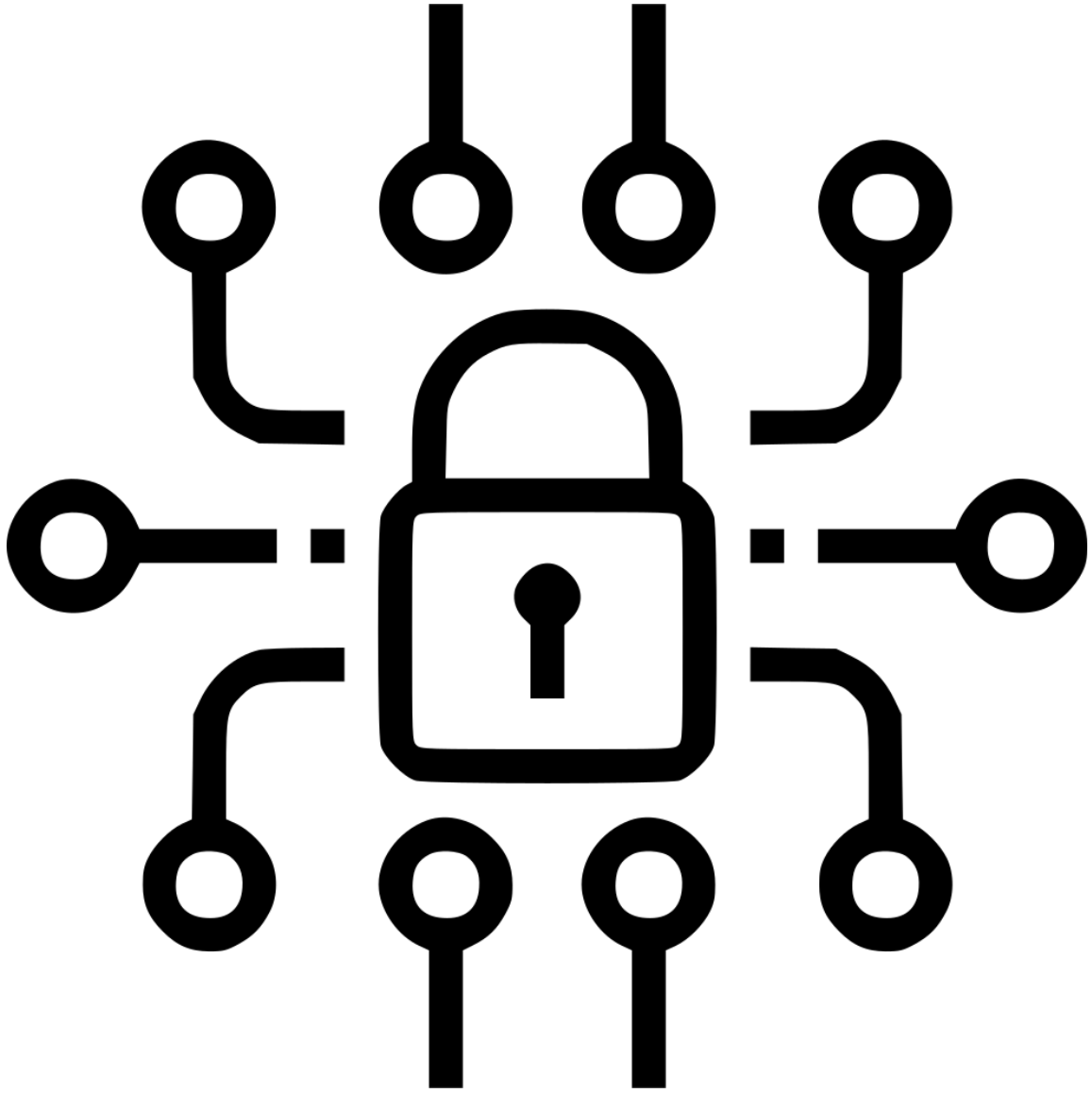


فاصلة منقوطة

أساسيات في الأمن السيبراني

CYBER SECURITY

Presented by: Meaad Alotaibi.

Interduce my self

ميعاد العتيبي

- حاصلة على درجة البكالوريوس في علوم الحاسب.
- اعمل بإدارة الأنظمة بقسم تقنية المعلومات ومسؤولة عن تطبيق سياسات الأمن والجرائم المعلوماتية بالمنشأة.
- حاصلة على شهادة تدريب وإعداد المدربين ومدرب معتمد من قبل المؤسسة العامة للتدريب التقني والمهني.
- عملت كمدربة ضمن برنامج اتقن بمؤسسة التدريب التقني والمهني لتقديم كورس أمن المعلومات والأمن السيبراني.
- متطوعة مع منظمة ArabWIC لدعم المرأة في مجالات الحوسبة ورئيسة الموقع الالكتروني بالمنظمة .

