جامعة تبوك
University of Tabuk

الحقيبة التدريبية

الوقاية من المخاطر السيبرانية

إعداد وتنفيذ: د. عادل راضي الحربي

نبذة

- **نبذة تعريفية:**
- د. عادل الحربي تخرج بدرجة البكالوريوس بتخصص علوم الحاسب الآلي من جامعة القصيم بالمملكة العربية السعودية في عام 2008 م. و لقد حصل على درجتي الماجستير في تخصص هندسة أمن المعلومات وهندسة الحاسب الآلي من جامعة ساوثرين ميوديست يونيفرستي بالولايات المتحدة الأمريكية في ولاية تكساس بمدينة دالاس في عامي 2013 م و 2015 م على التوالي. وفي عام 2017 م حصل على درجة دكتوراه الفلسفة في تخصص هندسة الحاسب الآلي من ساوثرين ميوديست يونيفرستي بالولايات المتحدة الأمريكية. كما وأنه تعيين كعضو هيئة تدريس بجامعة تبوك بكلية الحاسبات و تقنية المعلومات منذ عام 2009م. حيث أنه عضو بعدد من الجمعيات العلمية، كما أنه شارك بإقامة الكثير من الدورات والبرامج التدريبية. نشر العديد من الأبحاث العلمية الدولية و حصل على جوائز علمية، حيث أن أبحاثه العلمية تتمحور حول موضوعات أمن المعلومات وتطبيقات الأجهزة الذكية و تقنية القياسات الحيوية و التنقيب عن المعلومات وكذلك الذكاء الاصطناعي.
- **معلومات التواصل:**
  - البريد الإلكتروني: aalharbi@ut.edu.sa
  - الموقع الشخصي: https://dradel.website

دليل البرنامج التدريبي

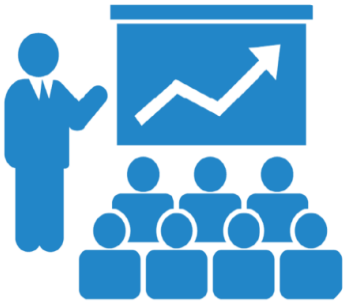
- الأهداف العامة للبرنامج التدريبي: يهدف البرنامج التدريبي إلى توعية المتدربين بضرورة الوقاية الالكترونية والأمن السيبراني.
- الأهداف التفصيلية للبرنامج التدريبي: في نهاية البرنامج التدريبي يجب على المتدرب أن:

- ✓ يحدد مفهوم الأمن السيبراني.
- ✓ يعدد خصائص الأمن السيبراني.
- ✓ يقدر أهمية الأمن السيبراني.
- ✓ يصنف أنواع التهديدات السيبرانية.
- ✓ يطبق طرق التشفير.
- ✓ يعرف أنواع الفيروسات وسبل الحماية منها.
- ✓ يعرف على الهندسة الاجتماعية.
- ✓ يعرف الشبكات وأنواعها وسبل الحماية بشكل آمن.
- ✓ شهادات وتخصصات الأمن السيبرانى.

إرشادات المتدرب

أخي إن هذا البرنامج التدريبي يهدف إلى مساعدتك على الوقاية من المخاطر السبرانية بكفاءة عالية.

وقد صمم هذا البرنامج مشتملاً على مجموعة من النشاطات العملية والعلمية التي تتطلب منك المشاركة الفاعلة مع زملائك، حيث تحترم خبراتك وهي المنطلق مع إفساح المجال للحوار والمناقشة وإبداء الرأي وصولاً إلى تكامل الخبرات عند المتدربين.



إرشادات المتدرب

عزيزي المتدرب الفاضل نأمل منك مراعاة الإرشادات التالية: -

- الاستعداد للمشاركة في البرنامج والحضور في الوقت والمكان اوحددين.
- ننصح بقراء ة الحقيبة التدريبية والاطلاع على المادة العلمية بتمعن.
- إثراء النقاش بكل ما لديك فيما يتعلق بالبرنامج.
- الالتزام بتواصل العمل وعدم الانشغال عن المجموعة.
- كن مشاركه في جميع الأنشطة.
- احترم أفكار المدرب والزملاء.
- أنقد أفكار المدرب والزملاء بأدب إن كانت هناك حاجة.
- احرص على استثمار الوقت.
- تقبل الدور الذي يسند إليك في المجموعة.
- حفز أفراد مجموعتك في المشاركة في النشاطات.
- احرص على بناء علاقات طيبة مع المدرب والزملاء أثناء البرنامج التدريبي.
- احرص على ما تعلمته في البرنامج وطبقه في الميدان.

وثيقة المحاضرة التدريبية

- يكون المرشح لحضور البرنامج التدريبي من ضمن الفئة المستهدفة من البرنامج التدريبي وهم حيث تم تصميم البرنامج التدريبي ليتوافق مع احتياجاتهم المحددة.
- الالتزام بحضور كامل الفترات التدريبية.
- الالتزام بتنفيذ كافة التمارين العلمية التي يطلبها منك المدرب وبتطبيق كافة التقنيات والمهارات المطلوبة من مدرب البرنامج التدريبي.
- الالتزام بغلق الجوال اثناء المحاضرة.
- احترام الآراء المختلفة.
- يمنع الأحاديث الجانبية مع زملائك.

خطة البرنامج التدريبي

الأساليب والأنشطة التدريبية التي يستخدمها البرنامج

الوسائل التدريبية

الوسائل والمواد التدريبية التي يتطلب توفرها في هذا البرنامج

التعارف

10
دقائق

المقدمة

شهدت البشرية منذ سنوات تقدما تقنيا وتكنولوجيا، قلما عرفه عصر من العصور السابقة من قبل، حتى بات هذا التقدم ثورة قائمة بذاتها في عالم الاتصالات والعلاقات، كما أصبح العالم بفضلها بمثابة قرية كونية فعلا، بحيث أصبح للفضاء السيبراني الافتراضي دور في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية، وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي، حتى أصبح العالم اليوم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي خلال الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف. (نورة شلوش، ٢٠١٨)

مفهوم الأمن السيبراني

- الجريمة السيبرانية: هي ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونياً وذلك من خلال قراصنة الكتابة أو أستخدام برامج الكمبيوتر الجاهزة.
- أما الأمن السيبراني Cyber security هو عبارة عن مجموع الوسائل التقنية و التنظيمية و الإدارية التي يتم استخدامها لمنع الاستخدام غير المرح به سوء الاستغدلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات و المعلومات التي تحتويها.
- الأمن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر، و الخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة.

مفهوم الأمن السيبراني

الأمن السبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر، و الخوادم، والأجهزة المحمولة، والأنظمة الإلكتورنية، والشبكات، والبيانات من الهجمات الخبيثة. وتتمثل خطورتها في:

