يرحب بكم التحول الرقمي

استراتيجيات حماية المنظمات من التهديدات السيبرانية

الاتفاقيات

تأقلمك مع المدرب وتنفيذ التمارين يسهل استيعاب المادة العلمية

لاتدع هاتفك المتنقل يشوش أفكار من حولك

الأسئلة والنقاش متاحة في محتوى البرنامج

الإلتزام بوقت البرنامج دليل وعيك

إعداد

أ.د/ فهد بن مزيد العضياني

الرئيس التنفيذي للمكتب الاستشاري كفاءة للإبداع وذكاء الأعمال بالجامعة

مستشار المسؤولية الاجتماعية بالإدارة العامة لخدمة المجتمع والمسؤولية الاجتماعية

أستاذ بكلية الحاسبات وتقنية المعلومات جامعة الملك عبدالعزيز- الفرع الرئيسي

k

عضو هيئه تدريس بقسم نظم المعلومات في الذكاء الاصطناعي وباحث وخبير بالامن السيبراني والجرائم المعلوماتية

مدرب معتمد في التنمية البشرية من مركز اعداد القادة بوزارة التعليم العالي.
درب اكثر من 15388ساعة تدريبية تقنية ادارية ودورات تدريب المدربين
خرج 2053مدرب ومدربة 19عام خبرة

مدرب متعمد من جامعة الملك عبد العزيز ورابطة المدربين العرب الدولية و البورد الكندي للتدريب في الموارد البشرية

مصمم ومقيم حقائب تدريبية تقنية إدارية
مؤلف كتابين تدريب المدربين وعش حياتك بلا قلق

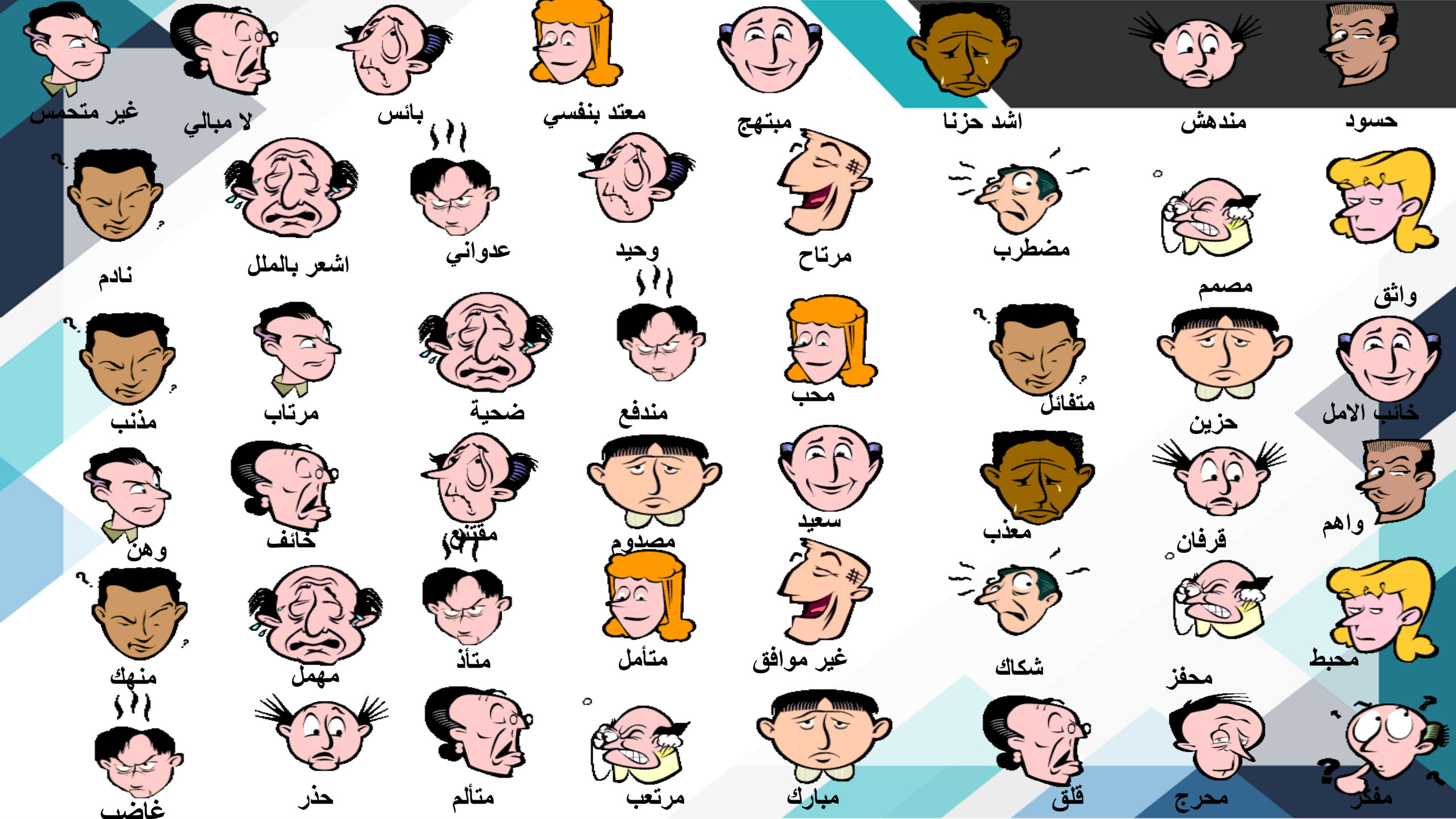
fmmalodayani@
Dr.fahad35
Dr.fahad2014
F_ff111@hotmail.com

.. الجلسة التدريبية..

المحتويات

الهدف العام

القدرة على معرفة اساسيات استراتيجيات الأمن السيبراني وخصوصية البيانات والتعرف على كيفية أمن الاجهزة الحاسوبية بالمنظمات.