الأهداف والمحاور:

- التعرف على المبادئ الأساسية للأمن السيبراني.
- التعرف على الإحصائيات العامة للبيانات في استخدام السوشل ميديا.
- القدرة على التعامل مع القضايا الأخلاقية بالأمن السيبراني وأبعاد أمن المعلومات.
- التعرف على الفيروسات والهجمات وأنواعها والهندسة الاجتماعية والتصيد الإلكتروني.
- التعرف على الجرائم السيبرانية وأثرها على المجتمع وأنواع الجرائم.
- التعرف على العقوبات بالقانون السعودي للجرائم السيبرانية.

نشأة أمن المعلومات والأمن السيبراني:

في عام ٢٠١٠م قامت جميع قطاعات الدولة بتطبيق الحكومة الإلكترونية، والتركيز على بناء الأنظمة والتحول الوطني الإلكتروني، ثم أصيبت هذه القطاعات بفيروس شمعون واحد وشمعون ٢ وفيروس الفدية.

مما يجعلنا اليوم نحتاج وبشدة لحماية وتأمين معلوماتنا، انطلاقاً من الامكانات العسكرية، مروراً بالحفاظ على استقرار النظام، وصولاً إلى حماية القيم الجوهرية للمجتمع والمحافظة على المصادر الحيوية للبلد.

النشأة القانونية للأمن السيبراني:

١١ صفر ١٤٣٩هـ الموافق ٣١ أكتوبر ٢٠١٧م

صدر أمر ملكي كريم برقم (٦٨٠١) وتاريخ ١٤٣٩/٢/١١هـ إنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) ترتبط بمقام خادم الحرمين الشريفين- أيده الله -، والموافقة على تنظيمها.

وهي الجهة المختصة في المملكة بالأمن السيبراني والمرجع الوطني في شؤونه بهدف

- تعزيز الأمن السيبراني للدولة
- حماية مصالحها الحيوية
- وأمنها الوطني
- والبنى التحتية الحساسة فيها

تعريف الأمن السيبراني:

الأمن السيبراني هو مجموعة من الأطر القانونية والتنظيمية والوسائل التقنية والتكنولوجية تهدف إلى حماية الفضاء السيبراني (الإنترنت) من تهديد عمل الشبكة وأمن المعلومات ومن سوء استغلال الشبكة لأهداف إجرامية تؤثر سلباً في سلامة البنى التحتية للمعلومات الوطنية والشخصية.

تعريف آخر :

هو المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية .

الفرق ما بين أمن المعلومات والأمن السيبراني :

أمن المعلومات أشمل وأوسع من الأمن السيبراني

أمن المعلومات	الأمن السيبراني
يهتم أمن المعلومات بحماية المعلومات من الوصول غير المصرح به، والمعلومات قد تكون على هيئة وثائق ورقية أو مخزنة في وسائط إلكترونية	يهتم بأمن المعلومات التي يتم نقلها أو تخزينها أو معالجتها في أنظمة الاتصالات وتقنية المعلومات
أمن المعلومات يهتم بمجالات ضخمة كالتشفير والتخزين والتأمين الفيزيائي والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر.. وغيرها من المجالات	يهتم بوسائل الحماية والدفاع عن كل أنظمة الحواسيب والشبكات الذكية؛ فهو لا يركز كثيرًا على الوسائل التأسيسية -كوسائل التشفير مثلاً- بقدر تركيزه على الإفادة من هذه الوسائل في الدفاع الرقمي. الأمن السيبراني هو مجال يضع في أولوياته تقنيات الدفاع وأنظمته واستراتيجياته
أمن المعلومات يهتم بحماية المعلومات ولا يكترث بمدى سلامة وتوافر الخدمات الإلكترونية	الحفاظ على توافر وسلامة الخدمات التي يتم تقديمها عبر الفضاء السيبراني كالطاقة الكهربائية ووسائل الاتصالات
النسخ الاحتياطي للبيانات	يهتم بنسخ البيانات وتشفيرها
تحديث الانظمة وزيادة أمنها	تحديث الأنظمة وحمايتها والتوعية ومحاربة البرمجيات الخبيثة

الأخطار والتهديدات

مع الاعتماد المتزايد في حياتنا اليومية على الأنظمة المعلوماتية والأجهزة المتصلة بالشبكة العالمية للمعلومات، وتشعب طبيعة هذه الأجهزة من هواتف خلوية وأجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة.

فقد أشار تقرير صادر عن ماكينزي، إلى توقع زيادة المعلومات الرقمية بمعدل ٤٤%، خلال الأعوام من ٢٠٠٩م إلى ٢٠٢٠م. كما يشير العديد من التقارير إلى توالي حوادث اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات سوني، التي نتج عنها تسرب بيانات مليون مستخدم.

فالمعلومات التي تضخ وتنساب وتحفظ في الفضاء السيبراني وعبره، من أهم الموجودات التي يسعى إليها جميع المعنيين بهذا الفضاء دون استثناء. فالشركات والحكومات ومستخدمو الإنترنت يلاحقون المعلومات كلٌ بحسب أهدافه.

وتصدر الأخطار والتهديدات السيبرانية عن أعمال قصدية كالاختراقات والاعتداءات، وأعمال غير قصدية كالإهمال وقلة الوعي والإدراك.