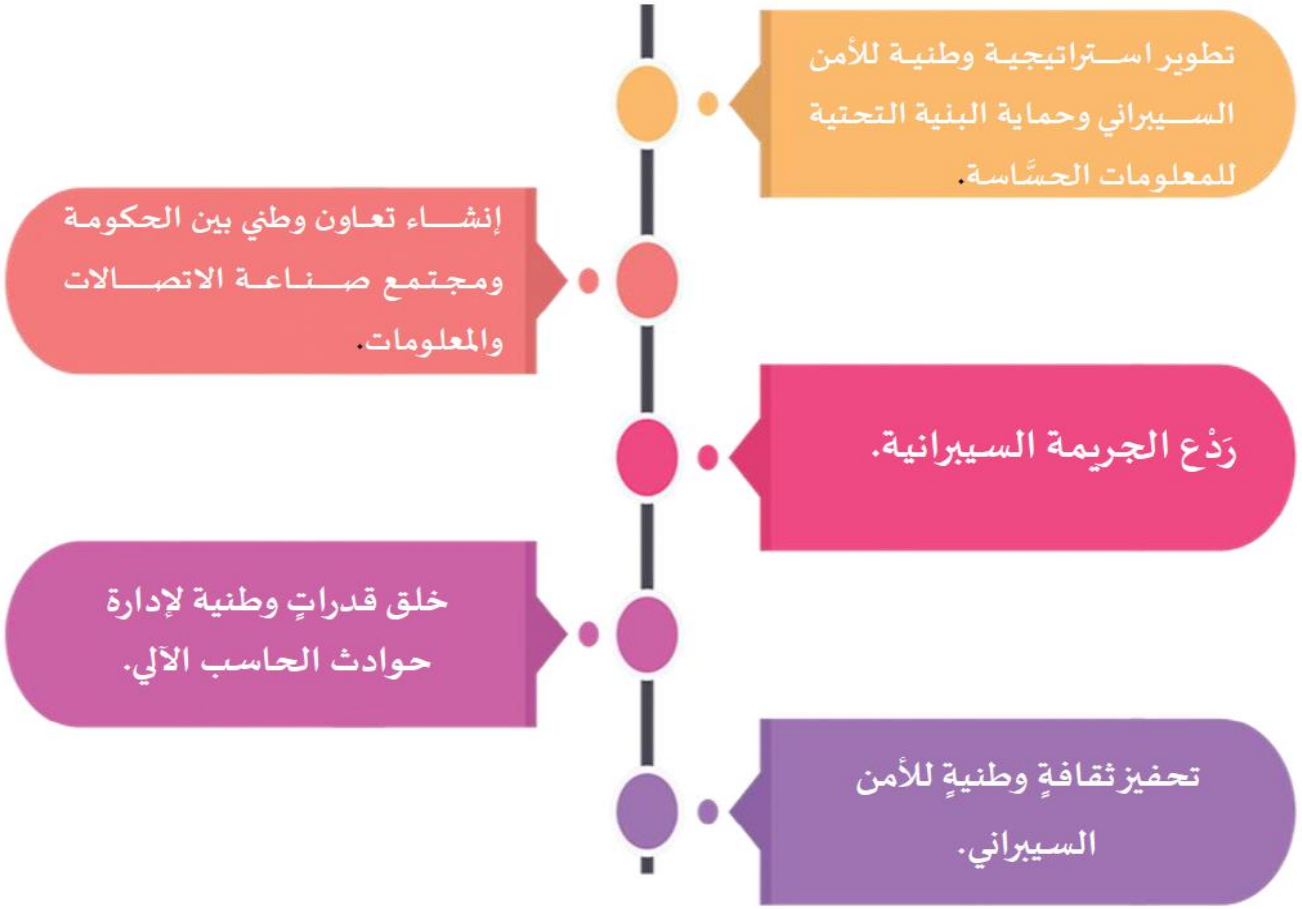
- عدم توافر رؤية مناسِبة في استخدام الشبكات والبيانات تسمح للمهاجمين بالعمل في الخفاء.
- قلة ثقافة المواطنين حول قهم التأثير الذي تشكله الهجمات الإلكترونية.
- الحاجة إلى التدريب في مجال تكنولوجيا المعلومات على قضايا الأمن المعلوماتي.
- ارتفاع عدد المجموعات المتطورة التي تهاجم الأهداف بإستخدام البرمجيات الضارة malware
- انتشار الهواتف الذكية.

خصائص الأمن السيبراني

- وتكمن مخاطر هذا المجال في صعوبة تحديد هوية الكيان الذي نفذ الهجات السيبرانية في الكثير من الحالات.
- وكذلك غياب التشريعات الدولية التي تضع الدول أو المؤسسات التي تقوم بمثل هذه الأنشطة تحت طائلة القانون الدولي، ما يعني عدم القدرة على ملاحقتها قانونيا، على خلاف مجالات الحرب التقليدية.

(نورة شلوش، ٢٠١٨) تعتمد صلاحية الأمن السيبراني على الركائز الخمس التالية:

تعتمد صلاحية الأمن السيبراني على الركائز الخمس



أبعاد الأمن السيبراني

1. البعد العكسري

من المعلوم، أن بدايات الإنترنت، قد طورت في بيئة عسكرية، بشكل أساسي، لتضاف إليها فيما بعد البيئة الإكاديمية، بما تمثل من أبحاث تخدم تطوير القدرات العسكرية.

2. البعد الاجتماعي

تسمح طبيعة الإنترنت المفتوحة، عبر المدونات والشبكات الإجتماعية بشكل خاص، لكل مواطن، بأن يعبرعن تطلعاته السياسية، وطموحاته الإجتماعية، بأشكالها كافة.

3. الابعاد السياسية

تتمثل الابعاد السياسية للأمن السيبراني، بشكل أساسي، في حق الدولة في حماية نظامها السياسي، وكيانها، ومصالحها الاقتصادية، التي تعني، حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن، أن يتحول إلى لاعب أساسي، في اللعبة السياسية.

أبعاد الأمن السيبراني

4. الابعاد الاقتصادية

يرتبط الأمن السيبراني، أرتباطاً وثيقاً بالإقتصاد. فالتلازم واضح، بين إقتصاد المعرفة وتوسع إستخدام تقنيات المعلومات و الإتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، والمخزنة، والمستخدمة، على كل المستويات.

5. الابعاد القانونية

يرتب النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، كما أسلفنا، نتائج قانونية، وموجبات، تستدعي إهتماما، لجهة إيجاد القواعد الخاصة، بحل النزاعات التي يمكن ان تنشأ عنها.

منهجية الاستجابة للحوادث السيبرانية
NIST standard

تمرين

- من وجهة نظرك حدد لماذا الأمن السيبراني مهماً لك ولغيرك.
- بالتعاون مع مجموعتك ابحث عن أحدث 3 حوادث عن الاختراق الأمني على الانترنت مبينا الأسباب وكيفية الحماية وعدد تكرك الحادثة مرة أخرى من وجهة نظرك. ثم تناقش مع المدرب.

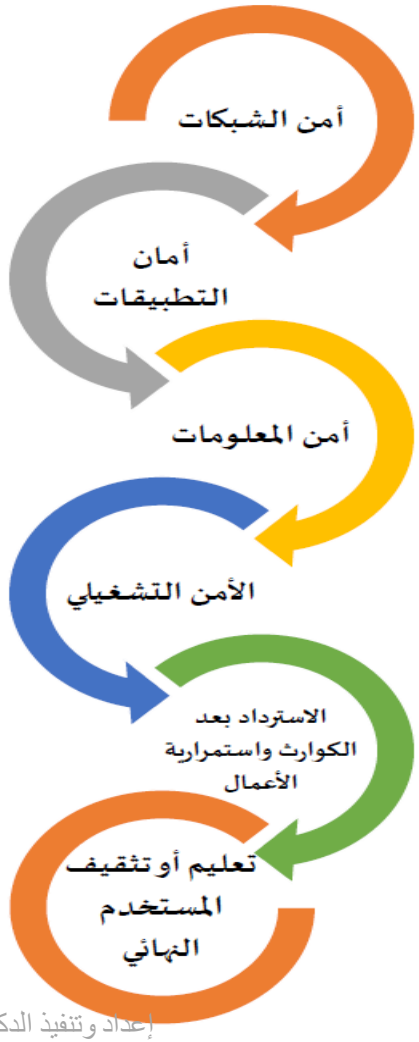
لماذا الأمن السيبراني مهماً؟

في عالمنا المرتبط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة.

لماذا الأمن السيبراني مهماً؟

- يمكن تلخيص أهمية الأمن السيبراني في:
  - تطوير استراتيجية وطنية و حماية البنية التحتية للمعلومات الحساسة.
  - إنشاء تعاون وطني بين الحكومة و مجتمع صناعة الاتصالات والمعلومات.
  - ردع الجريمة السيبرانية.
  - حلق قدرات وطنية لإدارة الحاسب الآلي.
  - تحفيز ثقافة وطنية للأمن السيبراني.
  - تحقيق سرية وخصوصية المعلومات.