حسود
مندهش
اشد حزنا
مبتهج
معتد بنفسي
بائس
لا مبالي
غير متحمس
واثق
مصمم
مضطرب
مرتاح
وحيد
عدواني
اشعر بالملل
نادم
خائب الامل
حزين
متفائل
محب
مندفع
ضحية
مرتاب
مذنب
واهم
قرفان
معذب
سعيد
مصدوم
مقتنع
خائف
وهن
محبط
محفز
شكاك
غير موافق
متأمل
متأذ
مهمل
منهك
مفكر
محرج
قلق
مبارك
مرتعب
متألم
حذر
غاضب

الاختبار القبلي

يقيس معلومات ومهارات المتدرب حول موضوع الدورة

	الأسئلة (اجب بصح او خطا)	الدرجة	الاجابة
1	أمن المعلومات هو حماية المعلومات والبيانات على شبكات الحاسب فقط؟	3	
2	هل يمكن مراقبة عمليات التصفح في المتصفحات المخفية؟	3	
3	إغلاق GPS في الهواتف المحمولة يمنع من تعقب موقعك ؟	3	
4	إذا كانت شبكة الانترنت في الأماكن العامة مأمنة برقم سري فهي آمنة؟	3	
5	في الغالب كم مرة يطلب البنك منك اعادة تعين كلمة المرور على الايميل ؟	3	
6	ماهو فيروس الفدية؟	3	
7	ماهي ملفات الارتباط؟	3	

مقدمة

تحدث تكنولوجيا المعلومات تحولاً في الأسلوب الذي يفكر به في كل شيء ونفعل به أي شيءفي حياتنا تقريباً فهي تستحدث تغييرات هيكلية مهمة عن طريق السماح لنا بنمذجة الأشياء المحسوسة من جميع الأنواع على شكل معلومات

المعلومات الرقمية

1. تخلق الرقمنة صورة رقمية لشئ حقيقي (نسخة تقديرية من الشئ المحسوس)
2. يمكن لكل المعلومات مهما كانت طبيعتها-سواء كانت صوت او بيانات او صورة ان ترقمن وان تقدم بصورة موحدة
3. تضيف المعلومات في حد ذاتها (المحتوى) بشكل الكتروني تعتبر رقمنة قيمة
4. حقيقة المعلومات ناتجة من بيانات ثم تتحول المعلومات الى معرفة يستفاد منها.

الأمن السيبراني

ماذا تعني كلمة سيبراني Cyber

السيبرانية ..

كلمه (سايبر) وتعني صفة لأي شيء مرتبط بالحواسيب والشبكات الالكترونية

وكل ما يتعلق بالويب في الشبكة العنكبوتية وملحقاتها من الأجهزة الأخرى

فالسيبرانية تعني فضاء المعلومات أو الفضاء السيبراني وهو مصطلح وكلمة يونانية الأصل .

تهديدات الأمن السيبراني للمعلومات

تقول احصائية امريكية لباحثين 2022 سوف يكون هناك 20بليون جهاز متصل بالإنترنت حول العالم عبر شبكات مختلفة وسيرفرات لنقل المعلومات وضخامة معلومات كثيرة تؤثر على الشبكات وهناك هاجس الأمن وكيف تؤمنه؟

يجب أن تتوفر حلول جذرية :

- لحماية الاتصالات.
- والمعلومات والشبكات .

مواقع التواصل
إحصاءات وأرقام

المستخدمون النشطون شهريا

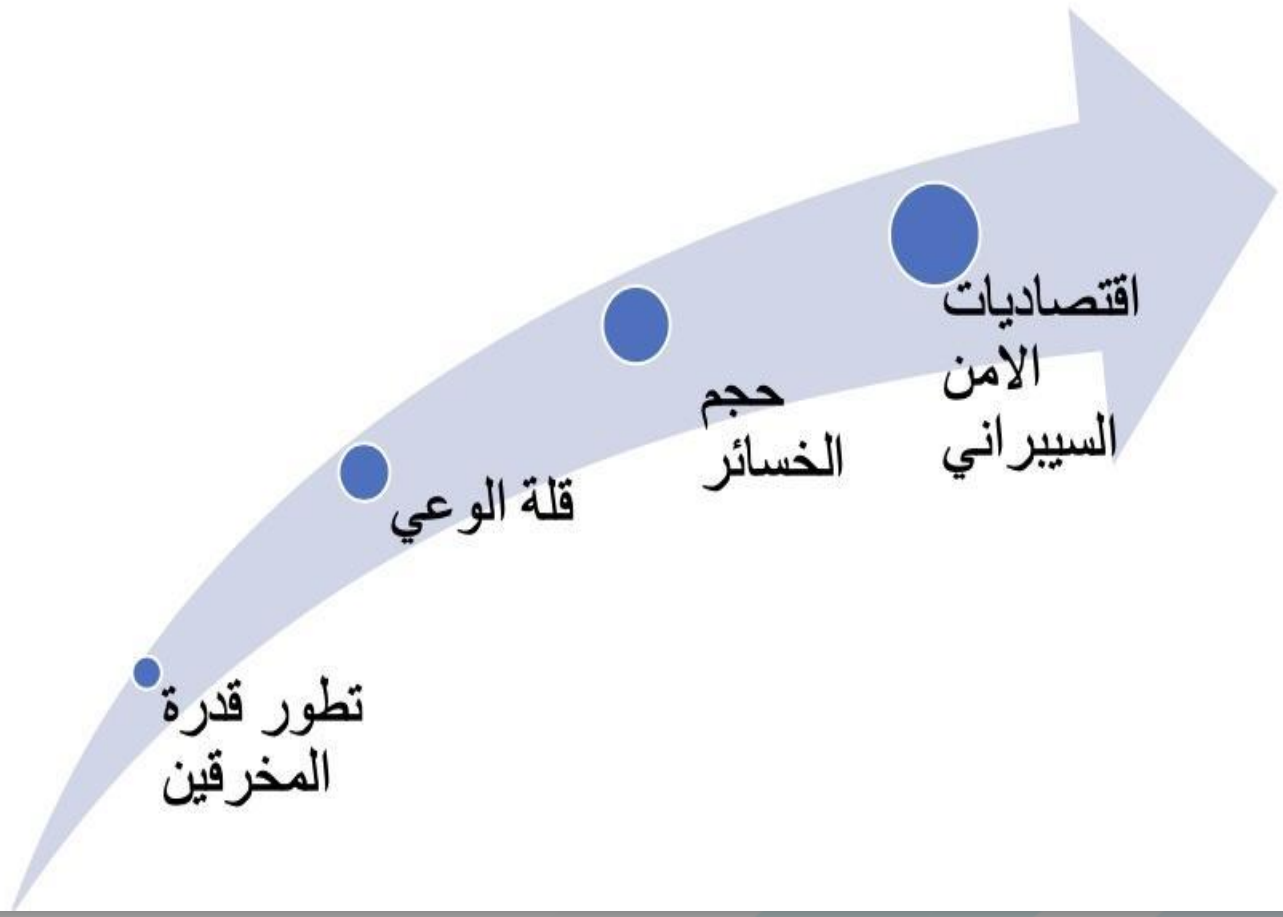
FACEBOOK	1.6	مليار
YOUTUBE	1	مليار
WHATSAPP	950	مليون
GOOGLE +	440	مليون
INSTAGRAM	430	مليون
LINKEDIN	420	مليون
TWITTER	325	مليون
TUMBLR	230	مليون
PINTEREST	110	مليون

