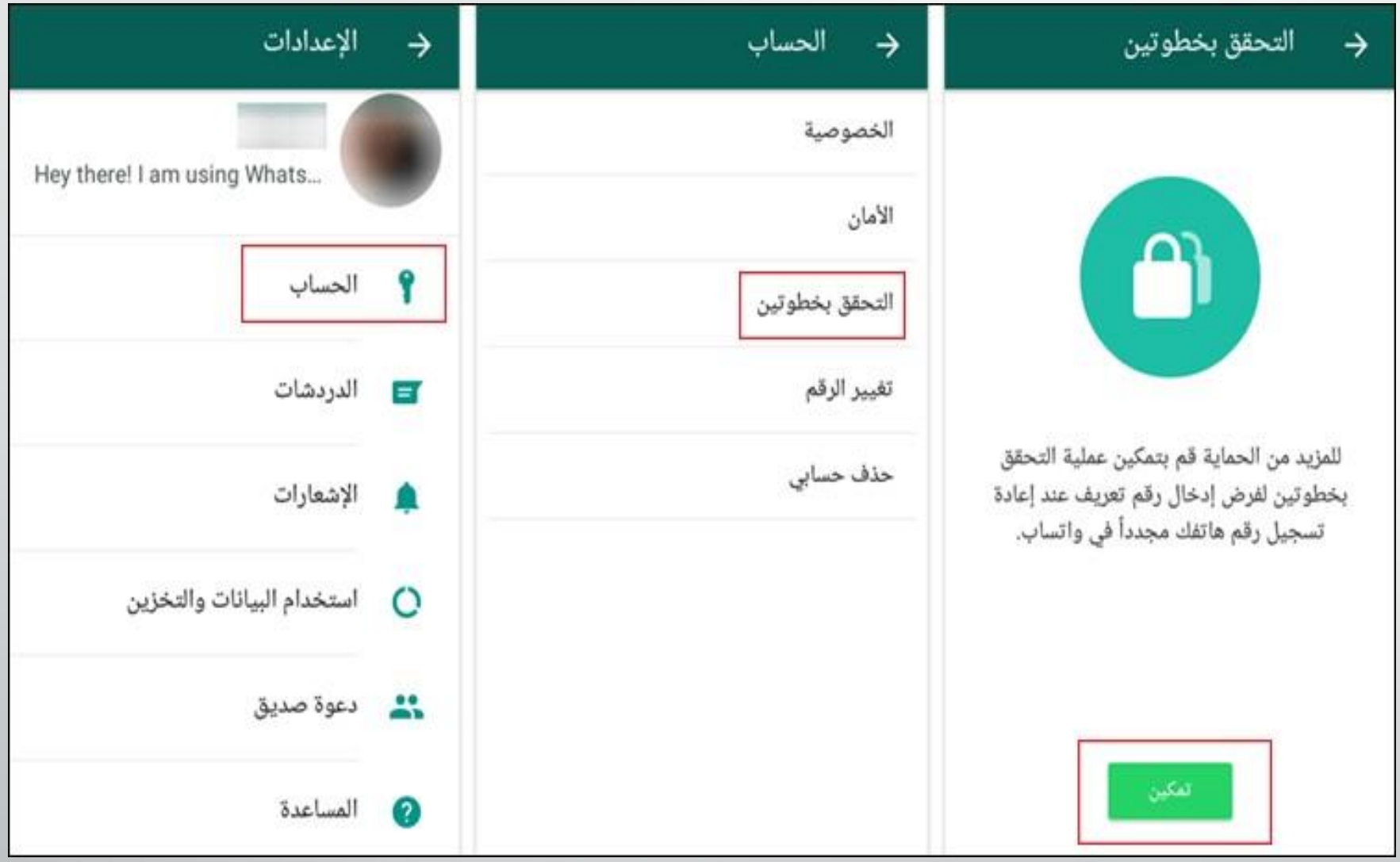
- ينبغي الدخول إلى الإنترنت من خلال الجهاز الخاص، وعن طريق شبكات واي فاي آمنة فقط، حيث إنّ شبكات الواي فاي غير الآمنة تسمح للمخترقين القريبين من التعرض للبيانات الشخصية عند الدخول إلى الإنترنت
- كما ينبغي عدم التسوق من الإنترنت أو القيام بالأمور المصرفية، باستخدام شبكات واي فاي عامة
- حيث إنّه يمكن للمخترقين 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

الثانية اليوم

الجلسة التدريبية الثالثة



حماية مواقع التواصل الاجتماعي



ادخل إلى حساب تويتر الخاص بك من جهاز الكمبيوتر، ثم اذهب إلى "الإعدادات والخصوصية" ثم اضغط على "الأمان"

- اللحظات
- وضع الترويج
- إعلانات تويتر
- التحليلات
- Media Studio
- الإعدادات والخصوصية

المصادقة بعاملين

المصادقة بعاملين

إذا قمت بتشغيل أكثر من وسيلة واحدة من وسائل الأمان هذه، فيمكنك اختيار الوسيلة التي تستخدمها في كل مرة تسجّل فيها الدخول. معرفة المزيد

طرق التوثيق

رسالة نصية

استخدم هاتفك المحمول لتلقي رسالة نصية تحتوي على رمز توثيق لإدخاله في كل مرة تسجّل فيها الدخول إلى تويتر.

تطبيق التوثيق على الهاتف المحمول

استخدم تطبيق توثيق عبر الهاتف المحمول لتلقي رمز توثيق لإدخاله في كل مرة تسجّل فيها الدخول إلى تويتر.

مفتاح الأمان

استخدم مفتاح أمان مادي يتم إدخاله في الكمبيوتر أو تتم مزامنته مع هاتفك المحمول في كل مرة تسجّل فيها الدخول إلى تويتر.


twitter


نسخ الرمز احتياطيًا
إذا فقدت إمكانية الوصول إلى جهازك في أي وقت، يمكنك استخدام هذا الرمز لتوثيق هويتك.
اكتب هذا الرمز أو التقط لقطة شاشة له واحفظه في مكان آمن. هذا الرمز يمكن استخدامه مرة واحدة فقط. معرفة المزيد
نسخ الرمز
إنشاء رمز جديد
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows.

التطبيقات والجلسات

التطبيقات

لا توجد لديك أية تطبيقات تم ربطها

عند ربطك لتطبيق تابع لجهة خارجية بحسابك على تويتر، فإنك تمنح هذا التطبيق حق الوصول لاستخدام حسابك.

الجلسات

Windows

جدة, المملكة العربية السعودية · نشط حاليًا

تسجيل الخروج من كل الجلسات الأخرى

سوف يعمل ذلك على إنهاء 2 من جلسات تويتر النشطة. ولن يؤثر على جلستك الحالية. معرفة المزيد

iPhone

مكة المكرمة, المملكة العربية السعودية · منذ ٥٤ دقيقة

iPhone

مكة المكرمة, المملكة العربية السعودية · منذ ٥٤ دقيقة


المصادقة الثنائية
لقد أرسلنا رمزًا إلى
يُرجى إدخاله أدناه.
2 7 6 8 4 1


المصادقة الثنائية
التحقق من تسجيل الدخول يساعد على زيادة تأمين حسابك.
عند تفعيل التحقق من تسجيل الدخول، ستحتاج إلى كلمة المرور ورمز التحقق المُرسَل إلى هاتفك لتسجيل الدخول على أجهزة جديدة.
متابعة


إعدادات
حسابي
الاسم
اسم المستخدم
عيد الميلاد
رقم الهاتف
البريد الإلكتروني
كلمة المرور
المصادقة الثنائية
التطبيقات المتصلة
الإشعارات
Bitmoji
Shazam
ادخل إلى
اعدادات الحساب
ثم اذهب إلى
المصادقة الثنائية

أساليب الحماية

- توتير
- فيس بوك
- سناب شات
- واتس

احذر من البرامج من غير المتجر الأصلي للبرنامج.