على ماذا ينطبق مصطلح الأمن السيراني



- ينطبق هذا المصلح على مجموعة متنوعة من السياقات، بدءاً من قطاع الأعمال، وصولاً إلى الحوسبة المتنقلة، و ابلإمكان عموماً تقسيمها إلى فئات شائعة كما يلي:

أنواع التهديدات السيبرانية

- حجم التهديد السيبراني
- تنفق حكومة الولايات المتحدة 19 مليار سنوياً على الأمن السيبراني لكنها تحذر من أن الهجمات السيبرانية تستمر في التطور بوتيرة سريعة
- هناك أنواع عديدة من التهديدات السيبرانية التي يمكنها مهاجمة الأجهزة عموماً في ثلاث فئات: وهي الهجمات على السرية، النزاهة، و التوافر.
  - الهجمات السرية Confidentiality
  - الهجمات على النزاهة Integrity
  - الهجمات على التوافر Availability

أنواع التهديدات السيبرانية

- بعض مجالات التهديدات الإلكترونية

الهدف من الأمن السيبراني

- ضمان توافر استمرارية عمل نظم المعلومات
- اتخاذ جميع التدابير اللازمة لحماية المواطنين و المستهلكين.
- تعزيز حماية وسرية وخصوصية البيانات الشخصية.
- حماية الأنظمة التشغيلية من أي محاولات للولوج.
- تعزيز حماية أنظمة التقنيات التشغلية وكموناتها من أجهزة و برمجيات.
- حماية مصالح المملكة الحيوية و أمنها الوطني، والبنى التحتية الحساسة فيها
- التأسيس لصناعة وطنية في مجال الأمن السيبراني
- تعزيز حماية الشبكات.
- تعزيز حماية أنظمة تقنية المعلومات.
- أن تكون المرجع الوطني للمملكة في شؤون تخصصها

تصنيف الثغرات الأمنية

- بشكل يومي تكتشف ثغرات أمنية على برمجيات، أنظمة التشغيل او تطبيقات الويب ومن الممكن الحصول عليها من جهات خارجية متخصصة او مسؤولةNCA-NCSC, Threat Intelligence, Vendors او من أحد المهتمين في الأمن السيبراني يقدم تقرير بوجود ثغرة قام بأكتشافها.
- حيث ان هناك دراسات تمت عام ٢٠٢٠ ميلادي أن عملية ظهور الثغرة وتوافر التحديث تقدر تقريبا 9 أيام، وتشير تقارير عالمية مثل تقرير الشركة FireEye أن الوقت ما بين اصدار التحديث واستغلال الثغرة من قبل المهاجمين تصل أحيانا الى ساعتين فقط من ظهور التحديث.
- يعتمد التعامل مع الحادثة الناشئة من الثغرات بناء على مدى خطورتها وحساسية النظام المكتشف فيه الثغرة وهنا يتم التصنيف على أربع فئات (حرج، عالي، متوسطة، منخفضة).

تصنيف الثغرات الأمنية

1. حرج:

- في حال وجود الخدمة خارجياً يتم فوراً حجب الوصول لها من الخارج حتى يتم تحديث النظام او حل المشكلة. (في حال عدم القدرة على حجب الخدمة يتم فورا العمل على تخفيف الخطر من تقنين صلاحيات الوصول أو حجب الأوامر المستخدمة في الثغرة او حتى حجب بعض المنافذ المستغلة.)
- في حال وجود الخدمة داخليا يتم العمل على تحديثها فوراً على ألا تزيد الفترة المتفق عليها داخل المنظمة.

2. عالي:

- في حال وجود الخدمة داخلياً / خارجية يتم العمل على تحديثها فوراً على ألا تزيد الفترة المتفق عليها داخل المنظمة.

تصنيف الثغرات الأمنية

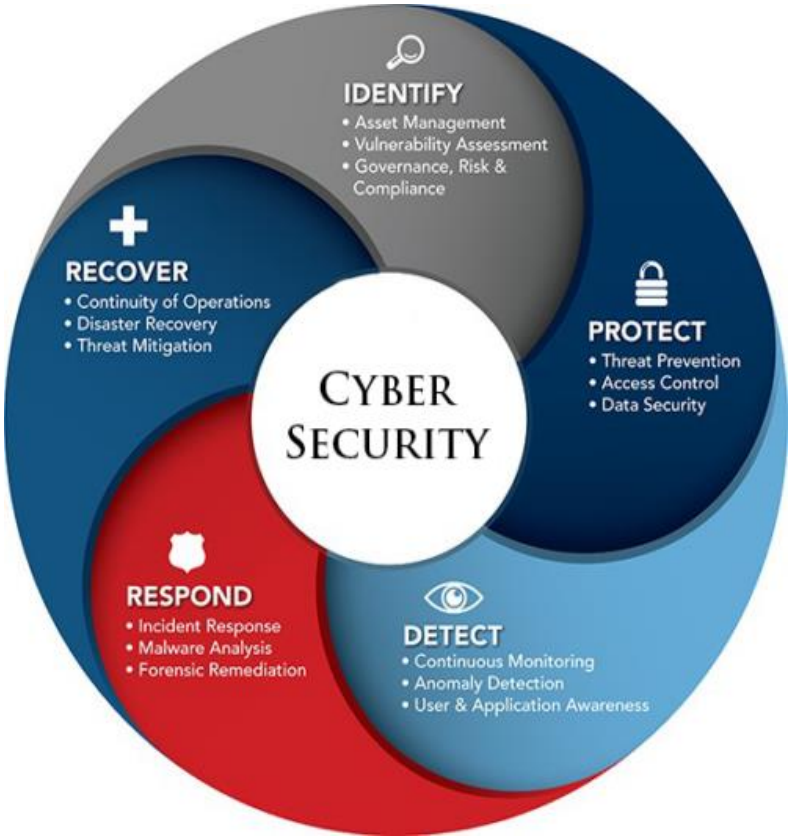
3. متوسط:

- في حال وجود الخدمة داخلياً / خارجية يتم العمل على تحديثها فوراً على ألا تزيد الفترة المتفق عليها داخل المنظمة.

4. منخفض:

- في حال وجود الخدمة داخلياً / خارجية يتم العمل على تحديثها فوراً على ألا تزيد الفترة المتفق عليها داخل المنظمة.

خطوات تخفيف المخاطر
Mitigation



- يوجد خدمات حساسة لا يمكن إيقافها فوراً بسبب إحتياج الاعمال لذا نلجأ إلى تخفيف الخطر وطرد المهاجم. كما هي موضحة بالخطوات التالية:
  - عمل تحديث لإغلاق ثغرات النظام في حال وجود ثغرة قائمة.
  - حجب العنوانين المشبوهة التي تم اكتشافها من خلال التحليل ويفضل عمل تقييد الوصول للخدمات والأنظمة على حسب الموقع الجغرافي.
  - تغيير جميع كلمات المرور المرتبطة بالخدمة المصابة.
  - مراقبة الخدمة أو النظام من خلال مركز السجلات المركزي SEIM.

استـراحــة

تطور التشفير

- تاريخ علم التشفير
- أشقت كلمة التشفير في اللغة الانجليزية cryptography من الكلمة اليونانية kryptos، والتي تعني مخفياً كتابة في الواقع كلمة مخفي تعني اختفاء المادة فيزيائياً من أعين العدو، في حين أن علم التشفير يسمح لأي شخصين بالتواصل عبر لغة لا يستيطع خصمهما فهمهما.
- محللو الشفرات الأوائل
- إن المعرفة بسلسة الخطوات اللازمة لتحويل نص عادي لأي رسالة إلى نص مشفر. تعرف بمفتاح الشفرة، والذي ينبغي بقاءها آمناً. ويتطلب كسر الشفرة من دون معرفة مفتاح الشفرة مهارة عالية.

تطور التشفير

- لم تكسر خوارزمية شفرة التعويض خلال الألفية الأولى للميلاد حق أدرك العالم العربي الكندي ضعف هذه الشفرة، وفقا لسيمون سينج Simon Singh مؤلف كتاب الشفرة. لاحظ الكندي أن بعض الحروف تتكرر في النص المشفر أكثر من غيرها.
- وكان الكندي قادراً على فك شفرة خوارزمية التعويض من خلال ملاحظته للحروف التي تكررت كثيراً في النص المشفر. وبهدا أصبح أصبح العلماء العرب أول محللي الشفرات في العالم. ما جعل محللي الشفرات يتبعون أساليب العلماء العرب.
- ومع تقدم علم التشفير، تضاعف التحدي على محللي الشفرات، من بين المناوشات الأكثر شهرة في هذه المعركة المستمرة جهود الحلفاء لكسر شفرة آلة اللغز Enigma الألمانية خلال الحرب العالمية الثانية، إذ كان الألمان يشفرون الرسائل بإستخدام تلك الآلة، والتي كان يغير مفتاحها يومياً، إلى أن استطاع محلل الشفرات الآن تورينج تطيور جهاز سمي بالقنية ليتتبع إعددات آلة اللغز و يسكر الشفرة، وفقاً لوكالة المخابرات المركزية الأمريكية.