تعريفات للأمن السيبراني

- الامن السيبراني، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، ، حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2018" ، هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية، وتوعية لإدارة المخاطر وممارسات للحماية، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

- الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

استراتيجيات حماية المنظمات



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

يستخدم %87 من البشر المُتصلون بالإنترنت شبكات التواصل

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

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

نسبة %72 من الاختراقات الإلكترونية ناجمة من الاخطاء البشرية

أهم تلك التحديات والأخطار السيبرانية هي

خطر اختراق وتخريب البني التحتية للاتصالات وتكنولوجيا المعلومات ظهرت أنماطاً جديدة خطيرة للغاية من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية

كذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية وخاصة في المرافق الهامة

ذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة بالإضافة الي القنوات الأخرى الشائعة البريد الالكتروني ومواقع الانترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية

1 خطر الارهاب والحرب السيبرانية

- انتشرت مؤخرا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد علي تقنيات متقدمة كالحوسبة السحابية والذكاء الاصطناعي وانترنت الاشياء وأجهزة تنصت علي شبكات الاتصال السلكية واللاسلكية وبرمجيات لفك شفرة ولاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات

1 خطر الارهاب والحرب السيبرانية

- برمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات اجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمي بالشبكات الآلية

2 خطر سرقة الهوية الرقمية والبيانات الخاصة

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الانترنت ومستقبل الخدمات الالكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو الزج باسمه في تعاملات مشبوهة أو غير قانونية

2 خطر سرقة الهوية الرقمية والبيانات الخاصة

عادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل على الانترنت وبخاصة على مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعي وشبكات الرعاية الصحية

ركائز التوجه الاستراتيجي لمواجهة الأخطار السيبرانية

يمكن تحديد أهم ركائز الاستعداد لمواجهة الأخطار السيبرانية فيما يلي:

- **الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي**

ويشمل ذلك الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية مع الاهتمام بالاستعداد المسبق

- **الاطار التشريعي**

وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات

- **الإطار التنظيمي والتنفيذي**

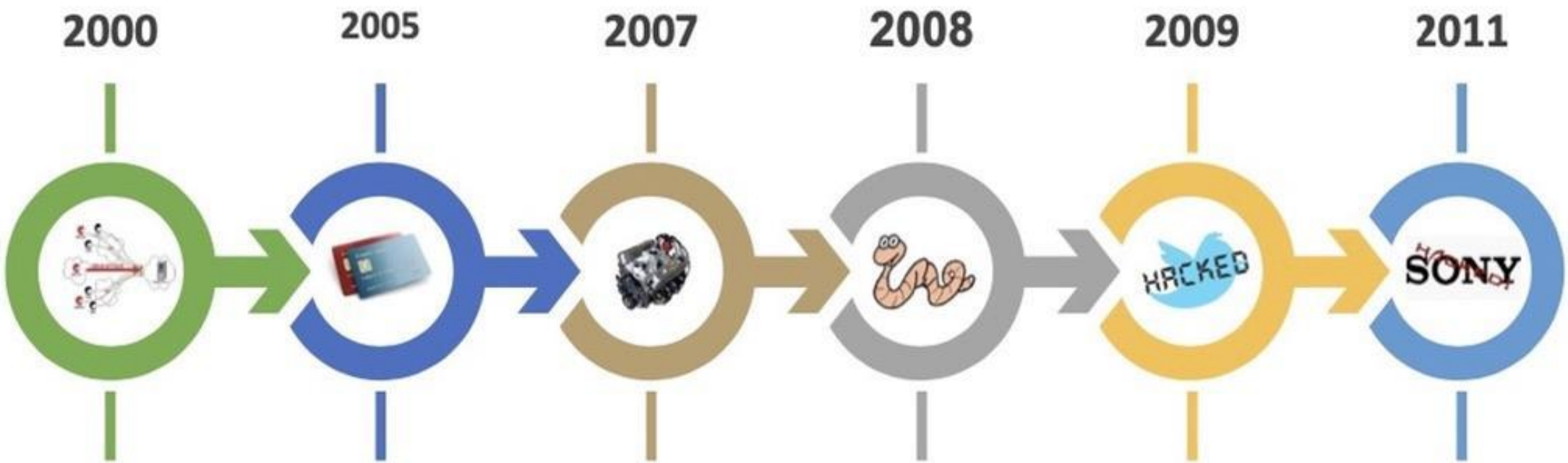
وضع الإطار التنظيمي وانشاء منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الانترنت