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

نشاط ٣-٧

فحص الملفات و الروابط

https://www.virustotal.com/gui/home

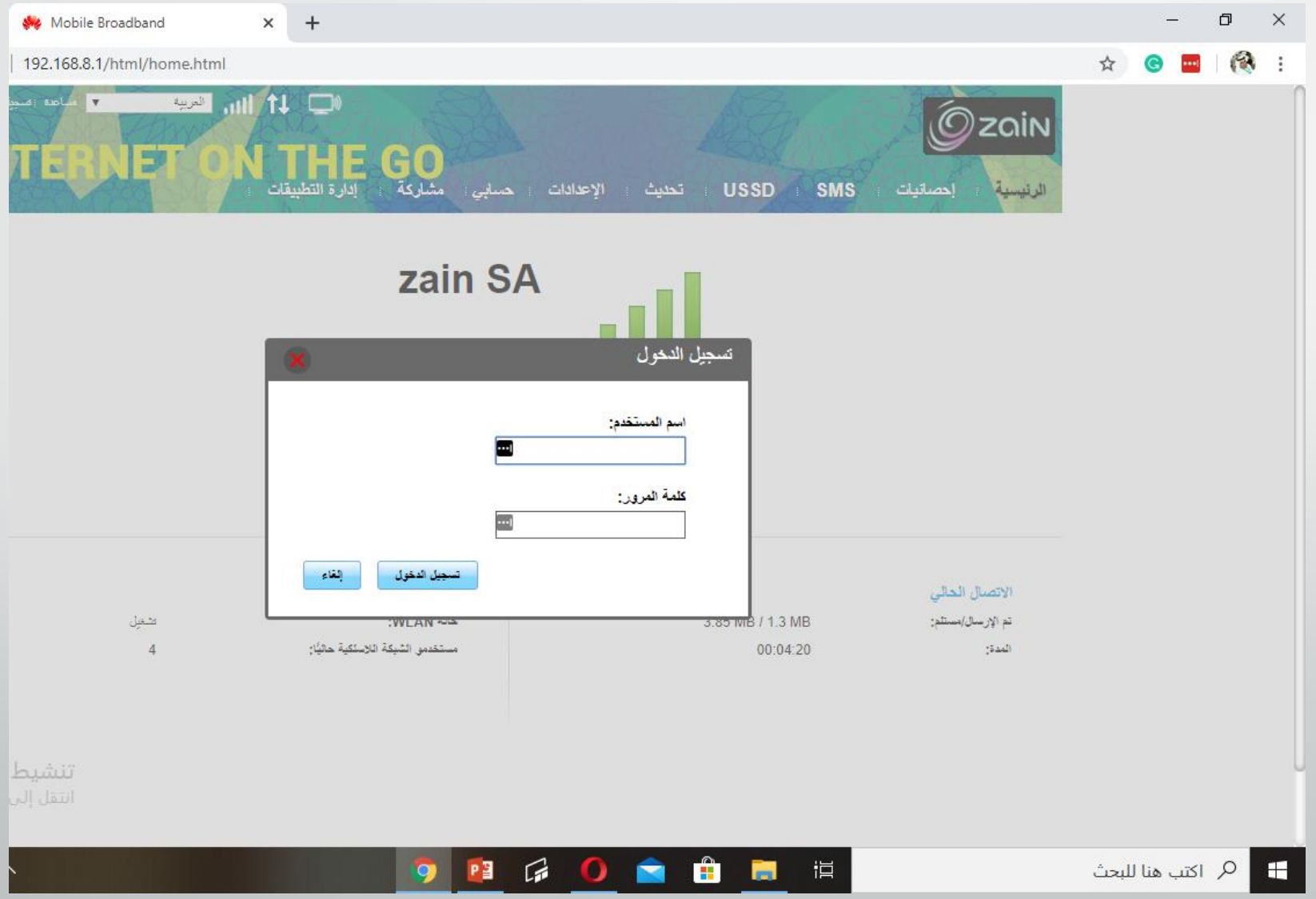
فحص الملفات و الروابط نورتن

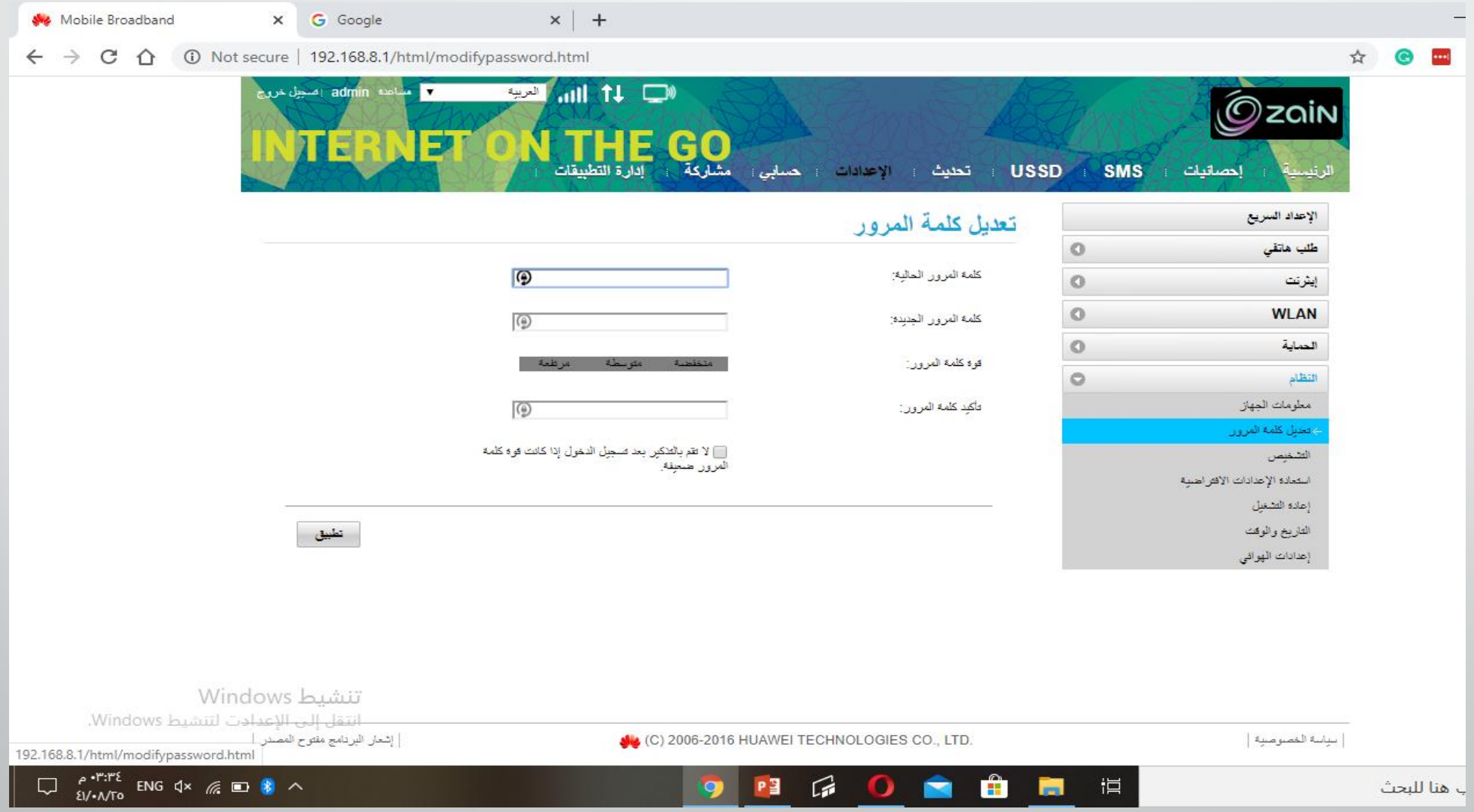
https://safeweb.norton.com/

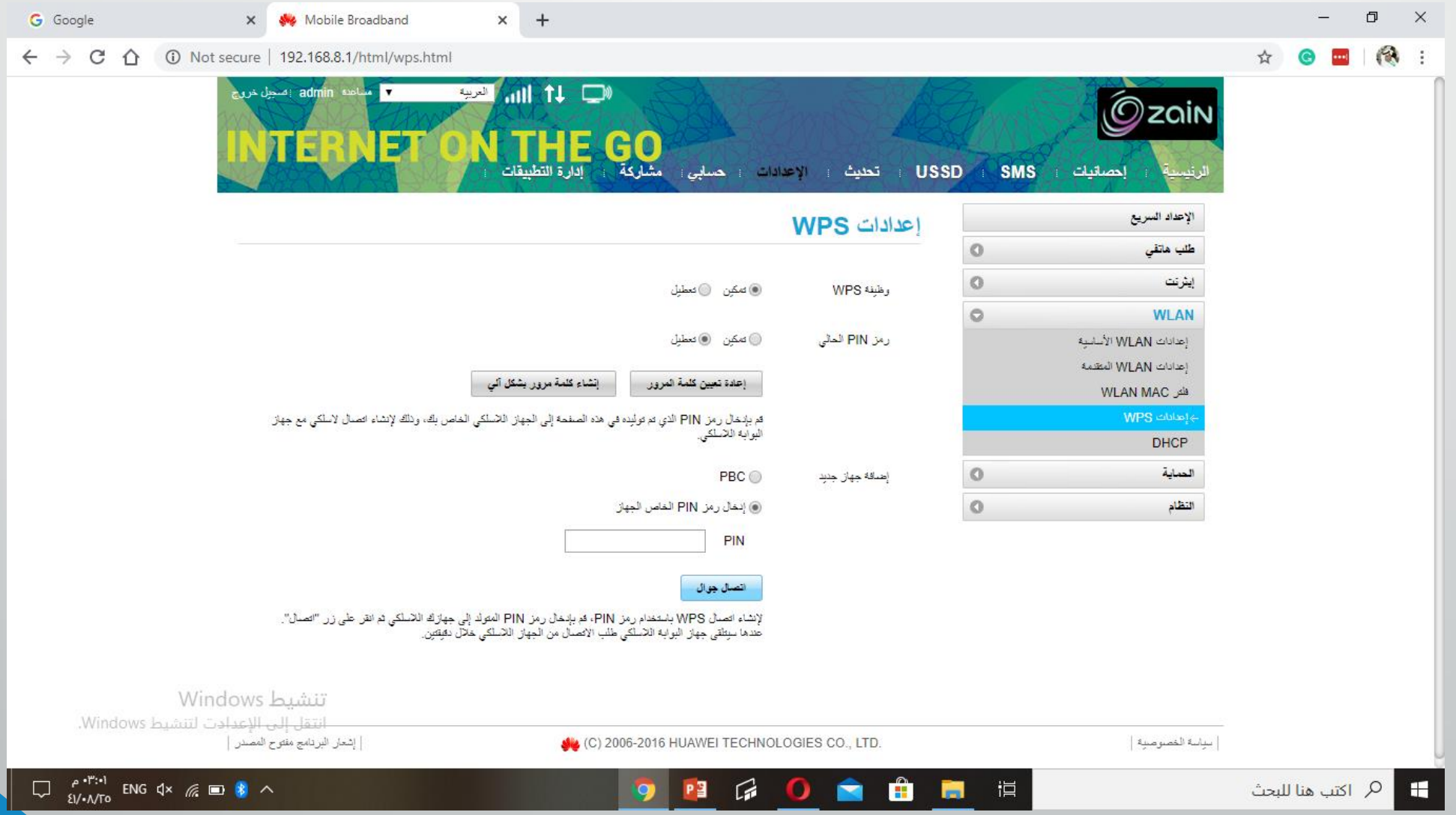
احم نفسك في عالم الانترنت

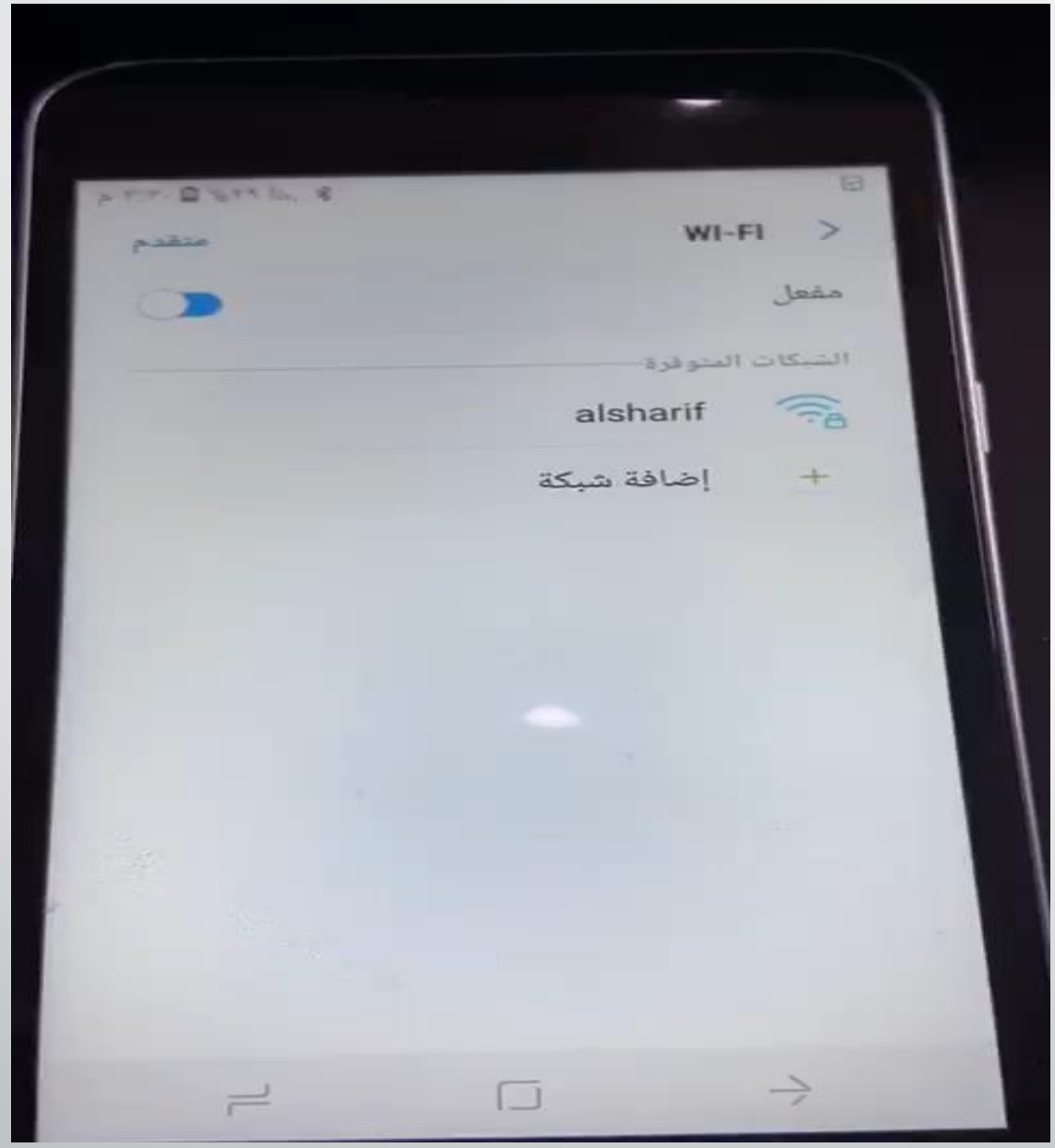
تامين شبكة wifi

تأمين الشبكة المنزلية




Mobile Broadband
Google
Not secure | 192.168.8.1/html/modifypassword.html
zain
INTERNET ON THE GO
الرئيسية | إحصائيات | SMS | USSD | تحديث | الإعدادات | حسابي | مشاركة | إدارة التطبيقات
admin | تسجيل خروج
العربية
الإعداد السريع
طلب هاتفي
إنترنت
WLAN
الحماية
النظام
معلومات الجهاز
تعديل كلمة المرور
التشخيص
استعادة الإعدادات الافتراضية
إعادة التشغيل
التاريخ والوقت
إعدادات الهوائي
تعديل كلمة المرور
كلمة المرور الحالية:
كلمة المرور الجديدة:
قوة كلمة المرور:
منخفضة متوسطة مرتفعة
تأكيد كلمة المرور:
لا تقم بالتذكير بعد تسجيل الدخول إذا كانت قوة كلمة المرور ضعيفة.
تطبيق
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows.
(C) 2006-2016 HUAWEI TECHNOLOGIES CO., LTD.
سياسة الخصوصية | إشعار البرنامج مفتوح المصدر
192.168.8.1/html/modifypassword.html
ENG
٠٣:٣٤ م
٤١/٠٨/٢٥
هنا للبحث


Google
Mobile Broadband
Not secure | 192.168.8.1/html/wps.html
zain
INTERNET ON THE GO
admin
العربية
الرئيسية | إحصائيات | SMS | USSD | تحديث | الإعدادات | حسابي | مشاركة | إدارة التطبيقات
الإعداد السريع
طلب هاتفي
إنترنت
WLAN
إعدادات WLAN الأساسية
إعدادات WLAN المتقدمة
فلتر WLAN MAC
إعدادات WPS
DHCP
الحماية
النظام
إعدادات WPS
وظيفة WPS
تمكين
تعطيل
رمز PIN الحالي
إعادة تعيين كلمة المرور
إنشاء كلمة مرور بشكل آلي
قم بإدخال رمز PIN الذي تم توليده في هذه الصفحة إلى الجهاز اللاسلكي الخاص بك، وذلك لإنشاء اتصال لاسلكي مع جهاز البوابة اللاسلكي.