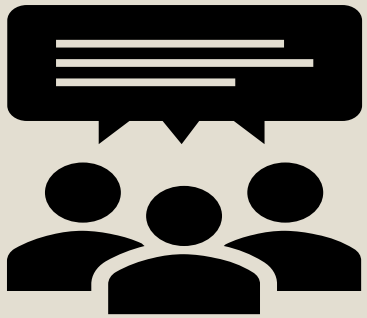
الانترنت في لحظة:

https://www.internetlivestats.com/

من أخطاء المستخدمين في الفضاء السيبراني:

و الآن يجدر بك الإجابة عن التساؤلات التالية لتقيس صحة تصرفاتك في الفضاء السيبراني

١	هل تقوم بتغير كلمة مرور حساباتك الشخصية بشكل دوري؟
٢	هل تستخدم نفس كلمة المرور في جميع حساباتك الشخصية؟
٣	هل تقوم بحفظ ملفات الارتباط على جهازك الشخصي؟
٤	هل تقوم بتحديث نظام التشغيل بشكل دائم؟
٥	هل تقوم بحفظ صورك الشخصية الخاصة والبيانات المهمة على خدمات التخزين السحابي؟



عناصر وأهداف أمن المعلومات CIA:

هناك ثلاث عناصر رئيسية ومقومات أساسية لابد أن تكون في كل التدابير والسياسات والعمليات والاجراءات المستخدمة في تأمين البيانات والمعلومات بحيث يتم بها تحقيق الأمن المعلوماتي ، هذه العناصر تختصر في الرمز **CIA.**

الرمز CIA :

الإتاحة أو التوافر:
Availability

يقصد بها توفر إمكانية الوصول الى البيانات والمعلومات للأشخاص المصرح لهم .

السلامة أو الدقة :
Integrity

وهي منع غير المصرح لهم من التعديل على البيانات والمعلومات .

الخصوصية أو السرية أو الموثوقية:
Confidentiality

وهي منع غير المصرح لهم من الاطلاع او الحصول على البيانات والمعلومات .

مبدأ AAA :

هذه العناصر الثلاث **(CIA)** يجب أن تمر من خلال **التحقق والتفويض والمحاسبة** وهو ما يطلق عليه معيار " **AAA** "

وهذا المفهوم أيضا يجب ان يستخدم عند تصميم او بناء أي خطة امنية لان معظم بروتوكولات أمن المعلومات قائمة في الأساس على هذا المفهوم.

والان لنتوقف قليلا لفهم هذا ال " **AAA**"

يعبر كل حرف من هذه الأحرف الثلاث لمصطلحات ثلاث هي:

Authentication

Authorization

Accounting

Authentication التحقق

هي الهوية الرقمية التي تمنح لك في عالم أمن المعلومات ولا تخلو من أن تكون:

1- شيئا تعرفه ككلمة مرور أو رمز دخول.

2 - شيئا تملكه مثل كارت ممغنط او مفتاح مشفر.

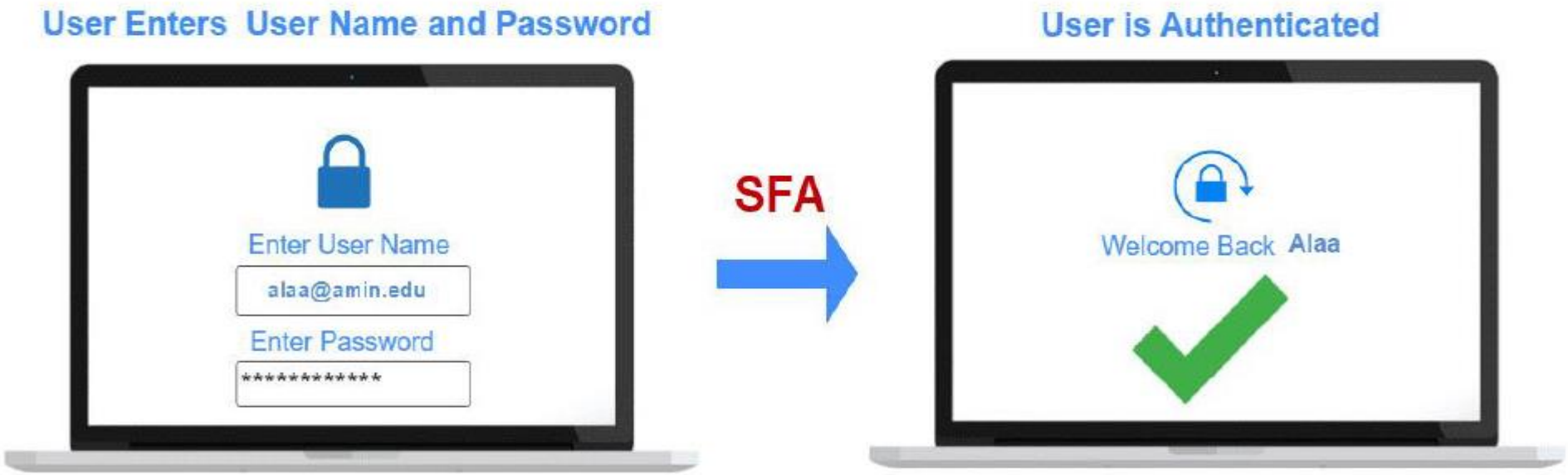
3 - شيئا يعبر عنك كبصمة الاصبع او العين أو بصمة صوتية.