- **البحث العلمي و تنمية صناع الأمن السيبراني**

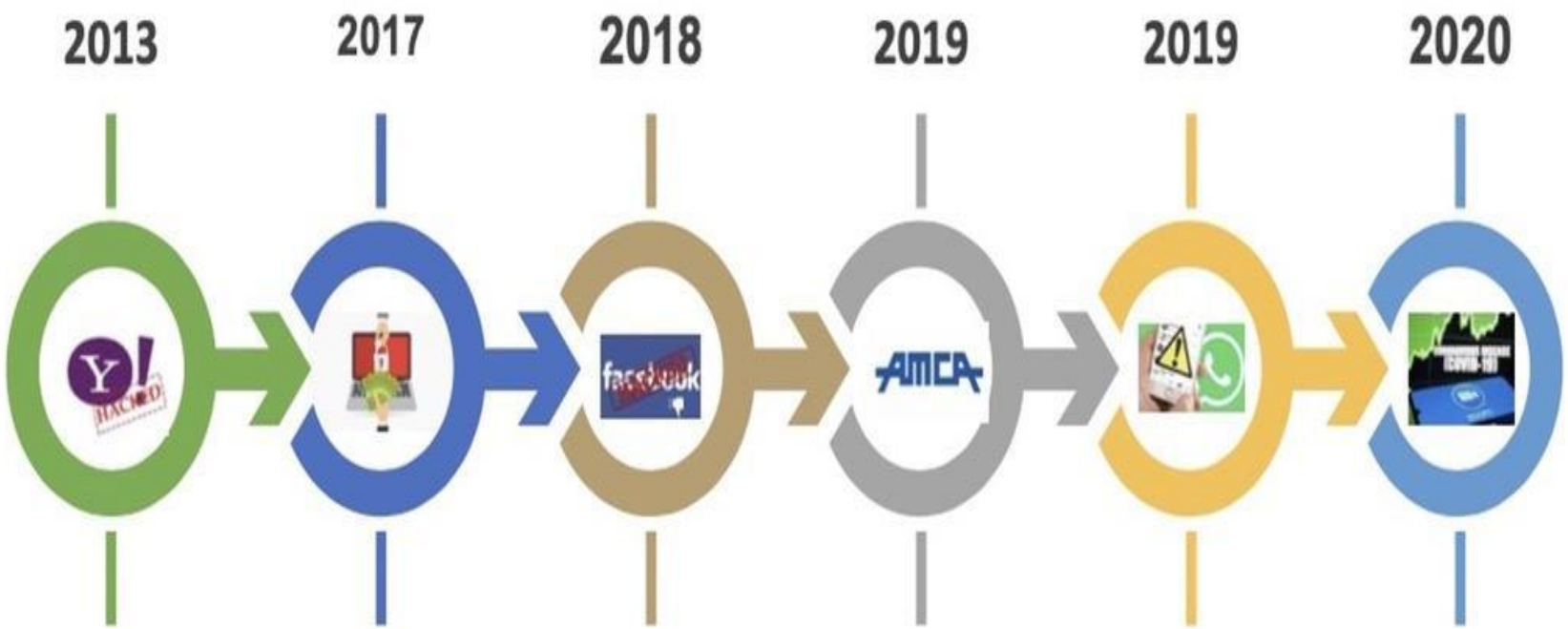
تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية، خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة، ومجال تحليل الأدلة ا

نظرة تاريخية
لأبرز الهجمات السيبرانية

نظرة تاريخية



نظرة تاريخية




فضاءات الأمن السيبراني والتهديدات

فضاءات الامن السيبراني

تهديدات سيبرانية

التهديد	الوسائل	النتيجة
التخريب	البرمجيات الخبيثة الاختراق اغراق الخادم بالطلبات	تعطل الخدمات تخريب الأجهزة تدمير البنية التحتية
سرقة البيانات واستغلال الحسابات الشخصية	الاختراق الهندسة الاجتماعية التصيد الإلكتروني	- الحصول على مُستندات، صور أو ملفات هامة - سرقة الأموال والحسابات - سرقة الهوية بهدف الحصول على قروض بنكية أو إتمام معاملات مالية بإسم الضحية - سرقة عناوين، أرقام تليفون، وعناوين البريد الإلكتروني الخاصة بالأصدقاء والمعارف بهدف إستهدافهم بحملات إعلانية
التجسس	البرمجيات الخبيثة الاختراق	السيطرة الكاملة على الأجهزة، حتى إنها تسمح للمخترقين بالاطلاع على كافة محتويات الهاتف والتجسس على المستخدمين دون علمهم.

أنواع البرمجيات الخبيثة والفيروسات

البرامج الخبيثة :

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

و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.

و يمكن يتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

1. الفيروسات (Viruses)
2. الديدان (Worms)
3. برامج التجسس (Spywares)
4. أحصنة طروادة Trojan Horses

الفيروسات Viruses:

- فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف 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.