إضافة جهاز جديد
PBC
إدخال رمز PIN الخاص الجهاز
PIN
اتصال جوال
لإنشاء اتصال WPS باستخدام رمز PIN، قم بإدخال رمز PIN المتولد إلى جهازك اللاسلكي ثم انقر على زر "اتصال".
عندها سيلتقي جهاز البوابة اللاسلكي طلب الاتصال من الجهاز اللاسلكي خلال دقيقتين.
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows.
(C) 2006-2016 HUAWEI TECHNOLOGIES CO., LTD.
سياسة الخصوصية | إشعار البرنامج مفتوح المصدر
اكتب هنا للبحث


WI-FI
متقدم
مفعل
الشبكات المتوفرة
alsharif
إضافة شبكة

ملخص اليوم التدريبي الثاني

اليوم الثاني

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

وزارة التعليم
Ministry of Education

NCEPD

الأمن السيبراني

خطة البرنامج التدريبي

اليوم التدريبي	الجلسة التدريبية	العنوان	الموضوع/الموضوعات	الهدف/ المحور	الزمن
الثالث	الأولى	البرامج الخبيثة	الفيروسات الديدان احصنة طروادة	التعرف على أشهر البرمجيات الخبيثة وطرق عملها.	٩٠ دقيقة
	استراحة				٢٠ دقيقة
	الثانية	البرامج الخبيثة	خبراء ومجرمي الأمن السيبراني	التعرف على خبراء ومجرمي الأمن السيبراني ودور كل منهم.	٦٠ دقيقة
	استراحة				١٠ دقائق
	الثالثة	البرامج الخبيثة	شهادات الأمن السبراني جهود المملكة سبرانيا	التعرف على تخصصات الأمن السبراني الاطلاع على جهود المملكة سبرانيا	٦٠ دقيقة


اليوم الثالث
الجلسة التدريبية الأولى

تحذيقة

أقوى كلمة مرور

https://forms.office.com/Pages/ResponsePage.aspx?id=DQSIkWdsWoyxEjajBLZtrQAAAAAAAAAAAFLgMEQB7pUNlVGMEYzSTFRNFcoQTZIUjBSSk8yRlpXWS4u

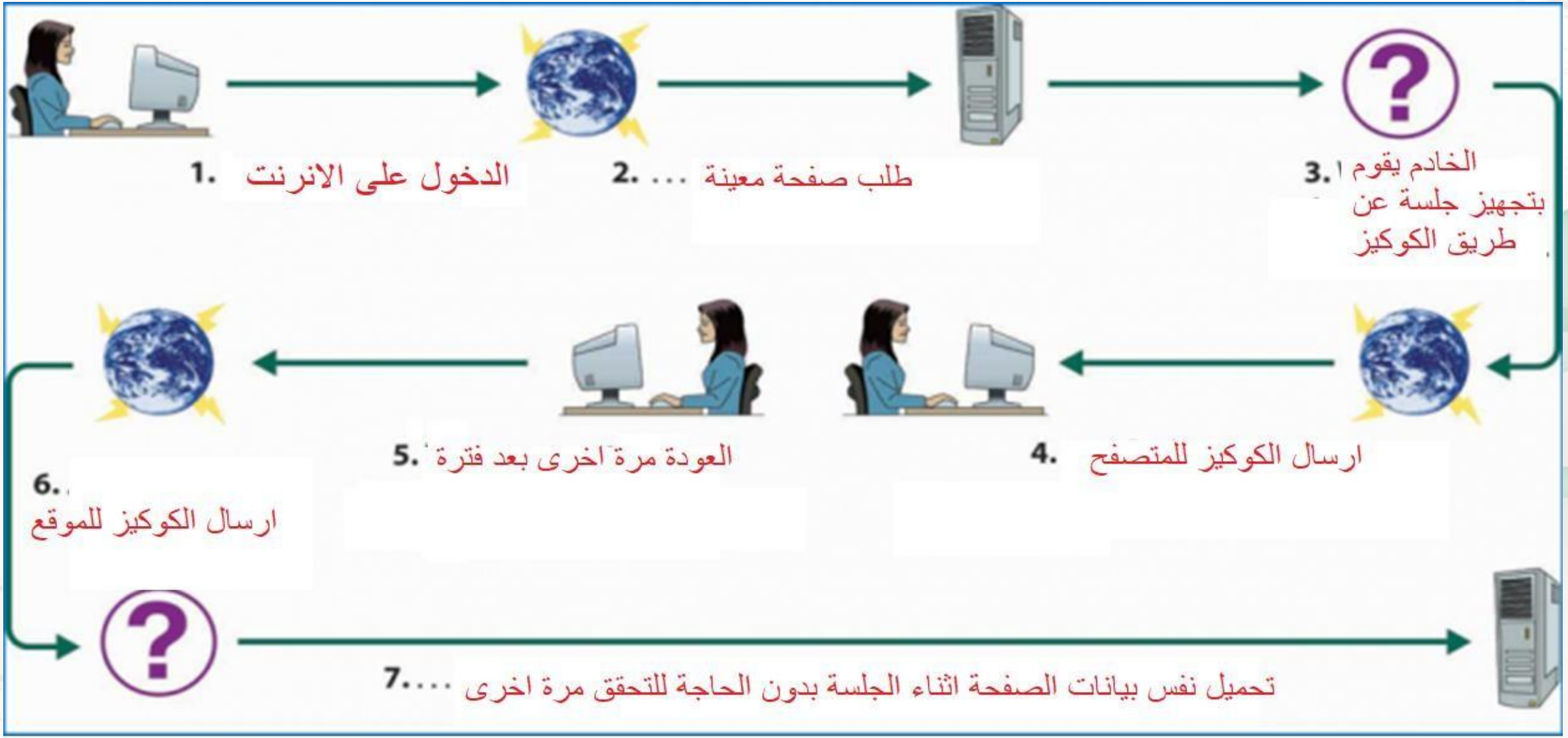
البرامج الخبيثة :

ملفات تعريف الارتباط (Cookie)

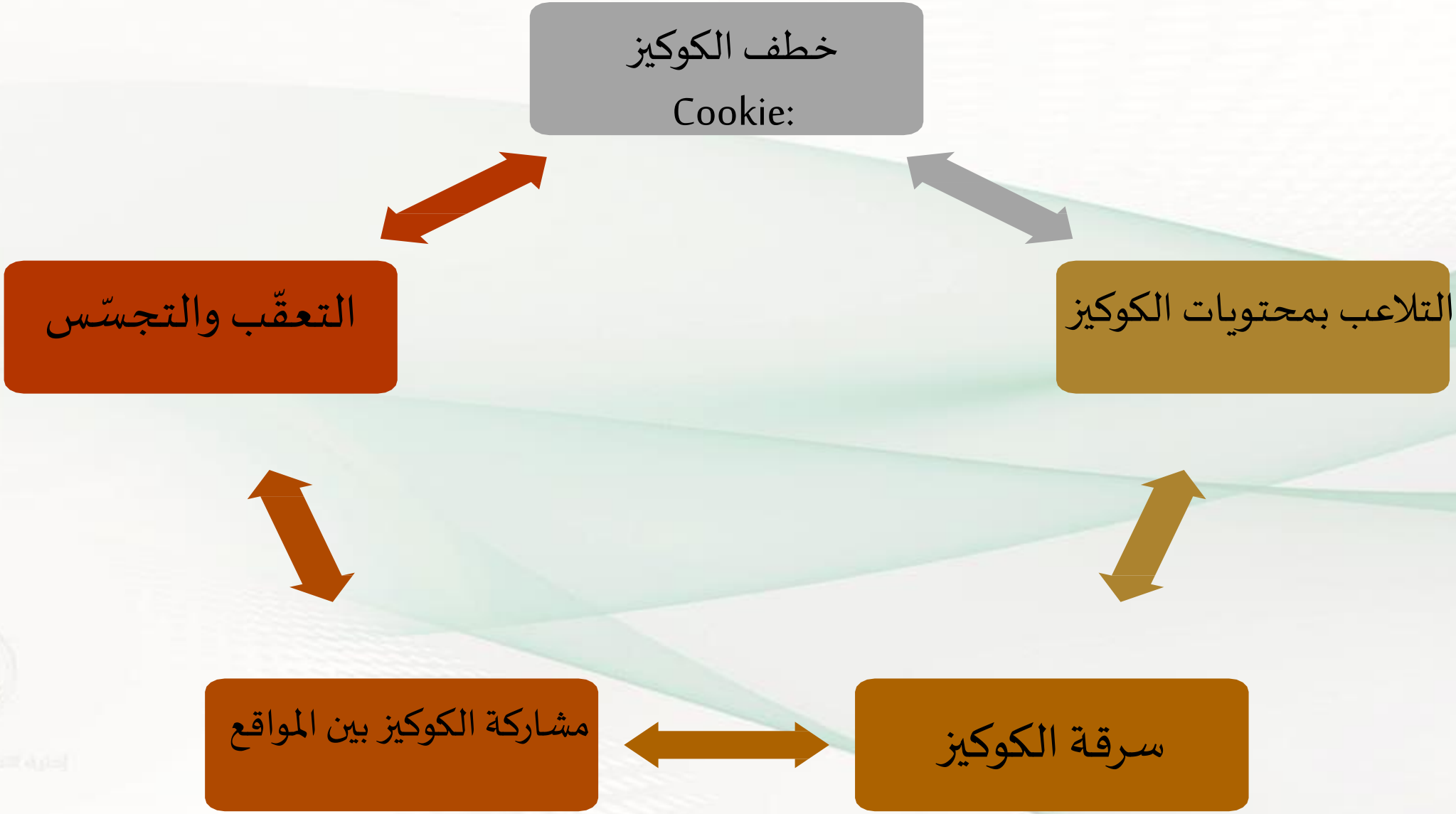
ماهي ؟ هي عبارة عن ملف نصّي يقوم الخادم بتخزينه على القرص الصلب لجهاز المستخدم عن طريق المتصفّح عند زيارة المستخدم لصفحة الويب. يتمّ تبادل ملفات الكوكيز بين الخادم وصفحة الويب عن طريق بروتوكول نقل النص التشعبي.