في أمن المعلومات نستخدم أشكال عديده للوصول لمعيار التحقق كأجهزة ال **Biometric** مثلا والشهادات الرقمية والبروتوكولات التي يتم التركيز عليها غالبا ، كما ان معيار التحقق نفسه هو الاخر يأتي في عده أشكال .

التحقق Authentication:

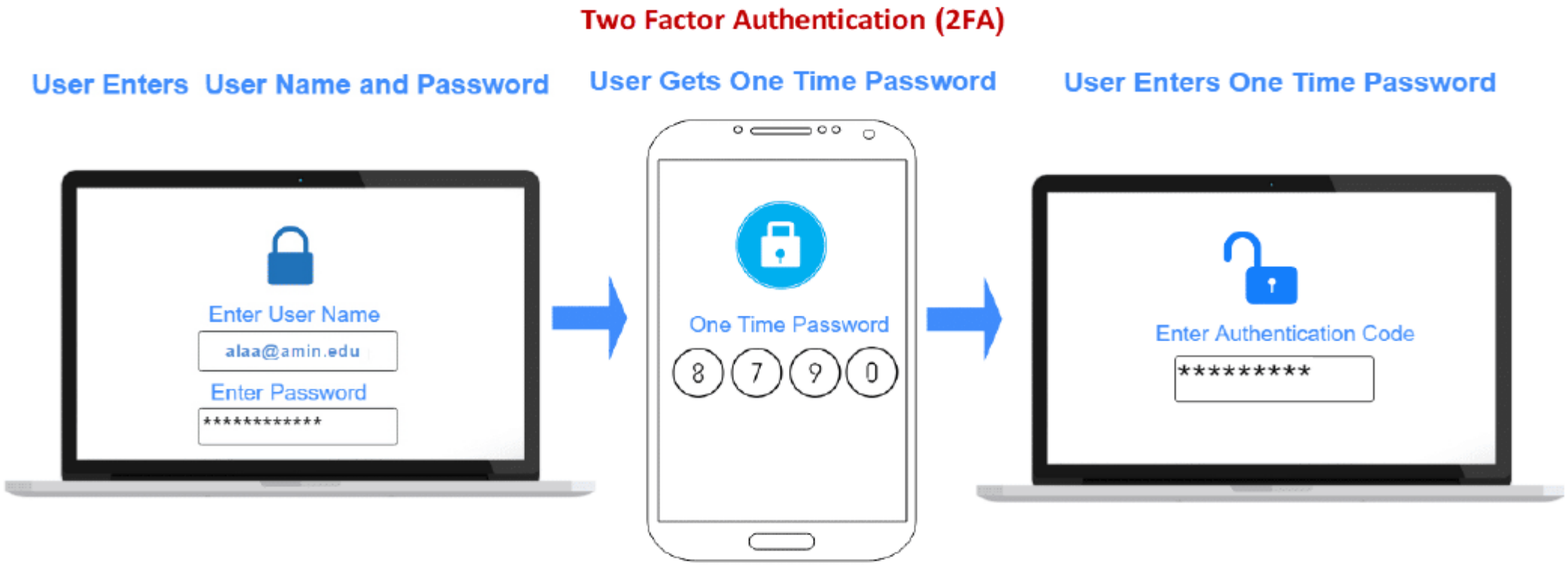
فقد يأتي الـ Authentication في صورة نوع واحد كبروتوكول Single-Factor Authentication (SFA)

والذي يعني ببساطة مطابقة الهوية بما هو موجود في قاعدة البيانات المخزنة كما في الشكل