: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

كيف تصاب بالفيروسات

مشاركة الملفات أو الصور مع مستخدمين آخرين

فتح البريد الإلكتروني العشوائي أو مرفق البريد الإلكتروني

تثبيت تطبيقات البرمجيات السائدة دون قراءة اتفاقيات الترخيص بدقة

زيارة موقع مصاب

تنزيل الألعاب وأشرطة الأدوات ومشغلات الوسائط وأدوات النظام الأخرى مجانًا

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

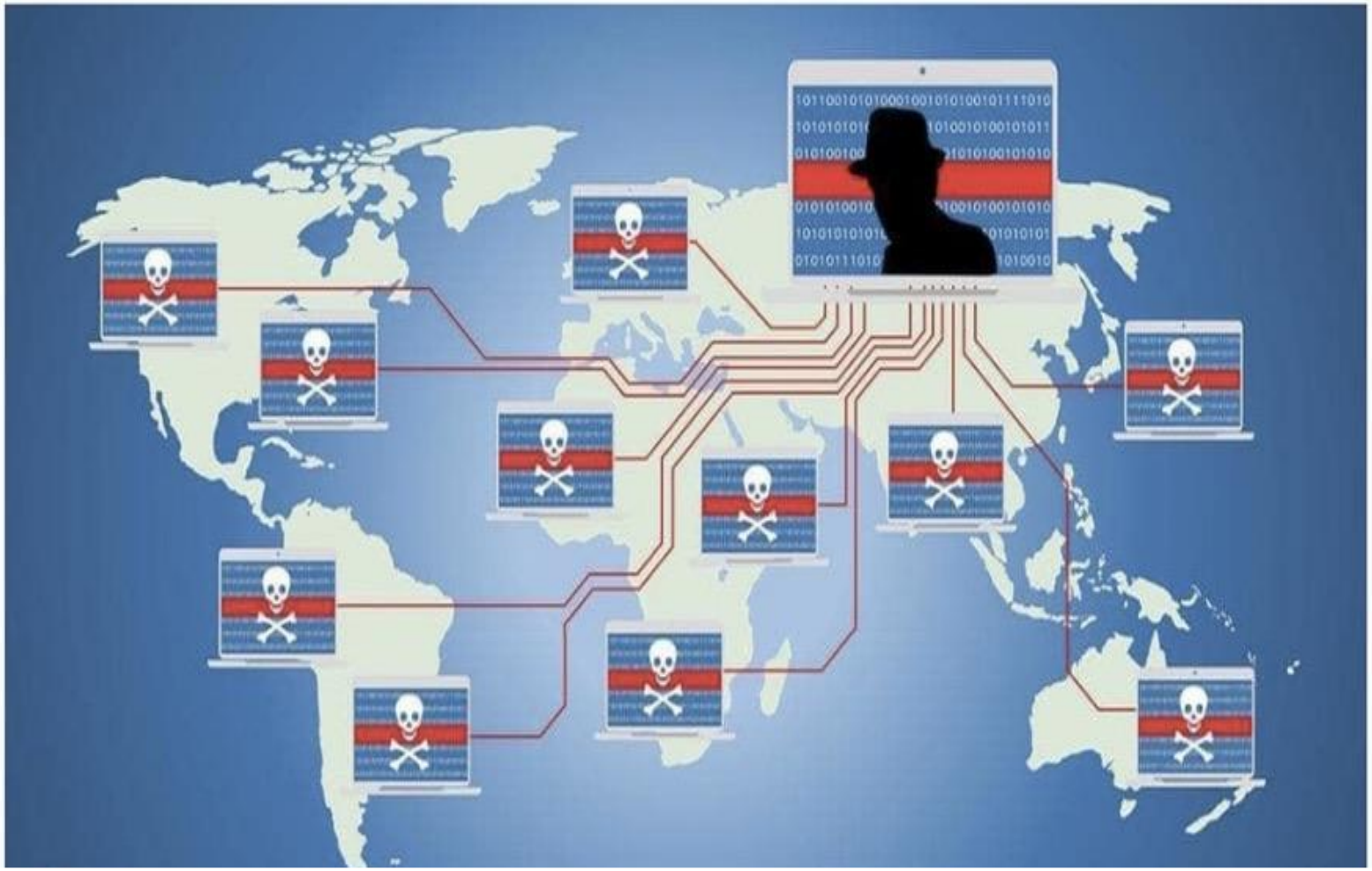
النوافذ المنبثقة على مواقع الويب المشكوك فيها

من خلال التخفي على أنها برامج مفيدة

باستخدام مكافح فيروسات الكمبيوتر غير محدث

أخطر الفيروسات

أخطر الفيروسات



البوت نت Botnet هو مجموعةٌ من أجهزةٍ متصلةٍ 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 مصابةً ويتم التحكم بها عبر نوع من البرامج الخبيثة، وفي حالاتٍ عديدةٍ قد لا يدرك المستخدم أن حاسبه يتعرض لهجومٍ أو إصابة بوت نت

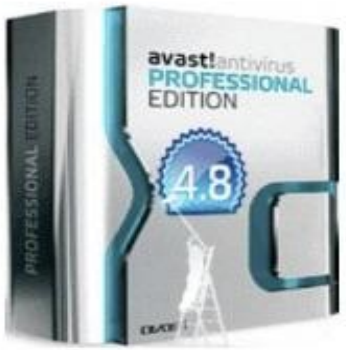
الحماية من التهديدات السيبرانية بالفيروسات

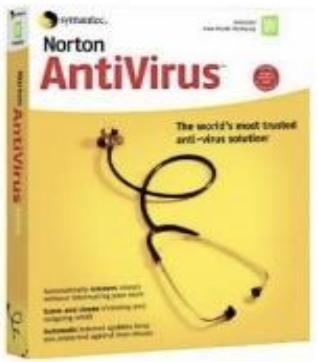
يُنصح المستخدم عادةً بحماية جهازه من الفيروسات ووقايته منها، وذلك باتباع الخطوات التالية:

- عدم تحميل أي برامج دون إجراء فحص لها، وكذلك الأمر بالنسبة للملفات المحملة والمنقولة من الشبكة العنكبوتيّة فيتوجب الفحص قبل التشغيل.
- تحميل البرامج الخاصة للكشف عن وجود الفيروسات ومكافحتها في جهاز الحاسوب.
- الاحتفاظ بنسخ احتياطيّة (Backup) للملفات والبرامج.
- الاعتماد على برامج الجدار الناري التي تقف عائقاً في وجه الفيروسات.
- تنصيب أنظمة تشغيل أكثر أماناً كنظام التشغيل جنو/لينكس.
- عدم تشغيل ملفات وبرامج مجهولة المصدر.
- أخذ الحيطة والحذر من الرسائل التي تصل عبر البريد الإلكتروني والروابط المجهولة المصدر وفحصها قبل فتحها.