تطور التشفير

- عصر الحاسوب الكمومي
- يبحث محللو التشفير اليوم في فيزياء الكم عن طريقة للتشفير غير قابلة للكسر، إذ تصف فيزياء الكم السلوك الغريب للمادة بمقاييس صغيرة بشكل لا يصدق. وكالحة قطة شرودنغر الشهيرة، توجد الجسيمات دون الذرة في العديد من الحالات في آن واحد.
- ولكن عند فتح الصندوق، فإنك تلاحظ حالة واحدة فقط في السبعينات والثمانينات، بدأ الفيزيائيون باستخدام هذه الخاصية غير المرغوب فيها التشفير الرسائل السرية. وهي طريقة تعرف الآن باسم: توزيع المفاتيح الكمومية.
- يمكن تبادل الكم لمسافات طويلة عبر الألياف البصرية، لكن ما أثار اهتمام الفيزيائين هو طريقة توزيع هذه المفاتيح، تتيح هذه التقنية، التي أقترحها أرتور لإيكيرت Artur Ekert، أن يتواصل فوتونان عبر مسافات شاسعة بفضل ظاهرة تعرف بالتشابك الكمومي.

تطور التشفير

- يقول إيكيرت، أستاذ في جامعة أوكسفورد ومدير مركز تكنولوجيات الكم في الجامعة الوطنية: «الجسيمات الكمومية المتشابكة لها خاصية مذهلة، إذ حتى بعد فصل بعضها عن بعض، وحتى على مدى مئات الأميال، فإنها تشعر ببعضها». . تشفير الكم هو أكثر من مجرد فكرة مجردة. ففي عام 2004، قام الباحثون بتحويل 3000 يورو إلى حساب مصرفي عن طريق الفوتونات المتشابكة، وفقاً لما ذكرته مجلة العلوم الشائعة-Popular Science

Cryptography
ماهو الشتفير أو التعمية

- هو عبارة عن فن وعلم صناعة وتطوير أنظمة التشفير القادرة على حماية المعلومات والتي تستخدم في أمن المعلومات وذلك من خلال تحويل البيانات والنصوص المقروءة إلى بيانات ونصوص غير مقروءة وغير مفهومة.
- كما يعرف انه هو خلط البيانات لجعلها غير قابله للقراءة بواسطه الأشخاص غير المصرح لهم بذلك.

Cryptography
ماهو الشتفير أو التعمية

- أما تحليل التشفير أو Cryptanalysis : هو عبارة عن علم وفن كسر وتحليل البيانات المشفرة والهدف منه ايجاد الطرق والأساليب التي يمكن من خلالها تحويل أي بيانات مشفرة وغير مقروءة إلى قيمتها الأصلية المقروءة والمفهومة.
- وينقسم التشفير إلى قسمين رئيسين:
  - تشفير البيانات Encryption
  - فك تشفير البيانات Decryption

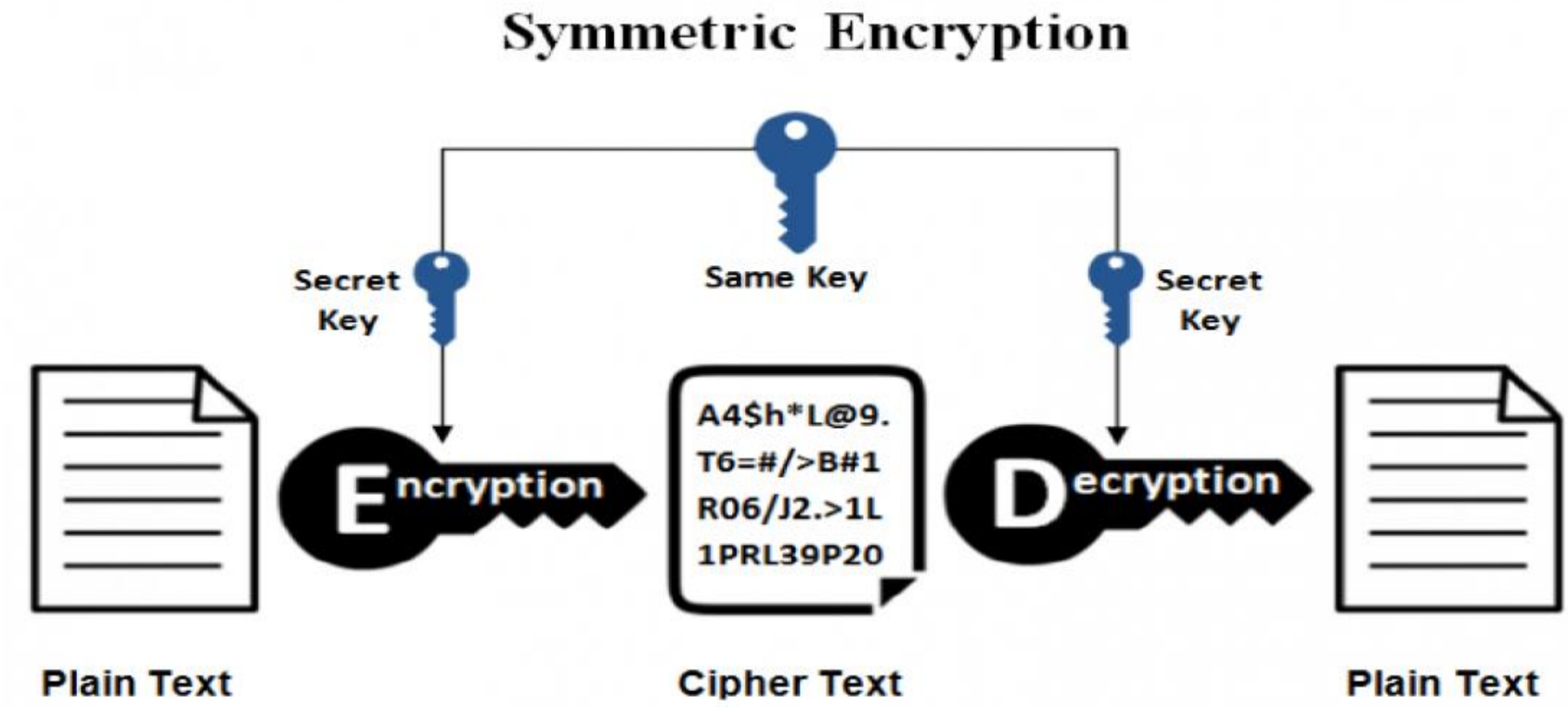
أهداف التشفير

- يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كتالي:

أنواع التشفير

- التشفير التقليدي:
- يسمى أيضا التشفير المتماثل Cryptography Symmetric وهو يستخدم مفتاح واحد لعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. مثال على ذلك؛ إذا أراد زيد إرسال رسالة مشفرة إلى عبيد، عليه إيجاد طريقة آمنة لإرسال المفتاح إلى عبيد. فإذا حصل أي شخص ثالث على هذا المفتاح فإن بإمكانه قراءة جميع الرسائل المشفرة بين زيد وعبيد كما في الصورة التالية و التي توضح عمل التشفير باستخدام المفتاح الواحد.

أنواع التشفير



بعض الأمثلة على أنظمة التشفير التقليدي

- شيفرة قيصر:
- وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها. المثال التالي يوضح طريقة عمل شيفرة قيصر: إذا شفرنا كلمة SECRET واستخدمنا قيمت المفتاح ٣، فإننا نقوم بتغيير مواضع الحروف ابتداء من الحرف الثالث وهو الحرف D، وعليه فان ترتيب الحروف سوف يكون على الشكل التالي:

بعض الأمثلة على أنظمة التشفير التقليدي

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" تكون على الشكل الحالي:
- DEFGHIJKLMNOPQRSTUVWXYZ ABC
- الآن قيمة ال Fac، BE a، DaA، وهكذا.
- بهذا الشكل فان كلمة SECRET سوف تكون VHFUHwلتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة : يجب أن ترسل له قيمة المفتاح 3.