محتويات الكوكيز؟ هذه المحتويات تشمل:(اسم الملف- مُحتوى الملف- عنوان صفحة الويب التي قامت بتخزين الملف- تاريخ انتهاء مفعول الملف- نوع اتصال الإنترنت)

ملفات تعريف الارتباط (Cookie)



ملفات تعريف الارتباط (Cookie)



البرامج الخبيثة :

يقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض.

ويمكن تصنيف أنواع البرمجيات الخبيثة على النحو التالي:

١) الفيروسات (Viruses)

٢) الديدان (Worms)

٣) برامج التجسس (Spywares)

٤) أحصنة طروادة Trojan Horses.

الفيروسات Viruses

فيروسات الكمبيوتر هي برامج تقوم بمهاجمة و إتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة

ديدان الحاسب Worm

- 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 Spyware:

- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

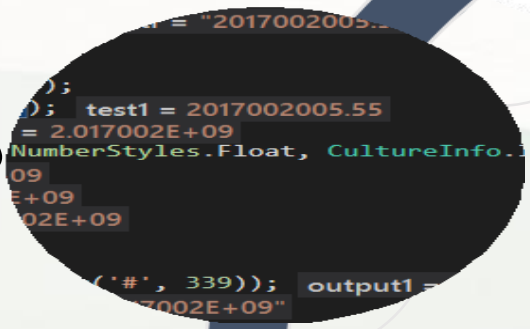
أحصنة طروادة : Trojan Horses

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

آثار الفيروسات

بطء في الجهاز

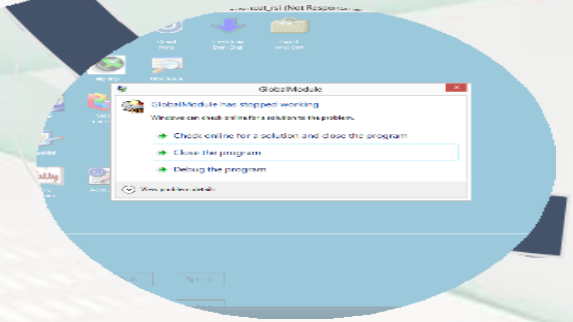
سلوك غريب للجهاز



أداء غير متزن

فقدان غير متوقع لبيانات مختلفة

إيقاف مفاجئ متكرر



كيف تصاب بالفيروسات

النوافذ المنبثقة على مواقع الويب المشكوك فيها

من خلال التخفي على أنها برامج مفيدة

ملفات مخفية في رسائل البريد الإلكتروني العشوائية من المخترقين أو الأنظمة المصابة الأخرى

باستخدام مكافح فيروسات الكمبيوتر غير محدث

زيارة موقع مصاب

فتح البريد الإلكتروني العشوائي أو مرفق البريد الإلكتروني

مشاركة الملفات أو الصور مع مستخدمين آخرين

تثبيت تطبيقات البرمجيات السائدة دون قراءة اتفاقيات الترخيص بدقة

تنزيل الألعاب وأشرطة الأدوات ومشغلات الوسائط وأدوات النظام الأخرى مجانًا

أخطر الفيروسات

KASPERSKY

فيروسات الفدية

متوسط الفدية التي يطلبها قراصنة فيروسات الفدية
قد تصل إلى قرابة **300** دولار أمريكي

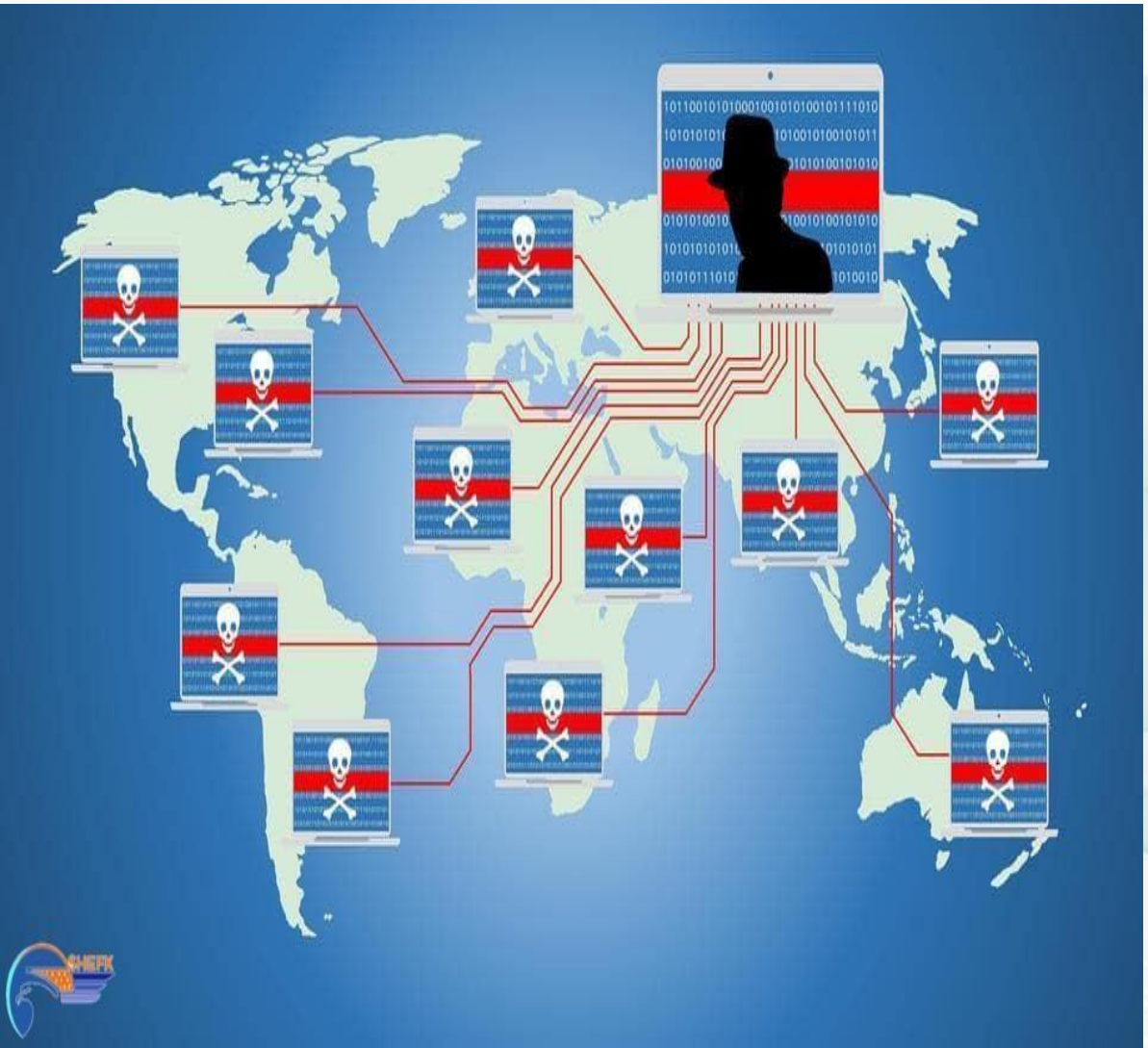
برامج التشفير

تعمل برامج التشفير على تشفير الملفات
حتى لا يتسنى لضحايا فيروسات الفدية استخدامها. ثم يطلب
القراصنة فدية مقابل استعادة إمكانية الولوج إلى الملفات.

برامج الحجب

تحجب هذه البرامج أجهزة الحاسوب الخاصة بالضحايا،
وبالتالي لا يستطيع أحدٌ استخدامَها. عادةً ما يسهل معالجة
هذا النوع من الفيروسات الخبيثة أكثر من برامج التشفير.

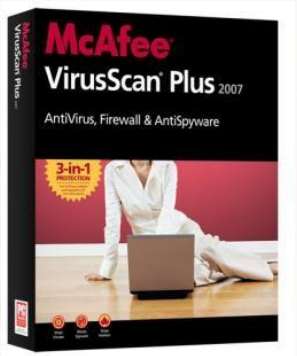
أخطر الفيروسات

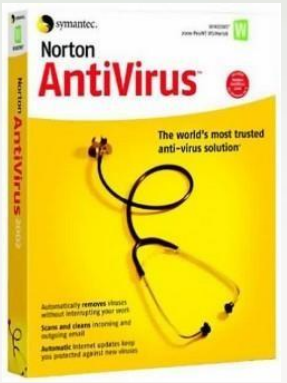


البوت نت Botnet هو مجموعة من أجهزة متصلة ببعضها عبر شبكة إنترنت، قد تكون هذه الأجهزة حواسب أو هواتف ذكية أو خوادم أو أجهزة أخرى تعرف بإنترنت الأشياء، وجميع هذه الأجهزة المتصلة تكون مصابة ويتم التحكم بها عبر نوع من البرامج الخبيثة، وفي حالا ت عديدة قد لا يدرك المستخدم أن حاسبه يتعرض لهجوم أو إصابة بوت نت

مكافحات الفيروسات Antis - spyware & Anti - virus

- يكتشف برنامج مكافحة الفيروسات البرامج الضارة ويمكن أن يتلفها قبل حدوث أي ضرر
- يجب تثبيت وصيانة برامج مكافحة الفيروسات لمكافحة برامج التجسس
- تأكد من تحديث برامج مكافحة الفيروسات
- توجد العديد من الخيارات المجانية والدفع





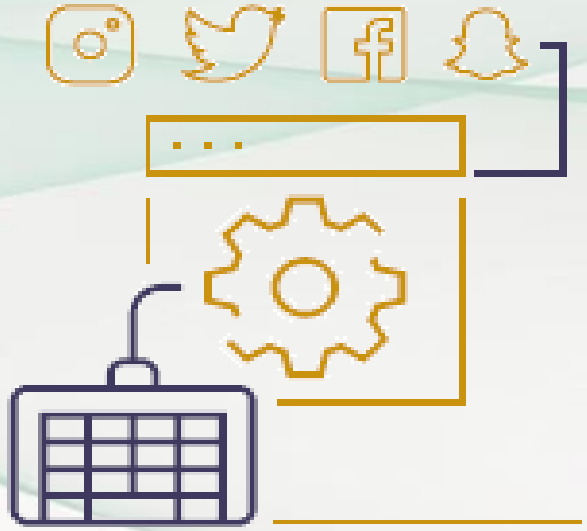
أخطر الفيروسات

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

الإبلاغ عن الإساءة – خدمة الترشيح

للإبـلاغ عـن المواقـع والمـواد التـي تتنافـى مـع الديـن الحنيف
والأنظمـة الوطنية يمكن طلب حجبها، مـن خلال القنوات التالية:

موقع ترشيح السعودية	تطبيق ترشيح السعودية	البريد الإلكتروني	الهاتف
www.filter.sa	البحث في متاجر الايفون والأندرويد	block@internet.gove.sa	011 - 4619485

الإبلاغ عن الإساءة - انستغرام

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : الموقع يشترط أن تبلغ من العمر ١٣ عاماً لتكون مؤهلاً لاستخدامه؟

المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية

- انتحال الشخصية
- العنصرية، الكراهية أو السلوك العنيف.
- انتهاك حقوق الملكية.
- انتهاك الخصوصية.
- الإساءة المضايقة أو التهديد.
- القري أو الإباحية.