مكافحات الفيروسات
:Anti-virus & anti-spyware

- 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

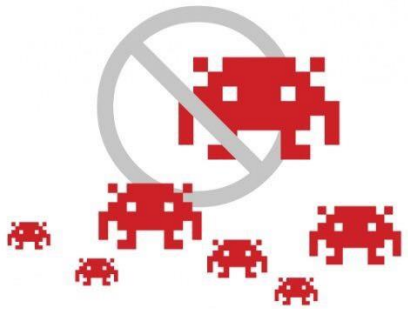




إزالة فيروسات الحاسوب

ينصح المستخدم في حال اكتشافه وجود فيروسات بجهازه اتخاذ الإجراءات التالية:

- تنصيب برامج حماية من الفيروسات (Anti-Virus).
- البدء بعمل Scan لكل الملفات الموجودة.



وكما يمكن ذلك من خلال الاتصال بشبكة الإنترنت والولوج إلى مواقع الإنترنت والقيام بعملية الفحص، وتوفر Microsoft.com ذلك، إذ يتطلب ذلك من المستخدم الوصول إلى صفحة (برنامج مكافحة الفيروسات من Microsoft) على الشبكة العنكبوتيّة، واختيار "Download Now" التنزيل الآن، واتباع التعليمات لحين الانتهاء من التنزيل.

الإبلاغ عن المواقع التي تحمل فيروسات أو الإساءة
(خدمة الترشيح)

هذا التطبيق من إنتاج هيئة الاتصالات وتقنية المعلومات للإبلاغ عن مواقع و المواد التي تتنافى مع الدين الحنيف والأنظمة الوطنية يمكن طلب حجبها من خلال القنوات التالية:

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

تطبيق الترشيح لمواقع النت

خطوات طلب حجب مواقع هادمة من خلال تطبيق ترشيح :

طاقة ايجابية بعد التخويف من الفيروسات

أشهر أقوال الفيلسوف ديكارت :

ليس كافياً أن تمتلك عقلا جيداً، فالمهم أن تستخدمه جيداً

كن حذرا لحماية بياناتك اتبع التعليمات للأمان بدل أن تخسر كل شيء .

التصيد؟

التصيد الإلكتروني هو نوع من أنواع الجرائم الإلكترونية الأكثر انتشارا. يعد التصيد الإلكتروني أحد أساليب الاحتيال عبر الإنترنت وذلك لمحاولة الحصول على معلومات شخصية أو مالية عن طريق رسائل البريد الإلكتروني أو من خلال مواقع الإنترنت.

يقوم المتصيد بإرسال رسالة مزيفة إلي المستخدم

المتصيد

الرسالة المزيفة

المستخدم

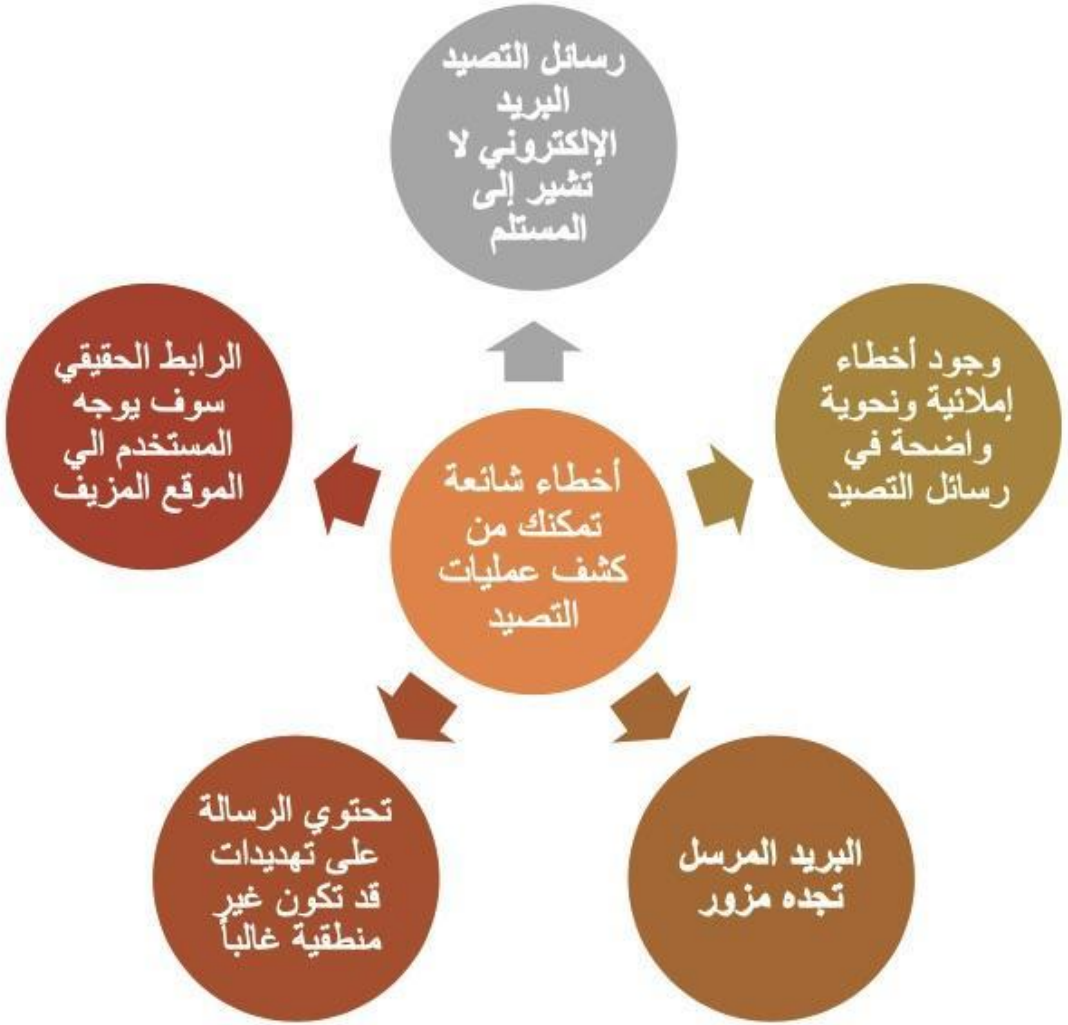
الصفحة المزيفة

يظن المستخدم أنه يقوم بادخال
بيانات الدخول في الصفحة الصحيحة
ولكن يتم تحويله إلي الصفحة المزيفة