تشفير البيانات القياسي DES

- طور هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الكمبيوتر وزيادة سرعة معالجته للبيانات، حيث أنه قد يتم كشف محتوى رسائل مشفرة به في وقت قصير

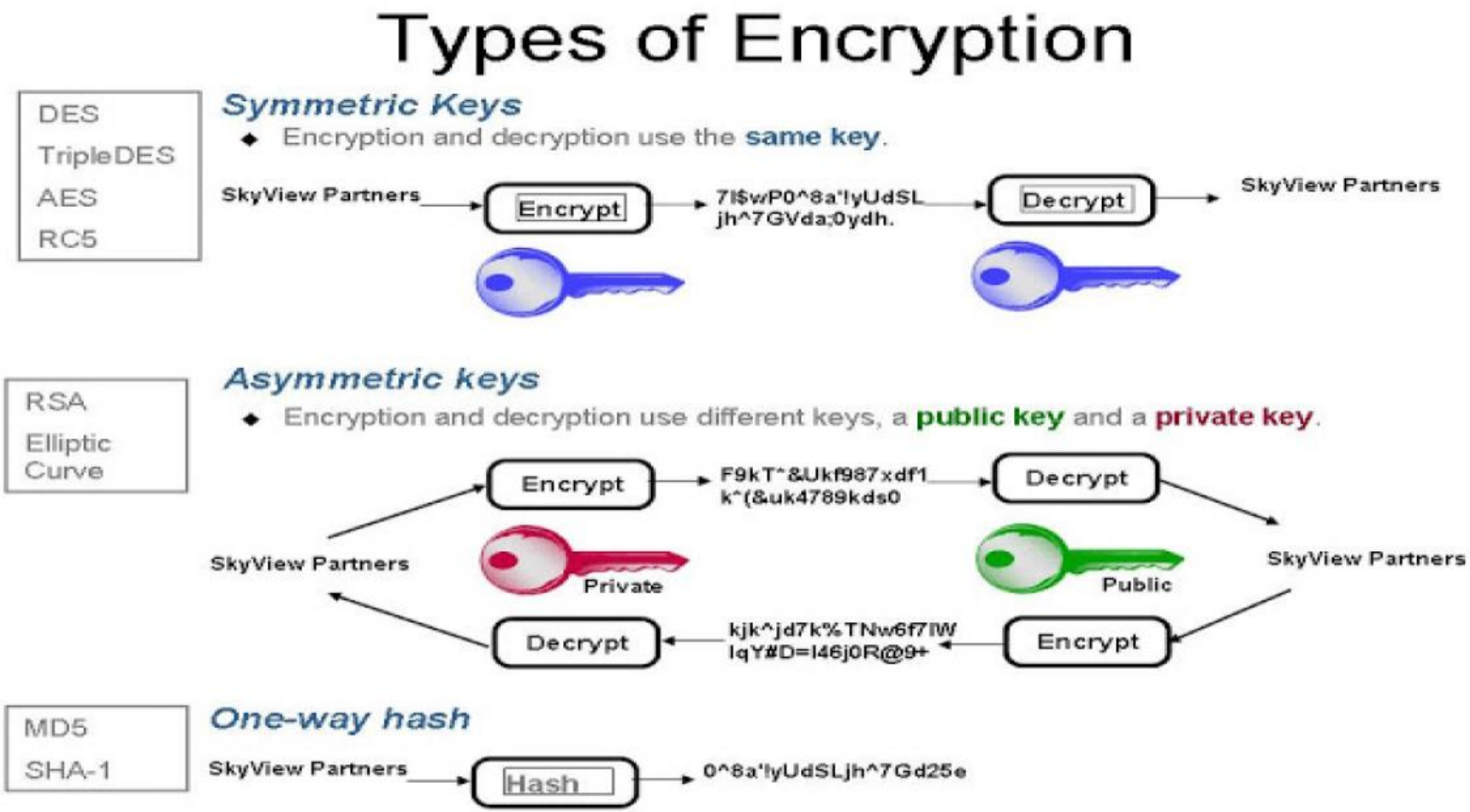
AES, IDEA, DES, blowfish

- وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير.
- كل ما ذكر من الأمثلة السابقة يعتمد على مبدأ المفتاح الواحد لعملية التشفير وفك التشفير

تشفير المفتاح العام:(اللامتماثل)

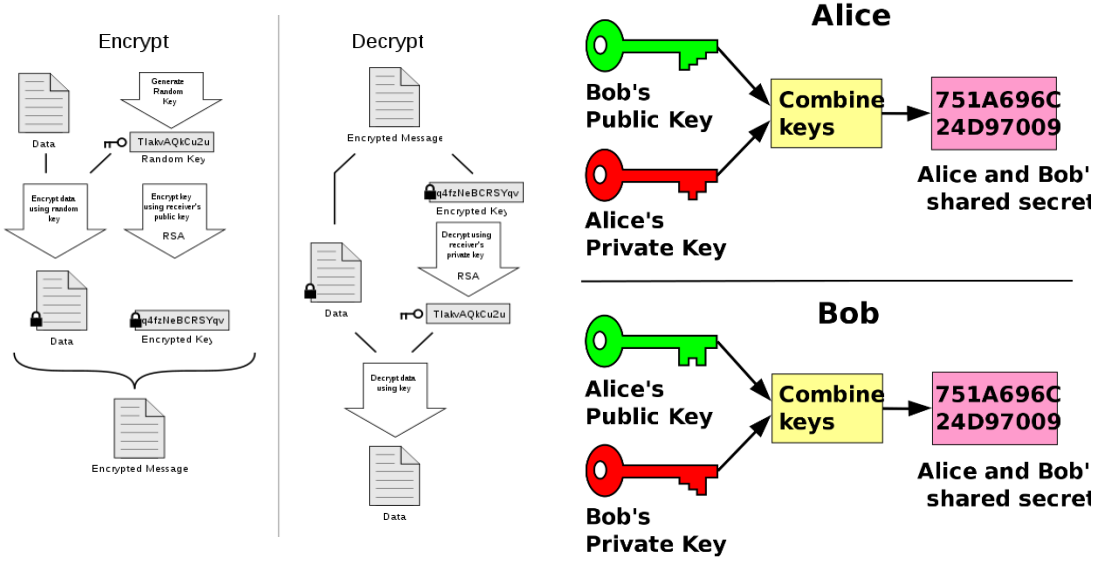
- يعرف بالتشفير اللامتماثل Cryptography Asymmetric تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاص Privet key، حيث أن المفتاح العام هولتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل.
- المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص كما في الصورة التالية:

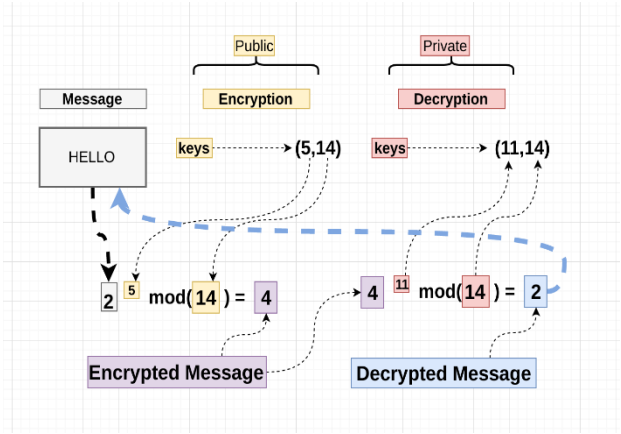
تشفير المفتاح العام:(اللامتماثل)



تشفير المفتاح العام:(اللامتماثل)