٢ أدوات الإبلاغ

هل تعلم بأن موقع انستغرام يوفر أدوات فعالة للإبلاغ عن الإساءات التي يتعرض لها المستخدمون، ومن ذلك أدوات الإبلاغ عن

- الحسابات المخترقة.
- إنتحال الشخصية.
- الأطفال دون السن القانونية.
- العنصرية، الكراهية أو السلوك العنيف.
- إنتهاك حقوق الملكية.
- إنتهاك الخصوصية.
- إيذاء الذات.
- الإساءة، المضايقة أو التهديد.
- الفري أو الإباحية.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://help.instagram.com

الإبلاغ عن الإساءة – يوتيوب

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية:

- انتحال الشخصية
- انتهاك الخصوصية.
- التهديدات.
- تعريض الأطفال للخطر.
- المحتوى الذي يضم مشاهد عُري ومشاهد جنسية.
- محتوى يضم مشاهد عنيفة أو قاسية.

٢ أدوات الإبلاغ

هل تعلم بأن موقع يوتيوب يوفر أدوات فعالة للإبلاغ عن الإساءات التي يتعرض لها المستخدمون، ومن ذلك أدوات الإبلاغ عن

- حماية الخصوصية.
- التحرش والتسلط بر الإنترت
- كلام يخص على الكراهية.
- إنتحال الشخصية التهديدات.
- تعريض الأطفال للخطر.
- المحتوى الذي يضم مشاهد عُري ومشاهد جنسية.
- محتوى يضم مشاهد عنيفة أو قاسية.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://www.youtube.com/reportabuse

الإبلاغ عن الإساءة – سناب تشات

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : الموقع يشترط أن تبلغ من العمر ١٣ عاماً لتكون مؤهلاً لاستخدامه؟

المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية

- انتهاك الخصوصية.
- انتهاك الحقوق التجارية، الملكية أو النشر
- الإساءة، المضايقة، التهديد أو التشهير.
- الإباحية.
- العنف أو الكراهية
- الرسائل المزجة، الفيروسات، البرمجيات
- الخبيثة أو تعريض الخدمة للاختراق.

٢ أدوات الإبلاغ

هل تعلم بأن موقع سناب تشات يوفر أدوات فعالة للإبلاغ عن الإساءات التي يتعرض لها المستخدمون، ومن ذلك أدوات الإبلاغ عن

- الإساءة أو المسائل المتعلقة بالأمان أو بالمحتوى غير الملائم.
- الرسائل المزعجة.
- إنتحال الشخصية.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://support.snapchat.com

الجلسة التدريبية الثانية

الأمن السيبراني - عالم من الخبراء والمجرمين :

الأمن السيبراني - عالم من الخبراء والمجرمين

من هم الهاكرز؟؟؟؟

الهاكرزهم الأفراد ذوي المهارات البرمجية المتقدمة، يستخدمون هذه المهارات لاختبارحدود وقدرات النظم المبكرة، وقد شاركوا في وقت مبكرأيضا في تطويرألعاب الكمبيوتر.

مجالات الأمن السيبراني

- مع وجود الكم الهائل من البيانات في العالم الرقمي لابد من توفير مجال محمي سواء بحدود منطقية أو مادية.
- يتعين على خبراء الأمن السيبراني حماية مجالاتهم وفقًا لقوانين بلدهم.

أمثلة على مجالات الأمن السيبراني

نمو المجالات السيبرانية

البيانات التي يتم جمعها داخل الإنترنت هي أكثر بكثير من مجرد البيانات التي يساهم بها المستخدمون طواعية

مع ظهور تكنولوجيات جديدة، مثل نظم المعلومات الجغرافية GIS و انترنت الأشياء IOT تشكل البيانات التي يتم جمعها بواسطتها تحدًا هائلاً لمحترفي الأمن السيبراني في المستقبل.

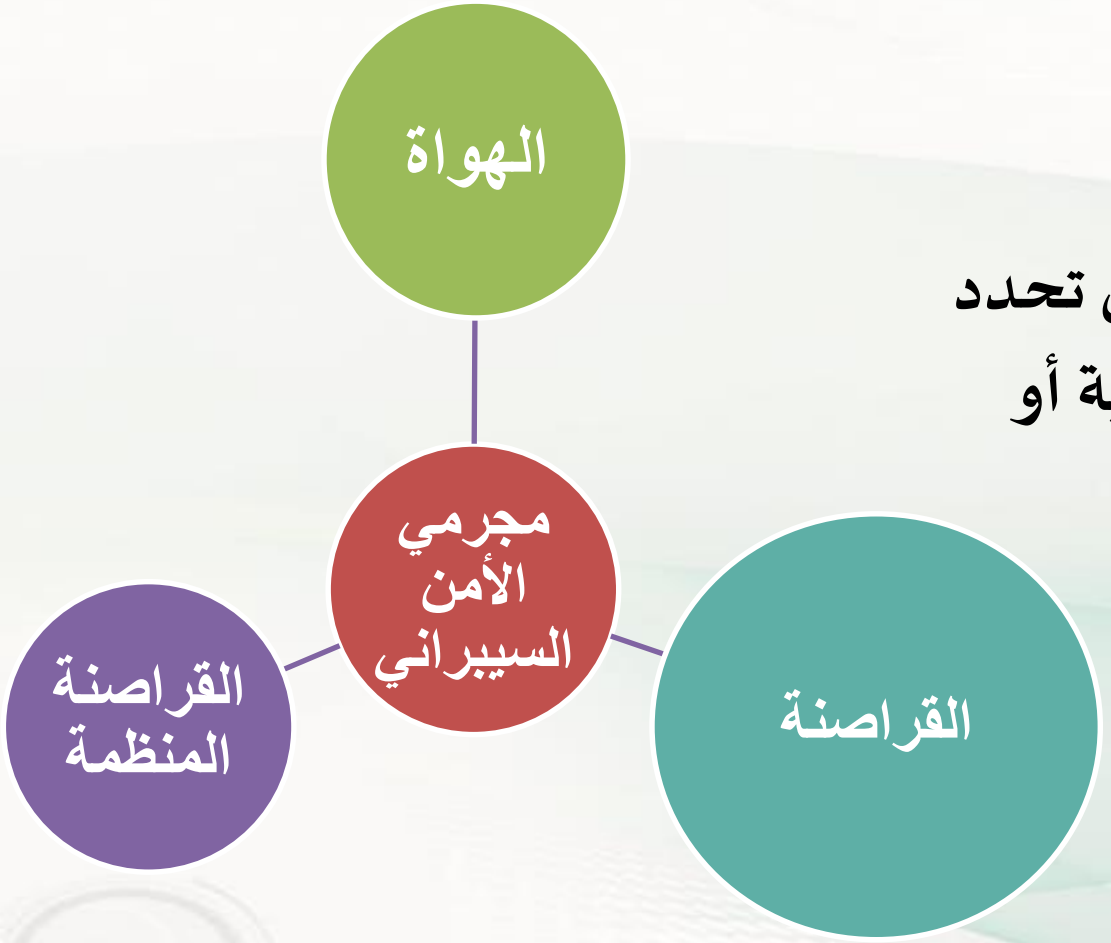
مجرمي الأمن السيبراني

مجرمي الأمن السيبراني

الهواة

- يمتلك الهواة أو مهربو البرامج مهارة قليلة أو معدومة ، وغالبًا ما يستخدمون أدوات أو تعليمات موجودة على الإنترنت لشن هجمات.
- بعضهم فضولي ، بينما يحاول البعض الآخر إظهار مهاراتهم والتسبب في ضرر.
- حتى وأن استخدموا الأدوات الأساسية لشن هجماتهم، لكن النتائج قد تكون مدمرة.