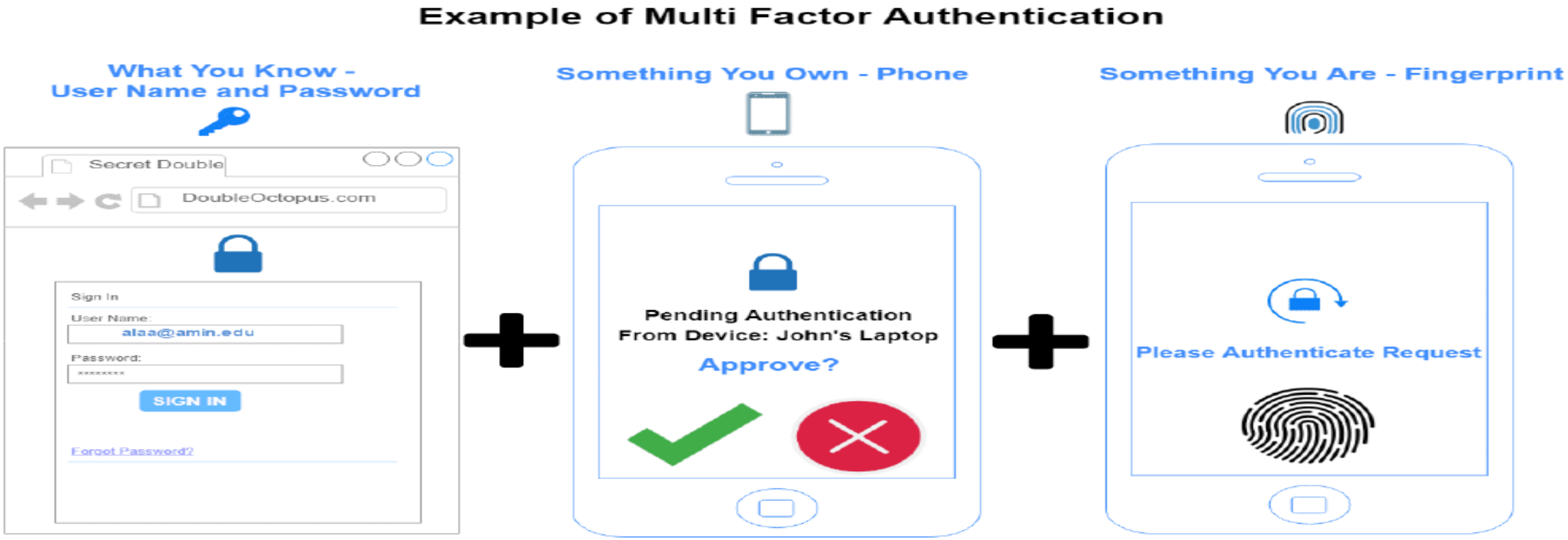
التحقق Authentication:

أو بدمج نوعين معا وهو ما يعرف بـ Two Factor Authentication (2FA)



التحقق Authentication:

أو بتداخل الأنواع كلها معا وهو ما يعرف بـ Multi-Factor Authentication (MFA) .



Authorization التفويض

وهو المصطلح الثاني في مفهوم (AAA) ويعني التفويض ويأتي مباشرة بعد التحقق ومن خلاله يتبين ما الذي يمكن لهويتك فعله وما لا يمكن .

المحاسبة Accounting

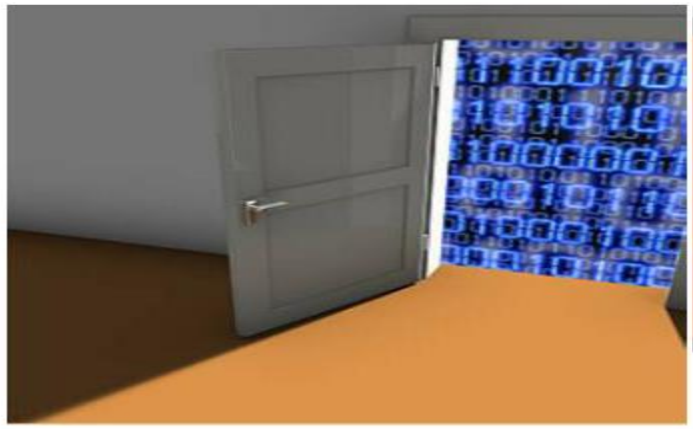
لتتبع وتأكيد عمليات ال Authenticationو ال Authorization

فهي تسجل وتراقب وتتابع جميع العمليات كتسجيل الدخول وأوقاتها والصلاحيات الممنوحة وتعد مرجعاً واثباتاً لمسؤول أمن المعلومات في حالات التسلل والعبث.

البرمجيات الضارة والفيروسات:

البرمجيات الضارة: هي برمجيات تصيب الأنظمة بطريقة خفية لانتهاك سرية أو سلامة أو توافر البيانات أو التطبيقات أو نظم التشغيل.

الفيروسات: برامج يكتبها مبرمجون ترتبط بالبرامج والملفات بغرض تغيير خصائصها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب تحتاج للتدخل من الانسان وتربط نفسها بمرفقات أخرى قادرة على التناسخ والانتشار.