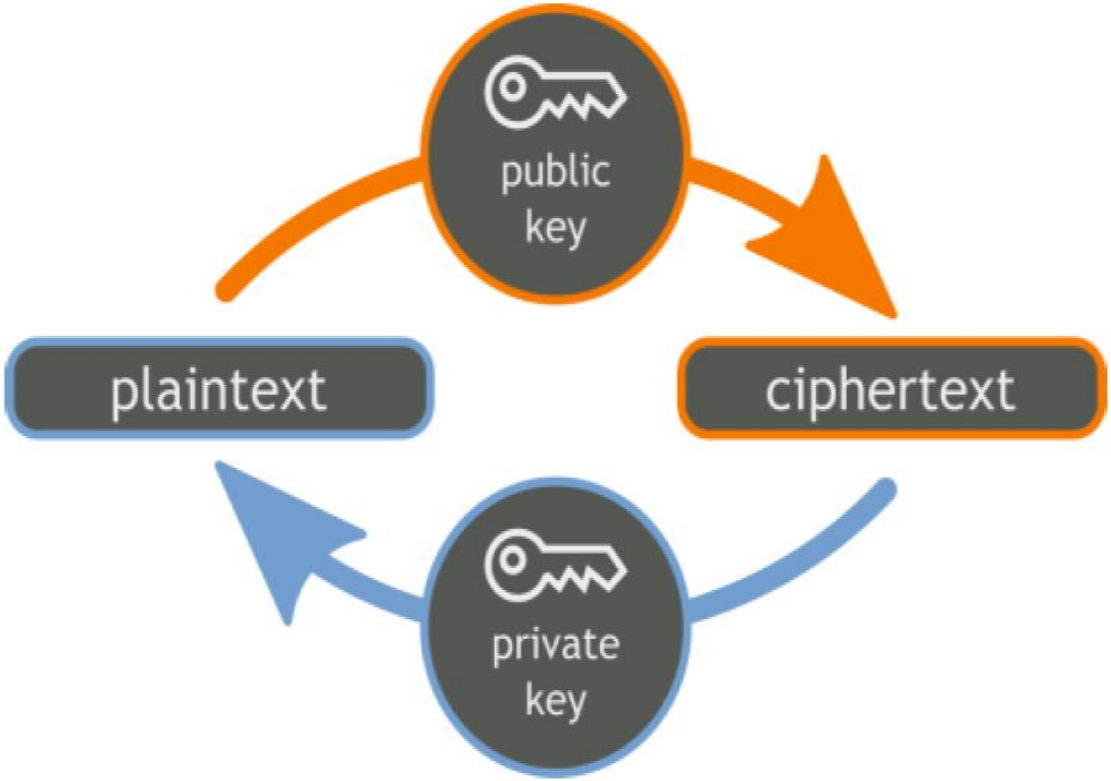
- PGP, DSA, Deffie-Hellman, Elgamal, RSA
- جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص.





مراحل التشفير

- التشفير يمر بمرحلتين رئيستين:

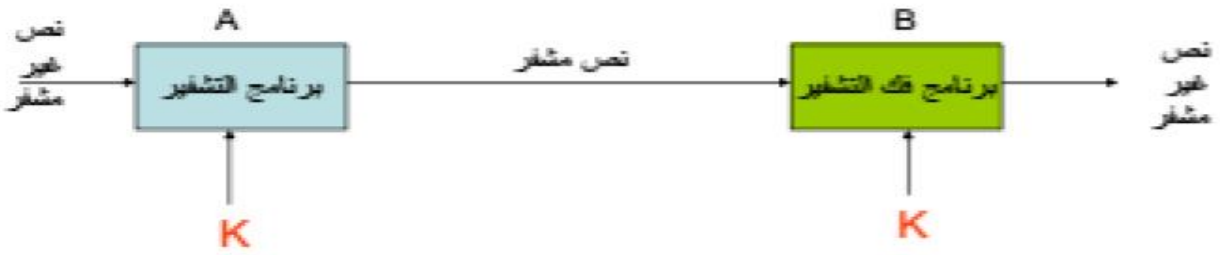


طرق التشفير

- الخطوات التي تتم بها خطوات التشفير بالمفتاح العام:

1. يرغب المرسل في إرسال رسالة مشفرة إلى المستقبل.
2. يقوم المرسل بإرسال الرسالة المشفرة باستخدام القنوات العادية في الاتصال.
3. يقوم المستقبل (المرسل إليه) بتلقي الرسالة وباستخدامه مفتاحه.

نظام تشفير المفتاح السري المتماثل (المشترك)



طرق التشفير

- Data Encryption Standard (DES)
- يستخدم مفتاح بطول 56 بت وبلوك بطول 64 بت.
- تم تطويره بواسطة IBM وتم اعتماده واستخدامه بواسطة NIST الجمعية الوطنية الأمريكية للمقاييس والتقنية.
- صمد على مدى 15 عام ثم توقف اعتماده نتيجة الشك في وجود بوابات خلفية في تصميمه لكن لم يثبت احد هذه الشكوك
- يمكن تكرار استخدامه على النص لزيادة قوته التشفيرية- مثلا في انظمة يونكس يتكرر استخدامه 22 مرة لحماية كلمات السر.

طرق التشفير

- خطوات التشفير من خلال المزج بين نظام المفتاح المتماثل والمفتاح العام:
  1. تشفير الرسالة الأصلية بمفتاح متماثل (الطريقة الأولى)
  2. تشفير المفتاح المتماثل (بالمفتاح العام للمرسل إليه) (المستقبل)
  3. يتم إرسال الرسالة المشفرة بالمفتاح المتماثل والمفتاح المتماثل المشفر بالمفتاح العام للمرسل إليه .
  4. يستقبل المرسل إليه المفتاح المتماثل المشفر بالمفتاح العام ويقوم بحل شفرة هذا المفتاح باستخدام المفتاح الخاص به ليحصل على المفتاح المتماثل المشفر به الرسالة الأصلية
  5. يقوم بإستخدام المفتاح المتماثل بعد فك تشفيره في فك الرسالة الأصلية المشفرة .

بروتوكولات التشفير

- في حالة الرغبة في إخفاء البيانات فهناك أكثر من بروتوكول يمكنك من هذا الأمر.
- هناك أيضا تشفير المتصفحات، كمتصفح جوجل كروم، وموزيلا فاير فوكس، وغيرها .
- أما عن الرغبة في تشفير خدمة ال Wi-Fi، فهذه الخدمة عبارة عن كنز من المعلومات المنتشرة بشكل لاسلكي، وبالطبع قراصنة الواي فاي منتشرون جدا.

الفيروسات

- فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات. وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة. والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.
- يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
- أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.
- يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة.

أنواع الفيروسات

- أولاً: فيروسات تقليدية Classic Virus و هي برامج هدفها تخريب النظام و إحداث أعطال و أخطاء فيه بشكل رئيسي و هناك نوع جديد من الفيروسات يستخدم أسلوب الإنحقان بالملفات حيث يضيف جزء من كوده البرمجي إلى الملف فيصيبه و يصبح جزء منه و بشكل عام تضع الفيروسات قيودا و تعديلات في الريجستري فمثلاً تمنع المستخدم من استخدام إدارة المهام و إظهار الملفات المخفية و ملفات النظام بطئ بسبب استهلاكها لموارد النظام و غيرها الكثير.

أنواع الفيروسات

- تقسم الفيروسات إلى :
  - File Viruses و تتبع واحدا على الأقل من هذه الأساليب لإصابة النظام :
    - فيروسات منحقنه تصيب الملفات التنفيذية و في هذه الحالة عندما يكتشفه مضاد فيروسات يعطيك خيار التصحيح Disinfect , Cure , Repair ,...etc حيث يختلف حسب نوع مضاد الفيروسات الذي تستخدمه و من أشهر هذه الفيروسات فيروس سالتي الشهير Sality و فيروس Mabezat و للأسف أكثر الفيروسات من هذا النوع.
    - فيرروسات تكرر الملفات الموجودة على الجهاز Duplicate Files حيث تمتلئ ذاكرة الجهاز بسبب تكرار الملفات (تخيل لديك ملفات و بيانات شركة و تملئ 75% من ذاكرة الجهاز فإذا بدء الفيروس بنسخ كل ملف مرة واحدة تكون النتيجة الجهاز لا يملك ذاكرة كافية) و لهذا تسمى هذه الفيروسات بفيروسات الشركات مثل فيروس Temp.exe.
    - هذه الفيروسات تعمل نسخ عن نفسها في مسارات مشهورة بالجهاز,%SystemRoot% ...etc %userprofile% , %Temp% %systemdrive%,

أنواع الفيروسات

- فيروسات تستعمل ميزات ملفات النظام
  - Boot sector viruses و هي فيروسات تصيب الملفات المسؤولة عن إقلاع الجهاز و النظام . فتضيف نفسها إلى ملفات الإقلاع و قد تغير مسار تلك الملفات . و لا تصيب إلا الأقراص المرنة .
  - هذه الفيروسات إنتشرت في التسعينيات من القرن الماضي و لكن مع تقدم معالجات 32 بت و تناقص استخدام الأقراص المرنة تضاءل عددها مع أنه من الناحية التقنية يمكن إنشاء هكذا فيروسات تعتمد على ال Cd و على الفلاشات .
  - Macro viruses و هذه الفيروسات تصيب ملفات محررات النصوص مثل MS Worde -MS Exel- Power Point و هذا النوع من الفيروسات غير منتشر و نادر. حيث بمجرد فتح مثل هذه الفيروسات تصاب الملفات الأخرى بهذا الجهاز. مثال عليها أحد الفيروسات ما أن تفتحه بالجهاز حتى تمحى كل ملفات الأوفس التي تعمل بالجهاز حتى و لو كانت مخزنة.
  - Script Viruses و هي فيروسات تستخدم الأكواد للغات رمزية (جافا سكريبت , فيجوال بيسك سكريبت ,Phpملفات باتش ,...الخ) و هي تصيب النظام و تؤدي إلى تحويل الأكواد إلى عمليات تخل بالنظام .