مجرمي الأمن السيبراني

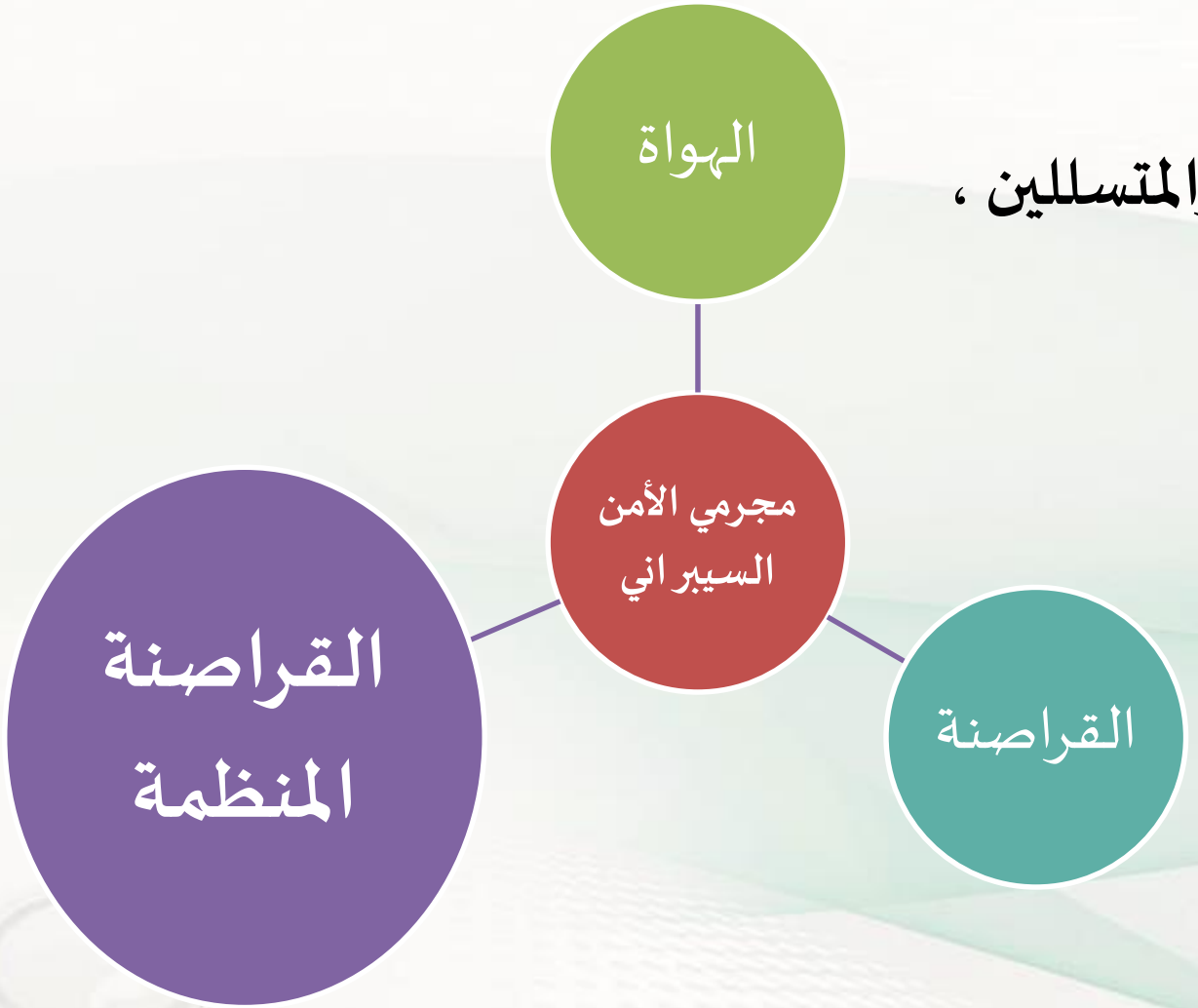


القراصنة

هذه المجموعة من المجرمين تقتحم أجهزة الكمبيوتر أو الشبكات للوصول لأسباب مختلفة. نية الاقتحام هي التي تحدد تصنيف هؤلاء المهاجمين على أنهم قبعات بيضاء أو رمادية أو سوداء.

- قبعات بيضاء
- قبعات سوداء
- قبعات رمادية

مجرمي الأمن السيبراني



قراصنة المنظمة

يشمل هؤلاء المجرمون منظمات مجرمي الإنترنت ، والمتسللين ، والإرهابيين ، والمتسللين الذين ترعاهم الدولة.

- مجرمو الإنترنت
- المتسللون
- المهاجمون الذين ترعاهم الدولة

مجرمي الأمن السيبراني

تاريخ عملية القرصنة:

- بدأت عملية القرصنة في الستينيات من القرن الماضي.
- في منتصف الثمانينات من القرن العشرين ، استخدم المجرمون أجهزة مودم الاتصال الهاتفي.
- في الوقت الحاضر، يتجاوز المجرمون سرقة المعلومات.
- الدافع الأكبر لمعظم مجرمي الإنترنت هو المال.

مجرمي الأمن السيبراني

Script kiddies:

- يشير إلى المراهقين أو المتسللين عديمي الخبرة

- **Vulnerability broker:**
- هم عادة قراصنة ذوو قبعة رمادية

- **hacktivists:**
- هم قراصنة قبعة رمادية يتظاهرون ويحتجون على الأفكار السياسة والاجتماعية المختلفة.

مجرمي الأمن السيبراني

- **Caper criminals:**
- هم قراصنة ذوو قبعة سوداء.

State-sponsored:

- إما يكونون قبعة بيضاء أو سوداء

لماذا تصبح أخصائي الأمن السيبراني؟

إمكانية أكبر في الكسب نتيجة ارتفاع الطلب على هذا المجال.

مهنة صعبة ورائعة، نتيجة للتغير السريع في تقنية المعلومات وبالتالي تغير في وسائل الحماية.

تواجد هذه المهنة في كل دولة ومنطقة تقريباً.

خدمة للجمهور وللدولة والحكومات والمنظمات من الهجمات والاختراقات المحتملة والتي تؤدي إلى كوارث لا تحمد عقباها.

إحباط مجرمي الإنترنت

إن إحباط مجرمي الإنترنت مهمة صعبة ومع ذلك ، بدأت الشركات والحكومات والمنظمات الدولية في اتخاذ إجراءات منسقة للحد من مجرمي الإنترنت أو صدهم.

تشمل ما يلي:

- إنشاء قواعد بيانات شاملة
- إنشاء أجهزة استشعار الإنذار المبكر وشبكات التنبيه
- تبادل المعلومات الاستخباراتية الإلكترونية
- وضع وتأسيس معايير لإدارة أمن المعلومات بين المنظمات الوطنية والدولية
- سن قوانين جديدة لثني الهجمات الإلكترونية و انتهاكات البيانات

التهديدات الشائعة للمستخدمين النهائيين

التهديدات ونقاط الضعف هي الشاغل الرئيسي لمحترفي الأمن السيبراني

عندما يكون التهديد هو احتمال وقوع حدث ضار، مثل الهجوم.

عندما تجعل الثغرة الأمنية هدفا عرضة للهجوم.

أنواع السجلات الشخصية

التهديدات التي يمكن للمجرمين إطلاقها ضد خدمات الإنترنت والشبكات

هناك العديد من الخدمات التقنية الأساسية اللازمة لشبكة ما ، وفي نهاية المطاف شبكة الإنترنت للعمل.

التهديدات لأسلوب حياة الناس

- **الأمن السيبراني**

هو الجهد المستمر لحماية الأنظمة والبيانات الشبكية من الوصول غير المصرح به.

- **على المستوى الشخصي**

يحتاج الجميع إلى حماية هويته وبياناته وأجهزته الحاسوبية.

- **على مستوى الشركات**

تقع مسؤولية حماية سمعة المؤسسة وبياناتها وعملائها على عاتق الموظفين.

- **على مستوى الدولة**

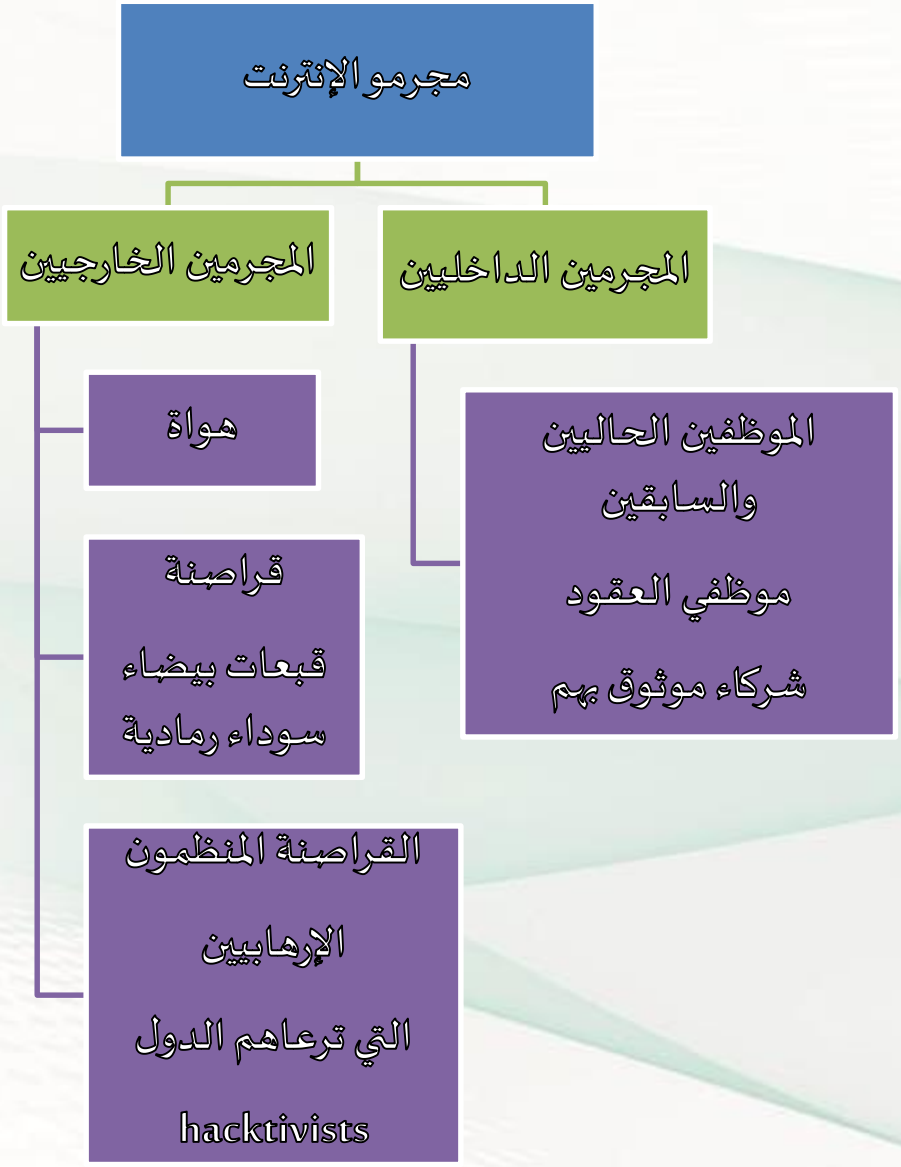
يتعرض الأمن القومي وسلامة المواطنين ورفاهيتهم للخطر.

التهديدات لأسلوب حياة الناس

- **وكالة الأمن القومي (NSA)في الولايات المتحدة:**

هي المسؤولة عن أنشطة جمع المعلومات الاستخبارية والمراقبة.

التهديدات الداخلية والخارجية



التهديدات الداخلية

يمكن أن يتسبب المستخدم الداخلي للمنظمة، مثل الموظف أو شريك العقد في الإضرار بالشركة، عن طريق الخطأ أو عن قصد من خلال التالي:

- تعطل البيانات السرية
- تهديد عمليات الخوادم الداخلية أو أجهزة البنية التحتية للشبكة
- تسهيل الهجمات الخارجية عن طريق توصيل وسائط USB المصابة بنظام الكمبيوتر الخاص بالشركة.
- دعوة البرامج الضارة عن طريق الخطأ إلى الشبكة من خلال البريد الإلكتروني أو مواقع الويب الضارة.

التهديدات الداخلية لها القدرة على إحداث أضرار أكبر من التهديدات الخارجية لماذا؟

التهديدات الخارجية

- يمكن للتهديدات الخارجية من الهواة أو المهاجمين المهرة استغلال نقاط الضعف في الأجهزة المتصلة بالشبكة ، أو استخدام الهندسة الاجتماعية ، مثل الخداع ، للوصول.
- الهجمات الخارجية تستغل نقاط الضعف أو الثغرات الامنية للوصول إلى الموارد الداخلية.

البيانات التقليدية

- تتضمن بيانات الشركة معلومات الموظفين والملكية الفكرية والبيانات المالية.
- معلومات الموظفين

تتضمن مواد التطبيق ، كشوف المرتبات ، خطابات العرض ، اتفاقيات الموظفين ، وأي معلومات تستخدم في اتخاذ قرارات التوظيف.

- الملكية الفكرية

مثل براءات الاختراع والعلامات التجارية وخطط المنتجات الجديدة ، للشركة الحصول على ميزة اقتصادية على منافسيها. النظرفي هذه الملكية الفكرية باعتبارها سرًا تجاريًا ؛ يمكن أن يكون فقدان هذه المعلومات كارثية على مستقبل الشركة.

- البيانات المالية

مثل بيانات الدخل والميز انية العمومية وبيانات التدفق النقدي ، تعطي نظرة ثاقبة على صحة الشركة.