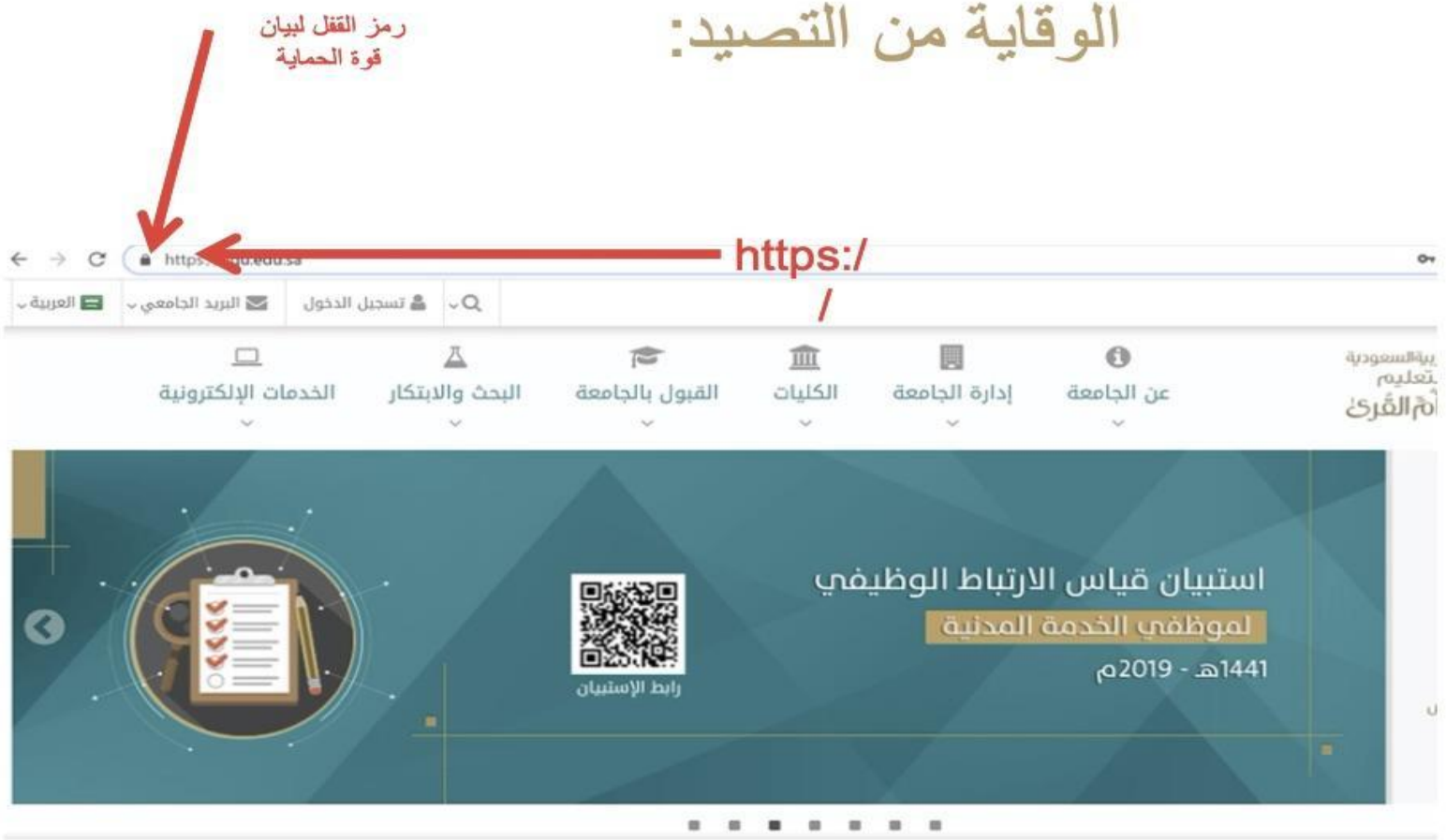
Username
&
Password

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
البريد المرسل تجده مزور
تحتوي الرسالة على تهديدات قد تكون غير منطقية غالباً
الرابط الحقيقي سوف يوجه المستخدم الي الموقع المزيف
أخطاء شائعة تمكنك من كشف عمليات التصيد

الوقاية من التصيد:



https://safeweb.norton.com/

الوقاية من التصيد:

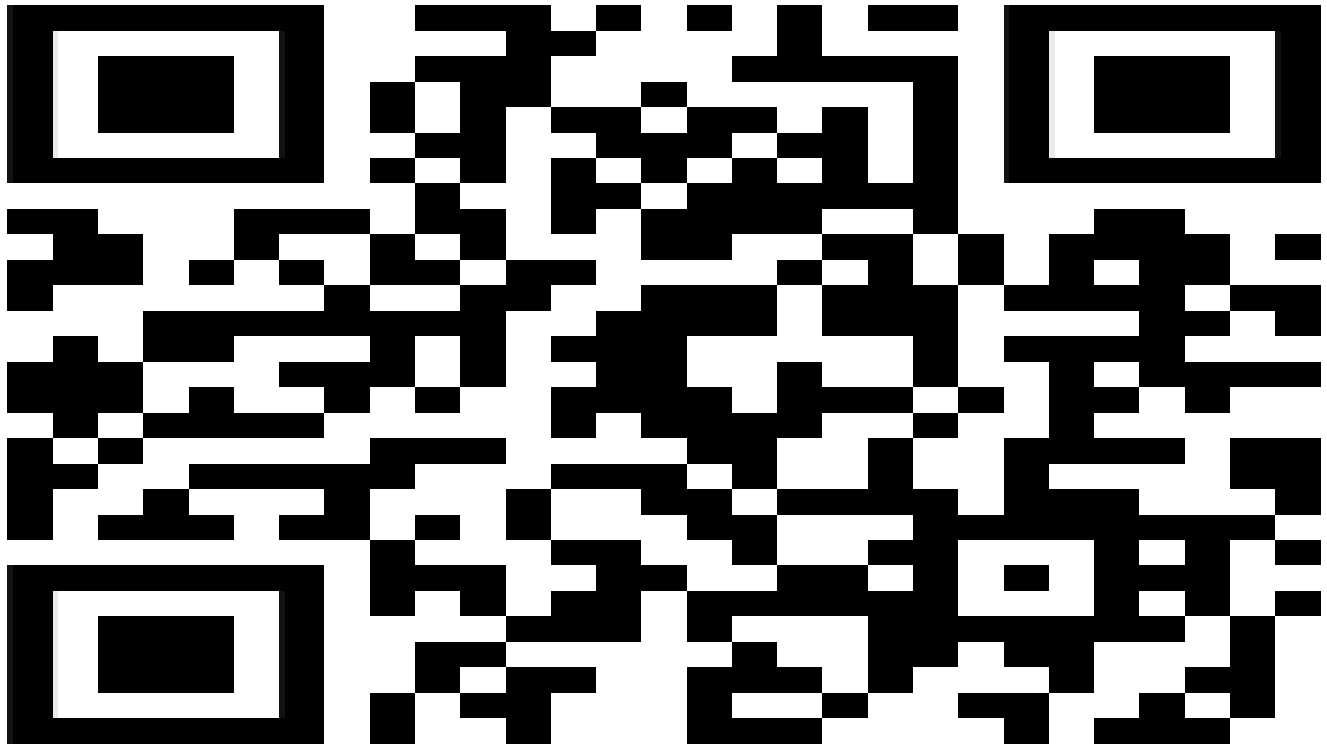
https://forms.gle/PTnBVpepkcUprZJUA


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority
رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA
نحو فضاء سيبراني سعودي آمن وموثوق
13
عالمياً
ترتيب المملكة العربية السعودية عام 2018م
من بين 175 دولة
في المؤشر العالمي للأمن السيبراني
46
ترتيب المملكة العربية السعودية عام 2016م
الأولى عربيًا
@NCA_KSA


G20
OSAK
SUMMIT 20
"يجب أن نعمل
واجهة التحديات السيبرانية
حتى لا تتحول إلى عوائق اقتصادية"
سمو ولي العهد
الأمير محمد بن سلمان بن عبدالعزيز


TRUSTED SECURITY
الثقة الامنية
www.trusted-sec.com
Trusted_Sec
10
شهادات مهنية في
الأمـــن
السيبراني
1
الهاكر الأخلاقي
المعتمد
CEH
2
تحكم في المخاطر
ونظم المعلومات
CRISC
3
دير أمن المعلومات
المعتمد
CISM
4
مدقق نظم
علومات المعتمد
CISA
5
خبير أمن
نظم المعلومات
6
متخصص أمن
وحماية الشبكات
CCNA SECURITY
7
محترف أمن
وحماية الشبكات
CCNP SECURITY
8
محقق جنائي
رقمي معتمد
CHFI
9
محترف أمن الحوسبة
السحابية المعتمد
CCSP
10
شهادة
COMPTIA
العنوان :
10 Hot Cybersecurity Certifications For IT
Professionals To Pursue In 2019

موقع لفحص الروابط



المراجع ..

- الشهري، حسن أحمد . (2011) . قانون دولي موحد لمكافحة الجرائم الإلكترونية. *المجلة العربية للدراسات الامنية والتدريب (السعودية)*، مج27 , ع 53 ، 5 - 54 .
- زيدان , زبيخة . (2011) . *الجريمة المعلوماتية في التشريع الجزائري و الدولي* . الجزائر : دار الهدى .

المومني , نهلا عبدالقادر . (2012) . *الجرائم المعلوماتية* (ط1) . عمان : دار الثقافة .

- جواد، أشرف حسن محمد . (2015) . الجريمة المعلوماتية أوالالكترونية: أنواعها وخصائصها وطرق الوقاية منها. *مجلة الدراسات المالية والمصرفية - المعهد العربي للدراسات المالية والمصرفية - الأردن*، مج23, ع1 ، 29 – 33 .
- الجهني، منصور مصلح . (2010) . الجرائم المعلوماتية أنواعها وصفات مرتكبيها. *المؤتمر الدولي الرابع للعلوم الاجتماعية (العلوم الاجتماعية : حلول عملية لقضايا مجتمعية) - الكويت*، الكويت: كلية العلوم الاجتماعية ، جامعة الكويت، 1 - 8 .

Information Systems Control And Audit (1
.by Ron Weber

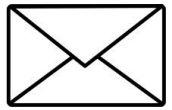
a.com4www.cb (2

www.wikipedia.com (3

د . فهد بن مزيد العضياني

شكراً
لحسن استماعكم

اتشرف بمتابعتكم بحساباتي على مواقع التواصل الاجتماعي
حيث الطاقة الإيجابية والمعلومات التقنية والدورات القيمة بإذن الله



Fmmalotaibi@kau.edu.sa

dr.fahad35

Fmmalodayani@

http://t.me/joinchat/AAAAAFV0nhL8KOTNuwzZRg