أنواع الفيروسات

- ثانياً: أحصنة طروادة Trojan ومن أشهر أنواعها Backdoors و هي الأخطر لأنها تأخذ صلاحيات مدير نظام و تعمل بسرية تامة و من دون علم المستخدم.
- و تستخدم شبكة محلية أو الإنترنت للتحكم بجهاز الضحية و تتبع سلوك أدوات مدير النظام RAT = Remote Administrator Tool و الفرق الوحيد بين التروجانات و برامج الإدارة هي أن التروجانات تنزل و تعمل بدون علم المستخدم بينما أدوات الإدارة تكون واضحة و تعطيك رسالة أنها تراقب النظام و هذا النوع يستخدم للتحكم بروتوكول TCP\IP و هو نفس البروتوكول المستخدم بالمسنجر و إدارة مقاهي الإنترنت و بعض البرامج و هذا النوع يتكون من جزأين الأول بجهاز الضحية يعمل بشكل خفي بحيث يتلقى الأوامر من المخترق و الثاني عند المخترق الذي بعث التروجان.

أنواع الفيروسات

- خطورتها تكمن في :
  - إرسال و إستقبال الملفات من و إلى جهاز الضحية
  - الدخول للملفات الخاصة و إمكانية حذفها و تعديلها
  - توجيه المستخدم إلى موقع إنترنت بدون إرادته و تغيير الصفحة الرئيسية أيضاً .
  - سرقة المعلومات الخاصة و كلمات السر
  - تشغيل البرامج و الأجهزة المرتبطة بالجهاز (طابعة أو كمرة ....الخ)
  - إعادة تشغيل الجهاز و إطفاءه
  - بيانات الدخول للإنترنت (رقم البطاقة و كلمة المرور للإنترنت)
  - كلمات السر للألعاب على الشبكات (بعض الألعاب على الشبكة تكون بمقابل مادي)
  - كلمات السر للإيميل و المواقع

أنواع الفيروسات

- General Trojans و هذا النوع يخرب الجهاز و يسرق البيانات من جهاز الضحية و أغلب مبرمجين البرامج الخبيثة يضيفون خصائص كثيرة لهذا النوع PSW Trojans و هو سارق كلمات السر حيث يقوم بفحص المواقع التي تحفظ بها كلمات السر و يأخذها ثم يرسلها للشخص الذي كونه . و بالعادة يسرق معلومات عن النظام و الرقم التسلسلي لنظام التشغيل (بالدول الغربية نظام التشغيل غالي فسرقة الرقم التسلسلي مهم جداً)
- Trojan Clickers و هذا النوع يقوم بتوجيه الضحية لموقع معين بدون إرادته و الهدف منه هو إما زيادة العدد للزائرين لموقع معين أو إستنفاذ حجم التبادل الشهري لموقع أو الهجوم على موقع أو مخدم معين بواسطة DOS Attack أو أخذ الضحية لموقع معين حيث يكون هذا الموقع مصاباً فيتم تنزيل فيروس أو برنامج أخر بجهاز الضحية.

أنواع الفيروسات

- قد تقوم هذه البرامج أيضا من منع المستخدم من الدخول إلى مواقع معينة كمواقع شركات الحماية و التحديث فلا يستطيع المستخدم تحديث مضاد فيروساته. Trojan Downloaders و هي برامج تتميز بصغر حجمها و وظيفتها تنزيل برامج أخرى (تروجانات أو فيروسات) إلى جهاز الضحية.
- فمثلا دمج أحدهم برنامج مكرك مع تروجان كامل (100 كيلوبايت) سيلفت الانتباه فيلجأ إلى دمجه مع برنامج صغير لا يتعدى 5 كيلوبايت وظيفته عند الإتصال بالإنترنت تحميل الملف الكبير من الإنترنت و فتحه بجهاز الضحية Trojan Droppers و هي برامج هدفها إخفاء البرامج الخبيثة عن أعين المستخدم أو عن مضاد الفيروسات كل ملف بالجهاز له توقيع رقمي يختلف عن غيره و مضاد الفيروسات يحوي بداخله تواقيع الفيروسات و البرامج الخبيثة (التحديث هو عملية إضافة تواقيع البرامج الحديثة المكتشفة إلى أرشيف البرنامج) فيقوم هذا النوع من البرامج بتشفير الكود البرمجي للبرنامج الخبيث و تغير توقيعه الرقمي فيصبح ملفا غير مكتشف بالنسبة لمضاد الفيروسات و يمر من قبضته.

أنواع الفيروسات

- و تحوي هذه البرامج على خيارات لإيهام الضحية أن البرنامج الذي تم إخفاؤه ملف سليم عن طريق تشغيل تطبيق أخر أو إظهار رسالة خطأ توهم المستخدم أن الملف سليم.
- مثال : دمج فيروس مع صورة فعند الضغط على البرنامج المشفر يظهر للضحية صورة أو دمج فيروس مع برنامج مسروق فيضغط الضحية على ملف التنصيب و ينصب البرنامج بشكل طبيعي و لا يدري أنه ينصب و بشكل خفي في جهازه فيروساً Trojan Proxies و هي برامج تستخدم لتحويل جهاز الضحية لبروكسي يمكن الذي ارسل التروجان إلى إستخدامه للدخول للإنترنت بشكل متخفي. و هذا النوع منتشر بكثرة بين الذين يستخدمون الرسائل المزعجة لكي يتمكنوا من الدخول لأعداد كبيرة من الأجهزة و بشكل متخفي لإرسال رسائل من أجهزة غيرهم. Trojan Spies و هذا النوع يستخدم للتجسس على نشاطات الضحية (ليس فقط كلمات السر كما في PSW Trojans بل على نشاطات أخرى) مثل تصوير سطح المكتب أو صور من الكمرة أو أية نشاطات يقوم بها المستخدم Trojan Notifiers و هي فقط لإعلام المخترق الذي أرسل التروجان بنجاح إصابة الجهاز بالبرنامج الخبيث حيث ترسل للمخترق معلومات عن الجهاز و IPو المنافذ المفتوحة.