البرمجيات الضارة أو الخبيثة


القنابل الموقوتة المنطقية Logic Bomb


احصنة طروادة Trojan Horse


الباب الخلفي Back Door


الفيروسات Virus

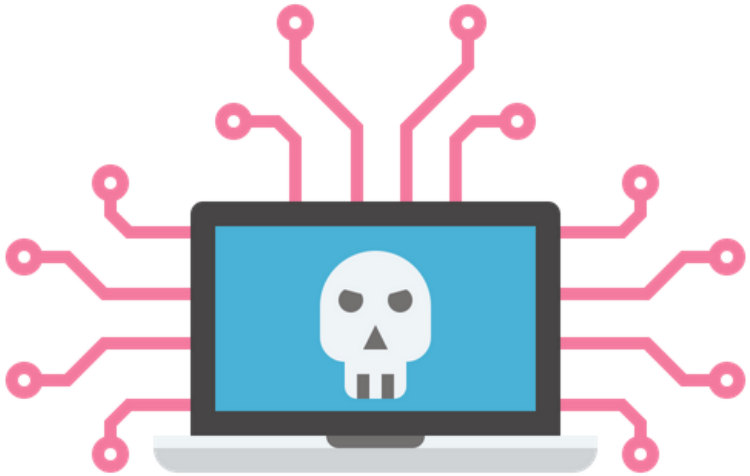

الديدان Worm


برامج الإعلانات والتجسس Spyware, Adware


البرامج الخبيثة الهجينة Hybrids


برامج تحكم وسيطرة Botnet

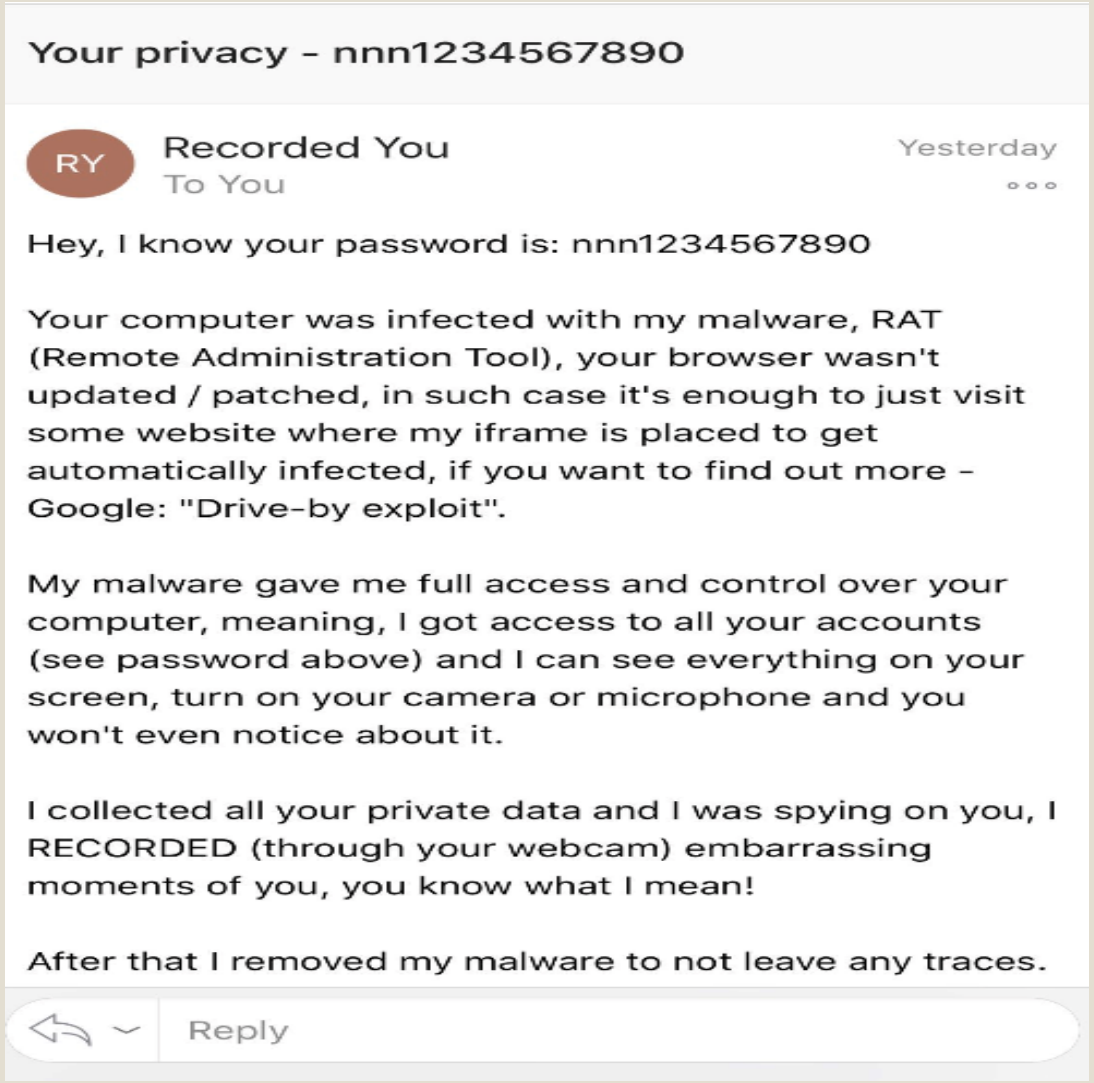

برامج الفدية الخبيثة Ransomware



الهجمات ATTACKS :

هو استغلال متعمد للضعف المكتشف في أنظمة معلومات الكمبيوتر .

أبرز أنواع الهجمات الإلكترونية:


Your privacy - nnn1234567890

RY Recorded You — Yesterday
To You

Hey, I know your password is: nnn1234567890

Your computer was infected with my malware, RAT (Remote Administration Tool), your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access and control over your computer, meaning, I got access to all your accounts (see password above) and I can see everything on your screen, turn on your camera or microphone and you won't even notice about it.