الثغرات الأمنية في الأجهزة المحمولة

- في الماضي ، كان الموظفون يستخدمون عادة أجهزة الكمبيوتر التي تصدرها الشركة والمتصلة بشبكة محلية خاصة بالشركة.
- اليوم ، أصبحت الأجهزة المحمولة مثل أجهزة iPhone ، والهواتف الذكية ، والأجهزة اللوحية ، والآلاف من الأجهزة الأخرى.
- أصبح إحضار الجهاز الخاص بك اتجاه متزايد لدى الشركات والمؤسسات..

ظهور أنترنت الأشياء

- انترنت الأشياء (IoT)هي عبارة عن مجموعة من التقنيات التي تمكن من توصيل مختلف الأجهزة بالإنترنت.
- تمكّن تقنيات إنترنت الأشياء الأشخاص من توصيل مليارات الأجهزة بالإنترنت.
- تؤثر هذه التكنولوجيا على كمية البيانات التي تحتاج إلى حماية.

البيانات الكبيرة Big Data

- مع ظهور إنترنت الأشياء ، هناك الكثير من البيانات التي يجب إدارتها وتأمينها.
- أدت إلى نمو هائل للبيانات.
- مجالًا جديدًا يسمى "البيانات الضخمة".

البيانات الكبيرة Big Data

- يجعل تطبيقات معالجة البيانات التقليدية غير كافية.
- تفرض البيانات الضخمة تحديات وفرصًا على أساس ثلاثة أبعاد:
  - حجم أو كمية البيانات
  - سرعة البيانات
  - تنوع البيانات ومصادرها
- هناك العديد من الأمثلة على الاختر اقات الكبيرة للشركات.

التهديد باستخدام الأسلحة المتقدمة

ثغرات البرامج

- تعتمد ثغرات البرامج اليوم على أخطاء البرمجة أو ثغرات البروتوكول أو أخطاء تكوين النظام، والتي تستغل من قبل المجرمين الإنترنت.
- على سبيل المثال: الهجوم شائع يتضمن إنشاء مدخلات لبرنامج معين لتخريبه، مما يتسبب في تعطيله. وفر هذا العطل مدخلًا إلى البرنامج أو يتسبب في تسرب المعلومات.

التهديد المستمر المتقدم APT

- هو اختراق كمبيوتر مستمر يحدث تحت الرادار ضد كائن محدد.
- عادة ما يختار المجرمون APT للعمل أو الدوافع السياسية.
- يحدث APT على مدى فترة طويلة مع درجة عالية من السرية باستخدام برامج ضارة متطورة.

التهديد باستخدام الأسلحة المتقدمة

الهجمات الخوارزمية

- يمكن للهجمات الخوارزميات تتبع بيانات نظام الإبلاغ الذاتي .
- يمكن للهجمات الخوارزمية أيضًا تعطيل جهاز الكمبيوتر.
- تعتبر هجمات الخوارزميات أكثر انحرافًا.

هجمات الاختيار الذكي للضحايا

- في الماضي ، كانت الهجمات تختار الضحايا الأكثر عرضة للخطر.
- سيتم إطلاق العديد من الهجمات الأكثر تطوراً فقط.

النطاق الواسع وتأثير المتتالي

إدارة الهوية الموحدة

- تشير إلى العديد من المؤسسات التي تتيح لمستخدميها استخدام نفس بيانات اعتماد التعريف للوصول إلى شبكات جميع المؤسسات في المجموعة.
- هذا يوسع نطاق ويزيد من احتمال وجود تأثير متتالي في حالة حدوث هجوم.
- تربط الهوية المتحدة الهوية الإلكترونية للموضوع (موقع - برنامج) عبر أنظمة منفصلة لإدارة الهوية. على سبيل المثال ، قد يكون بإمكان موضوع ما تسجيل الدخول إلى Yahoo! باستخدام بيانات اعتماد Google أو Facebook. هذا مثال على تسجيل الدخول الاجتماعي.
- الهدف من إدارة الهوية المتحدة هو مشاركة معلومات الهوية تلقائيًا عبر حدود واسعة، يعني هذا تسجيل دخول واحد إلى الويب.
- من الضروري أن تقوم المنظمات بفحص معلومات التعريف المشتركة مع الشركاء. قد تسمح أرقام التأمين الاجتماعي والأسماء والعناوين لصوص الهوية بفرصة لسرقة هذه المعلومات لارتكاب عمليات احتيال.
- الطريقة الأكثر شيوعًا لحماية الهوية المتحدة هي ربط إمكانية تسجيل الدخول بجهاز معتمد.

تداعيات السلامة

هجوم رفض الخدمة الهاتفية(TDoS)

- يستخدم هجوم رفض الخدمة الهاتفية (TDoS) المكالمات الهاتفية ضد شبكة الهاتف المستهدفة التي تقيد النظام وتمنع المكالمات المشروعة من الوصول.
- مراكز الاتصال لطلب المساعدة معرضة للخطر لأنها تستخدم أنظمة Voice-over-IP (VoIP) بدلاً من الخطوط الأرضية التقليدية بالإضافة إلى هجمات TDoS، قد تتعرض مراكز الاتصال هذه أيضًا لخطر هجمات رفض الخدمة الموزعة (DDoS)التي تستخدم العديد من الأنظمة لإغراق موارد الهدف مما يجعل الهدف غير متاح للمستخدمين الشرعيين.

المعهد الوطني للمعايير والتقنيات (NIST)

- في الولايات المتحدة .
- يمكّن الإطار الشركات من تحديد الأنواع الرئيسية من المسؤوليات وألقاب الوظائف ومهارات القوى العاملة اللازمة.
- هذا الإطار يصنف ويصف أعمال الأمن السيبراني.
- يساعد الإطار في تحديد المتطلبات المهنية في مجال الأمن السيبراني.

الجلسة التدريبية الثالثة

إطار القوى العاملة للأمن السيبراني

يصنف إطار القوى العاملة أعمال الأمن السيبراني إلى سبع فئات:

التحليل

- يتضمن إجراء مراجعة وتقييم متخصصين للغاية لمعلومات الأمن السيبراني الواردة لتحديد ما إذا كانت مفيدة للذكاء أم لا.

الرقابة والتطوير

- توفر القيادة والإدارة والتوجيه لإجراء أعمال الأمن السيبراني بفعالية.

التوفير الآمن

- يشتمل التوفير الآمن على تصميم أنظمة تكنولوجيا المعلومات الآمنة وتصميمها وبناءها.

إطار القوى العاملة للأمن السيبراني

يصنف إطار القوى العاملة أعمال الأمن السيبراني إلى سبع فئات:

التشغيل والصيانة

- يشمل توفير الدعم والإدارة والصيانة اللازمة لضمان أداء نظام تكنولوجيا المعلومات والأمن.

الحماية والدفاع

- تتضمن تحديد وتحليل وتخفيف التهديدات التي تتعرض لها الأنظمة والشبكات الداخلية.

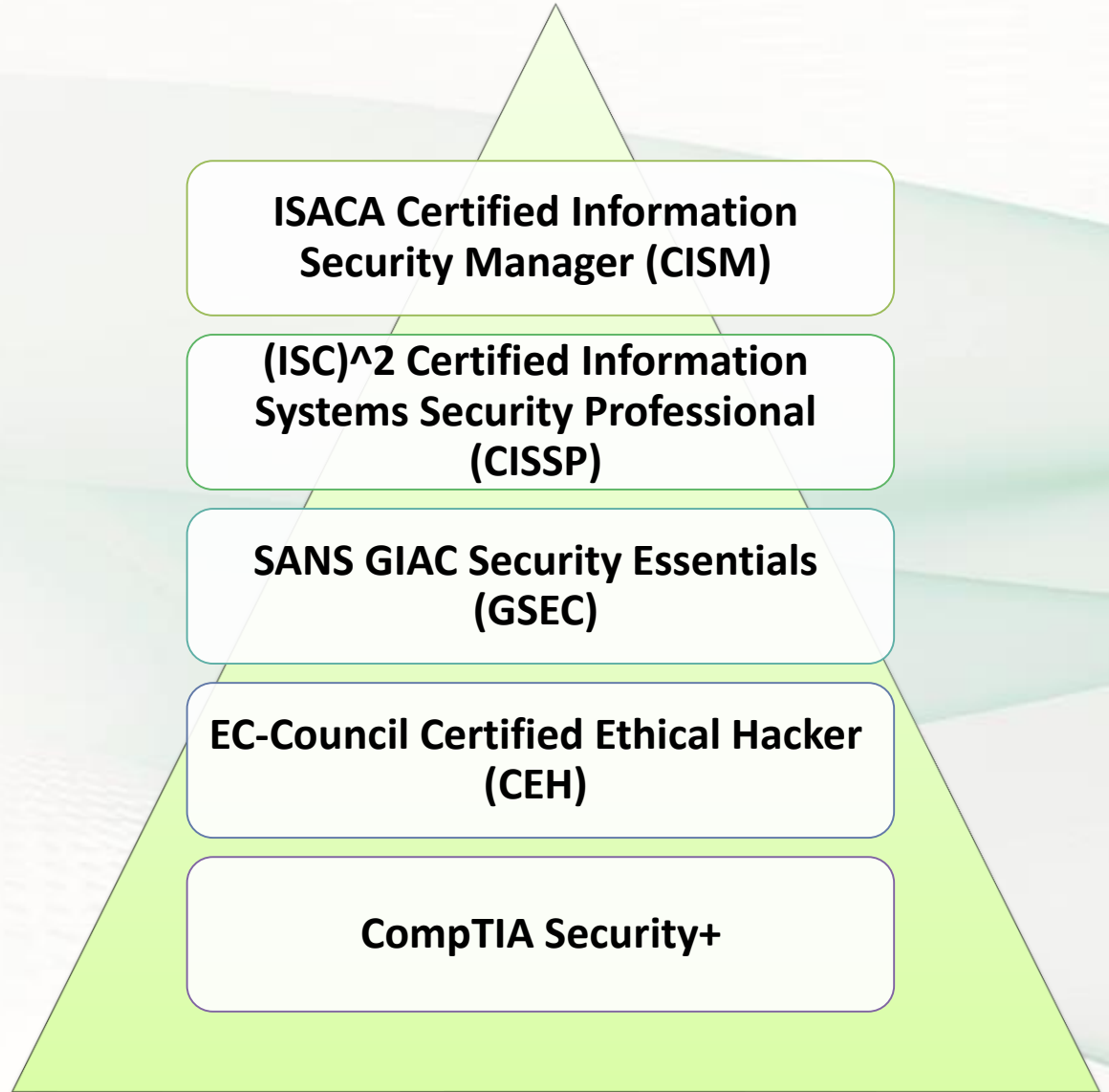
التحقيق

- يتضمن التحقيق في الأحداث السيبرانية و/ أو الجرائم الإلكترونية التي تنطوي على موارد تكنولوجيا المعلومات.

الجمع والتشغيل

- يشمل الجمع والتشغيل عمليات إنكاروخداع متخصصة وجمع معلومات حول الأمن السيبراني.