I collected all your private data and I was spying on you, I RECORDED (through your webcam) embarrassing moments of you, you know what I mean!

After that I removed my malware to not leave any traces.

Reply

الهندسة الاجتماعية : Social Engineering

الهجوم الذي يعتمد بشكل كبير على العنصر البشري حيث يستخدم التلاعب النفسي لخداع المستخدمين لارتكاب أخطاء أمنية أو التخلي عن معلومات حساسة.

مثال على هجمات الهندسة الاجتماعية عبر الايميل.

أبرز أنواع الهجمات الإلكترونية:

التصيد الإلكتروني:
Phishing

التصيد الاحتيالي هو أحد أكثر تقنيات **الهندسة الاجتماعية** شيوعًا اليوم ، هو جريمة إلكترونية يتم فيها الاتصال بالهدف عن طريق البريد الإلكتروني أو الهاتف أو رسالة نصية من قبل شخص يمثل مؤسسة شرعية لجذب الأفراد إلى توفير بيانات حساسة مثل معلومات التعريف الشخصية وتفاصيل البطاقات المصرفية وبطاقات الائتمان وكلمات المرور.

READ
BARCODE

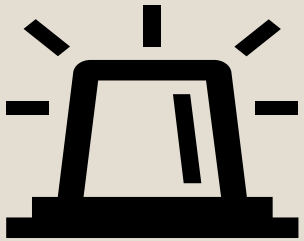
أبرز أنواع الهجمات الإلكترونية:

رفض الخدمة هجوم من نوع Dos:
Denial-of-service (Dos Attack)

هو هجوم عبر الانترنت يسعى فيه مرتكب الجريمة إلى جعل جهاز أو مورد الشبكة غير متاح.

الحرمان من الخدمة هجوم : DDos
Distributed denial-of-Service

هي محاولة ضارة لتعطيل الوصول إلى موقع الويب.



أبرز أنواع الهجمات الإلكترونية:

هجوم الرجل الموجود في المنتصف:
Man-in-the-middle Attack

هو هجوم يقوم فيه المهاجم باعتراض الاتصالات بين أجهزة الكمبيوتر لسرقة المعلومات التي تعبر الشبكة.

يمكن للمجرم أيضًا اختيار التلاعب بالرسائل ونقل المعلومات الخاطئة بين المضيفين لأن المضيفين لا يعلمون بحدوث تعديل للرسائل.

يسمحMitM للمجرم بالسيطرة على الجهاز دون علم المستخدم.

أبرز أنواع الهجمات الإلكترونية:

هجوم اليوم الصفر
: Zero-day attack

هو تهديد عن طريق مشكلة أو ثغرة أمنية غير معروفة لم يعرفها مطورو التطبيق أو البرنامج.

أبرز أنواع الهجمات الإلكترونية:

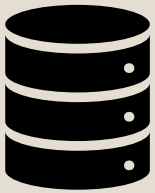
هجوم حقن قواعد البيانات SQL Injection attack :

تعتبر الـ SQL من المشاكل الشائعة في مواقع الويب التي تعتمد على العبث والاستغلال في قواعد البيانات.

على سبيل المثال، بكتابة بعض أوامر SQLفي أحد نماذج الويب التي تطلب معلومات الاسم والعنوان؛ وإذا لم يتم برمجة موقع الويب وقاعدة البيانات بشكلٍ صحيح، فربما تحاول قاعدة البيانات تنفيذ تلك الأوامر.

كسر كلمة المرور Password cracking :

محاولة كسر كلمة المرور اما عن طريق التخمين أو فك تشفيرها.



الجرائم السيبرانية وأنواعها

و قانون مكافحة الجرائم السيبرانية بالسعودية

تعريف الجريمة السيبرانية:

الدخول بغير وجه حق إلى جهاز حاسب آلي مستقل أو مرتبط بجهاز آخر مماثل، بواسطة شبكة محلية أو دولية وغيرها من الشبكات بغرض ارتكاب فعل ما يحرمه الشرع والقانون.

أبرز طرق الجريمة السيبرانية:

تخريب المعلومات وإساءة استخدامها: ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب	سرقة المعلومات: ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني	تزوير المعلومات: ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها
تزييف المعلومات: وتشمل تغيير في المعلومات على وضع غير حقيقي	انتهاك الخصوصية: ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد	التنصت: وتشمل الدخول لقواعد المعلومات على وضع غير حقيقي
التجسس: ويشمل اعتراض المعلومات ومحاولة معرفة ما يحدث	التشهير: ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف ونشرها بغرض الإساءة	السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية

سرقة الاختراعات: وخاصة في المجالات العلمية لاستخدامها في أو بيعها

الدخول غير القانوني: للشبكات بقصد إساءة الاستخدام أو الحصول على منافع

قرصنة البرمجيات: ويشمل النسخ غير القانوني للبرمجيات

قرصنة البيانات والمعلومات: ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها

خلاعة الأطفال: وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة

القنابل البريدية: وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية

إفشاء الأسرار: وتشمل الحصول على معلومات خاصة جداً ونشرها

الاحتيال المالي: بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقة التسوق ألمالية

سرقة الأرقام والمتاجرة بها: وخاصة أرقام الهاتف السرية أو استخدامها في الاتصالات الدولية

التحرش الجنسي: ويقصد بها المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة

قانون مكافحة الجرائم السيبرانية في المملكة العربية السعودية

إدراكاً من المملكة العربية السعودية بأهمية مواكبة تطورات التقنية الحديثة مع تحقيق الأمن المعلوماتي للفرد والمجتمع وللحد من إساءة استخدام النظم المعلوماتية وسداً للفراغ النظامي في هذا الجانب فقد صدر المرسوم الملكي الكريم رقم (م/١٧) وتاريخ ٨/ ٣/ ١٤٢٨هـ بالموافقة على نظام مكافحة الجرائم المعلوماتية من خلال تحديد تلك الجرائم والعقوبات المقررة لها وجهات الاختصاص.

وقد اشتمل النظام على (١٦) مادة استهلها بتقديم تعريف للمصطلحات الواردة في النظام والتي من أهمها تحديد مفهوم الجريمة السيبرانية.

كما حددت المادة الثانية الهدف من النظام وهو الحد من وقوع جرائم وذلك بتحديد الجرائم والعقوبات المقررة لكل منها بما يؤدي إلى:

- المساعدة على تحقيق الأمن المعلوماتي.
- حفظ الحقوق المترتبة على الاستخدام للحاسبات الآلية والشبكات المعلوماتية.
- حماية المصلحة العامة والأخلاق والآداب العامة.
- حماية الاقتصاد الوطني.

العقوبات النظامية عبر القانون السعودي للجرائم:

أقل عقوبة:

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

- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي- دون مسوغ نظام صحيح- أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.
- التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

العقوبات النظامية عبر القانون السعودي للجرائم:

أعلى عقوبة:

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

- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية.
- 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.

طرق الوقاية من القرصنة والجرائم الإلكترونية:

- أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
- تجنب فتح أي رسالة إلكترونية مجهولة المصدر بل المسارعة إلى إلغائها.
- وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعب من عملية القرصنة عليه، من هذه المواصفات: بأن يحتوي على أكثر من ثمانية أحرف، أن يكون متنوع الحروف والرموز واللغات إلخ..
- الحرص على المعلومات الشخصية والحاسب الشخصي وذلك بوضع برامج الحماية المناسبة.
- وضع سياسات دولية وعقوبات كبيرة على مرتكبي هذه الجرائم.
- تفعيل أحدث التقنيات والوسائل للكشف عن هوية مرتكبي الجرائم.
- نشر التوعية في المجتمعات حول الجرائم الإلكترونية ومخاطرها، وتعريف الأفراد بكيفية الحفاظ على معلوماتهم وخصوصياتهم؛ كحساباتهم البنكية وبطاقاتهم الائتمانية.
- إنشاء خطوط هاتفية ومؤسسات معينة تابعة للدولة للإبلاغ عن الحالات التي تتعرض لمثل هذا النوع من الجرائم.
- توجيه التشريعات والقوانين وتحديثها بما يتماشى مع التطورات التكنولوجية، لفرض قوانين جديدة فيما يستجد من هذه الجرائم.

طرق الوقاية من القرصنة والجرائم الإلكترونية:

التوصيات:

- أولاً: تحديث قوانين الجرائم المعلوماتية بشكل مستمر.
- ثانياً: استحداث هيئات للجرائم المعلوماتية في كل الدول مرتبطة بقطاع وزارة الداخلية.
- ثالثاً: توعية الأطفال والكبار والموظفين بشكل دائم بخطورة الجرائم الإلكترونية من خلال حملات توعوية دائمة وتدريب مكثف.
- رابعاً: الاهتمام بمكافحة الجرائم المعلوماتية لأن تأثيرها على المجتمع يمثل عدة جوانب اقتصادية ونفسية واجتماعية ومعاملتها بأهمية عالية.
- خامساً: مقاضاة الشركات التي تبيع البيانات الخاصة بالعملاء علماً بأنه نظاما يحق لك مقاضاتهم بالقانون.
- سادساً: يجب تطوير قدرات الهيئات أو الشرطة في كل الدول وإعطائهم دورات متعددة لمعرفه ما تم تحديثه مع الجهات العالمية المتقدمة.
- سابعاً: حث المنظمات في الدول على زيادة امن بياناتها وأنظمتها وتشفيرها وعمل جدران آمنة للتصدي لتلك الهجمات.

حماية
Hemaya

”يجب أن نعمل لمواجهة التحديات
السيبرانية حتى لا تتحول
إلى عوائق اقتصادية “

سمو ولي العهد
الأمير محمد بن سلمان بن عبدالعزيز

@areej_alamer7 HemayaGroup WWW. HEMAYAGROUP .ORG

Thank you For Listening

To Contact:

My Twitter page:

@meaad_310

QUESTIONS?