شهادات الأمن السيبراني



شهادات الأمن السيبراني

CompTIA Security+

- استراتيجيات الهجوم الشبكة والدفاعات
- عناصر السياسات الأمنية الفعالة
- أفضل ممارسات الأمان المستندة إلى الشبكة والمضيف
- استمرارية العمل والتعافي من الكوارث
- معايير التشفير والمنتجات

Certified Ethical Hacker (CEH)

- تقنيات القرصنة التي تستهدف تكنولوجيا الحوسبة السحابية ، والمنصات النقالة وأحدث أنظمة التشغيل
- تغطية لأحدث نقاط الضعف والبرامج الضارة والفيروسات
- قوانين ومعايير أمن المعلومات

Certified Information System Security Professional (CISSP)

- صلاحية التحكم صلاحية الدخول
- التشفير
- الاتصالات السلكية و اللاسلكية
- الشبكات

Certified Cloud Security Professional (CCSP)

- هندسة الحوسبة السحابية ومفاهيم التصميم
- أمن البيانات السحابية
- أمن البيئة السحابية والبنية التحتية
- عمليات الحوسبة السحابية
- القانونية والامتثال

Cisco Certified Network Associate (CCNA) Security

- التعرف على التهديدات ونقاط الضعف في شبكات سيسكو
- تخفيف التهديدات الأمنية
- تطوير البنية التحتية الأمنية الفعالة

شهادات الأمن السيبراني

CompTIA Security+

Security + هو برنامج اختبار برعاية كومبتيا يشهد على كفاءة مسؤولي تقنية المعلومات في ضمان المعلومات.

EC-Council Certified Ethical Hacker (CEH)

تؤكد هذه الشهادة المتوسطة المستوى أن متخصصي الأمن السيبراني الحاصلين على هذا الاعتماد يمتلكون المهارات والمعرفة لمختلف ممارسات القرصنة.

شهادات الأمن السيبراني

SANS GIAC Security Essentials (GSEC)

تعد شهادة GSECاختيارًا جيدًا للحصول على بيانات اعتماد للمبتدئين لمتخصصي الأمن السيبر اني .

يقدم برنامج SANS GIACعددًا من الشهادات الإضافية في مجالات إدارة الأمن والطب الشرعي والتدقيق.

(ISC)^2 Certified Information Systems Security Professional (CISSP)

شهادة CISSP هي شهادة محايدة للبائعين لمتخصصي الأمن السيبر اني ذوي الخبرة التقنية والإدارية.

شهادات الأمن السيبراني

ISACA Certified Information Security Manager (CISM)

يمكن أن يتأهل أبطال الإنترنت المسؤولون عن إدارة أنظمة أمان المعلومات وتطويرها والإشراف عليها على مستوى المؤسسة أو عن أولئك الذين يطورون أفضل ممارسات الأمان إلى CISM.

يمتلك حاملو الاعتماد مهارات متقدمة في إدارة المخاطر الأمنية.

شهادات الأمن السيبراني

Company-sponsored certifications

تقيس هذه الشهادات المعرفة والكفاءة في تثبيت منتجات البائع وتكوينها وصيانتها. تعد Ciscoو Microsoftمثالين للشركات التي حصلت على شهادات تختبر معرفة منتجاتها.

Cisco Certified Network Associate Security (CCNA Security)

تقوم شهادة CCNA Security بالتحقق من صحة أن أخصائي الأمن السيبر اني لديه المعرفة والمهارات اللازمة لتأمين شبكات سيسكو

كيف تصبح خبير في الأمن السيبراني

الدراسة: تعلم الأساسيات من خلال استكمال الدورات في مجال تكنولوجيا المعلومات.

الحصول على الشهادات: الشهادات للبحث عن عمل كمتخصص في الأمن السيبراني.

متابعة التدريب: البحث عن تدريب أمني كطالب.

الانضمام إلى المنظمات الاحترافية: الانضمام إلى مؤسسات أمان الكمبيوتر.

هل جهازي مخترق؟

تثبيت برامج جديدة

يعد تثبيت برامج جديدة على الجهازمن العلامات التي تدلّ على أنّ الجهاز مخترق (مهكر).

تواجد حسابات مُستخدمين غير معروفة

يتم التحقق من ذلك من خلال التوجّه إلى لوحدة التحكم لفتح القائمة ثم الضغط على خيارحسابات المستخدمين (بالإنجليزية:user accounts)، أومن 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.

Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

بعض العلامات التي تدل على اختراق الجهاز، ومنها:

١. إلغاء تثبيت أو تعطيل برامج مكافحة الفيروسات.

٢. إجراء الجهاز عدّة نشاطات من تلقاء نفسه.

٣. تغيير كلمة مرور الجهاز.

٤. زيادة نشاط الشبكة

تثبيت التحديثات
الجديدة على الجهاز

عزل الجهاز

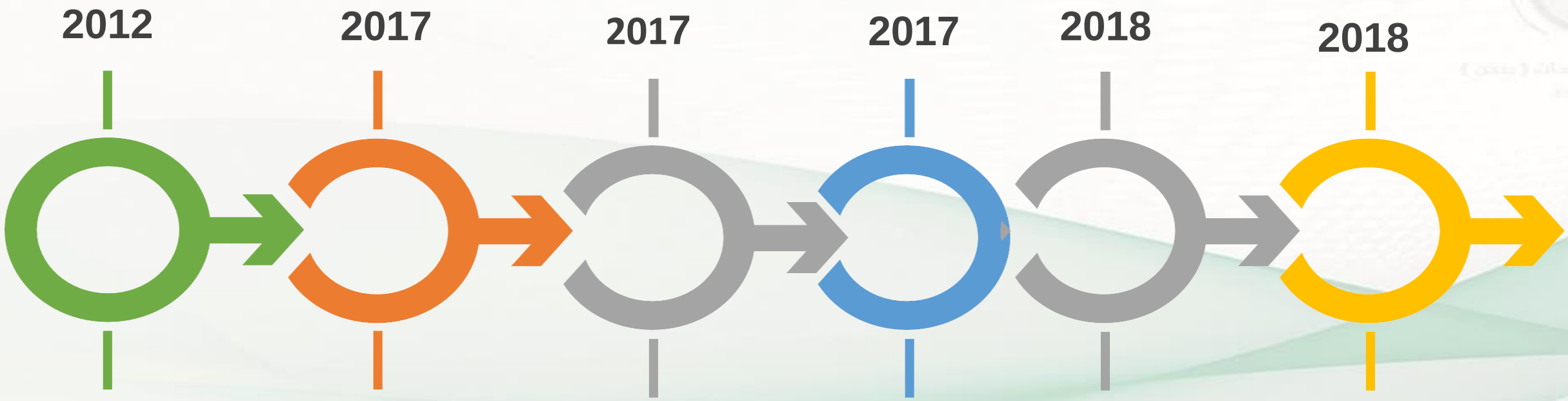
نسخ الملفات المهمّة

إزالة القرص الصلب

إعادة تحميل نظام التشغيل
من الوسائط الموثوق فيها

استخدام برامج
لمكافحة التجسس

المملكة العربية السعودية سيبرانياً


2012
فيروس "شمعون" الذي استخدم في الهجوم على قطاع الطاقة السعودي وكان من ضحايا الفيروس شركة ارامكو السعودية.
2017
تم شن هجوم الكتروني على نظام الامان التابع لشركة ارامكو
2017
فيروس الفدية يصيب الأنظمة التابعة لبعض الجهات الحكومية مما ادى الى اضرار كثيرة.
2017
المملكة تَعَرّضت إلى ٥٤ ألف هجوم إلكتروني
2018
تعرض مصنع للبتروكيماويات لنوع جديد من الهجمات الإلكترونية
2018
احتلت المملكة الاولى عربيا و ١٧ عالميا في عدد الهجمات السيبرانية الموجهة لها

جهود المملكة العربية السعودية في الأمن السيبراني

- تم تشكيل الهيئة الوطنية للأمن السيبراني في 31 , October 2017 لرفع مستوى الحماية للشبكات والاجهزة والأنظمة المعلوماتية وما تحويه من بيانات

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

جهود المملكة العربية السعودية في الأمن السيبراني

- تم إنشاء الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز

جهود المملكة العربية السعودية في الأمن السيبراني

- تم إنشاء مركز الأمن الإلكتروني لمواجهة التهديدات الالكترونية الموجهة على المملكة العربية السعودية

NCSC
مركز الأمن الإلكتروني
المملكة العربية السعودية

جهود المملكة العربية السعودية في الأمن السيبراني

- إنشاء كلية متخصصة بالأمن السيبراني والبرمجة والذكاء الاصطناعي
- وزارة التعليم والهيئة الوطنية للأمن السيبراني قامت بتخصيص ١٠٠٠ مقعد للمستفيدين و المستفيدات من برنامج خادم الحرمين الشريفين للإبتعاث الخارجي في مجال الأمن السيبراني
- العديد من الجامعات السعودية تضمن مجالي الذكاء الاصطناعي والأمن السيبراني في خططها
- وضع الاستراتيجية الوطنية للأمن السيبراني الجديدة من قبل الهيئة الوطنية للأمن السيبراني

جهود المملكة العربية السعودية في الأمن السيبراني
(المجموعات والجمعيات غير الربحية)

جمعية أمن المعلومات -حماية- جمعية أهلية رسمية مسجلة لدى وزارة الموارد البشرية والتنمية الاجتماعية

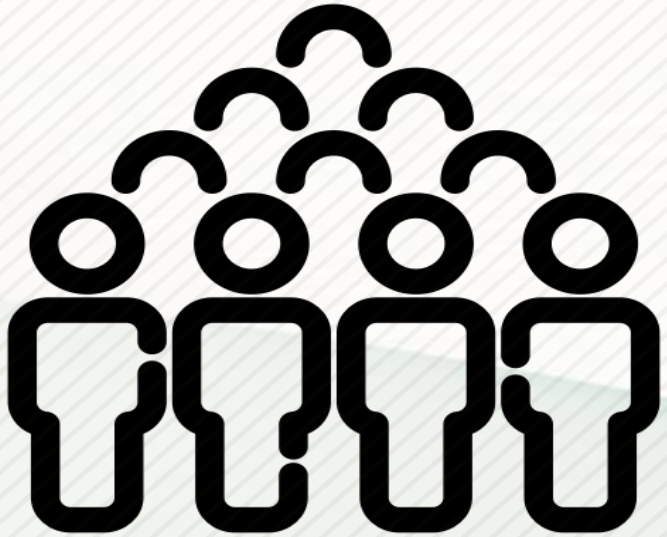
تتطلع سياج للريادة في مجال أمن المعلومات ولأن تكون مرجعًا لبناء المهارات في الوطن العربي.

جمعية تطوعية معتمدة (١٥٥٧) غير ربحية مخصصة لتقديم النصائح والإرشادات لحماية الأطفال في الفضاء السيبراني
Cybersecurity for Children Association

مجموعة صقر للأمن السيبراني

نفتخر إن مملكتنا الغالية الأولى عربياً و ١٣ عالمياً في مؤشر الأمم المتحدة للأمن السيبراني من بين ١٧٥ دولة حسب التقرير الصادر في يوم الخميس ٢١ رجب ١٤٤٠هـ


لنا جنـود في الأرض
وجنـود على الفضـاء السيـبراني
الاتحـاد السعـودي للأمـن السيبـراني والبرمجة والدرونـز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES
منصـة مكافآت الثغرات
BugBounty.sa
الشريك والممكن الرقمي
stc
/SAFCSP • SAFCSP.ORG.SA



كُلنا مسؤول

ملخص اليوم التدريبي الثالث

شكر وتقدير