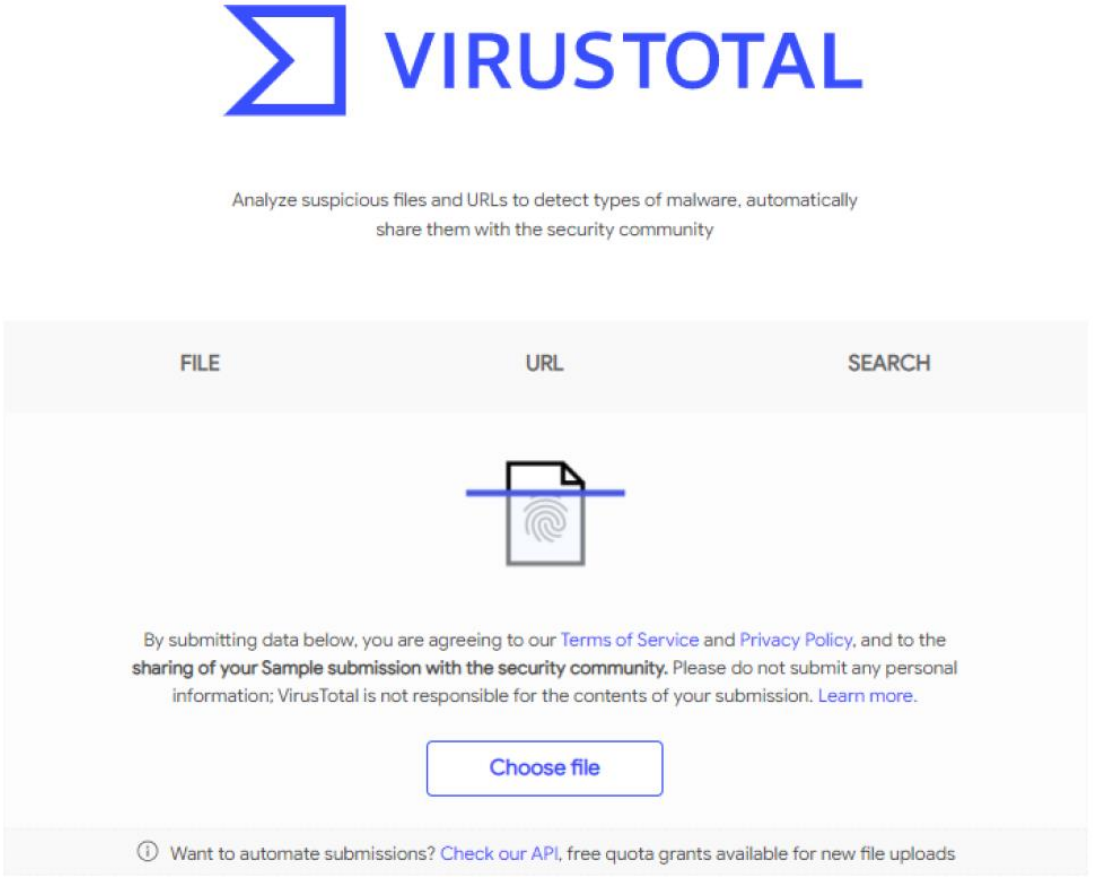
أنواع الفيروسات

- كثير من Backdoors و PSW Trojans ترسل مثل هذه التنبيهات أيضاً. Rootkits و هي برامج تقوم بإخفاء نشاطات التروجانات عن البرامج و لكن بطريقة لا تثير الريبة أبداً حيث تبقى مثلا إدارة المهام فعالة و لكن لا تظهر فيها أية نشاطات للتروجانات و لا تظهر بلوحة العمليات و تقوم بإخفاء نفسها بمفاتيح بالريجستري و قد تقوم أيضا بسرقة المعلومات الخاصة كسارق كلمات السر و تتميز هذه البرامج أنها تضيف نفسها كملفات نظام و تأخذ حقوق المدير. ArcBombs و هي ملفات مؤرشفة صممت لتخريب الملفات المضغوطة حيث تتضاعف أحجامها تلقائيا ألوف المرات فتتخرب و يمتلئ الجهاز بملفات فارغة تسمى قنابل الهواء خطورتها تكمن في إصابة خوادم الإنترنت و مخدمات البريد الإلكتروني.
- هناك ثلاث أنواع لها الأول :
  - النوع الأول يملئ الملفات المضغوطة بمعلومات و بيانات مكررة
  - النوع الثاني يخرب الملفات المضغوطة
  - النوع الثالث يضغط الملفات بشكل صغير جدا فمثلا حجم 5 جيجا يصبح 200 كيلو بايت

سبل الحماية من الفيروسات

- نعرض لكم بعض من المنصات المتوفرة أون لاين أو عبرالأنترنت المتخصصة لتحليل الروابط والملفات لأكتشاف التهديدات والفيروسات.
- تنوية: نأمل عدم تحميل أي ملفات حساسة لدى الجهة الخاصة بك في المواقع التي تتيح خدمة الفحص أون لاين أو عبرالأنترنت.
- علماً أنه يوجد عدد لا حصر له من أدوات فحص الفيروسات والروابط، مثل:
  - Kaspersky Threat Intelligence Portal
  - Cuckco
  - The Sleuth Kit(TSK)
  - Strings Utility
  - F-Secure
  - Volatility
  - Rekall

VirusTotal

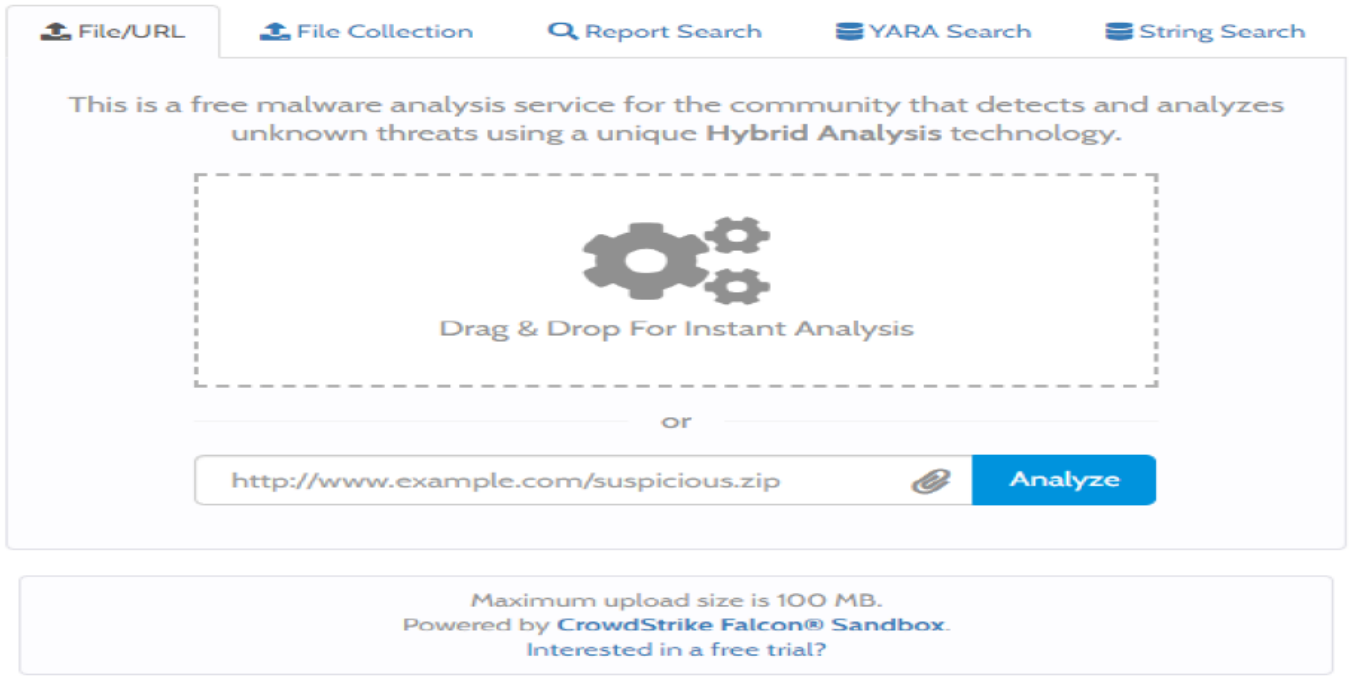


https://www.virustotal.com

Anyrun

https://app.any.run

HyberAnalsis



https://www.hybrid-analysis.com/

استـراحــة

الشبكات

- الشبكات بشكل عام هي وصل الحواسيب الموضوعة على مساحة محددة من أجل الاستخدام المشترك للمعلومات .الشبكات تقدم إمكانيات مذهلة في مجال تبادل المعطيات ومجال التعامل مع الملفات لعدد من المستثمرين بآن واحد معاً ، بالإضافة إلى بساطة المشاركة في الملفات FILES يمكن لمستثمري الشبكة أن يتشاركوا في الطابعات PRINTERS وسواقات الأقراص الليزرية CD-ROM والمودم MODEM وحتى جهاز الفاكس FAX
- وعموماً يقصد بالشبكة التفاعل المتداخل بين أجهزة الكمبيوتر أي كيف تعمل الأجهزة فيما بينها ضمن شبكة اتصال لتحسين قدراتك في إنجاز الأمور. وشبكات الاتصال وضعت عموماً للمشاركة في أمور مثل معالجة النصوص وبرامج أوراق العمل وفي الطابعات وفي الربط على أجهزة كمبيوتر وشبكات واسعة وأنظمة البريد هي وظيفة شبكة الاتصال.

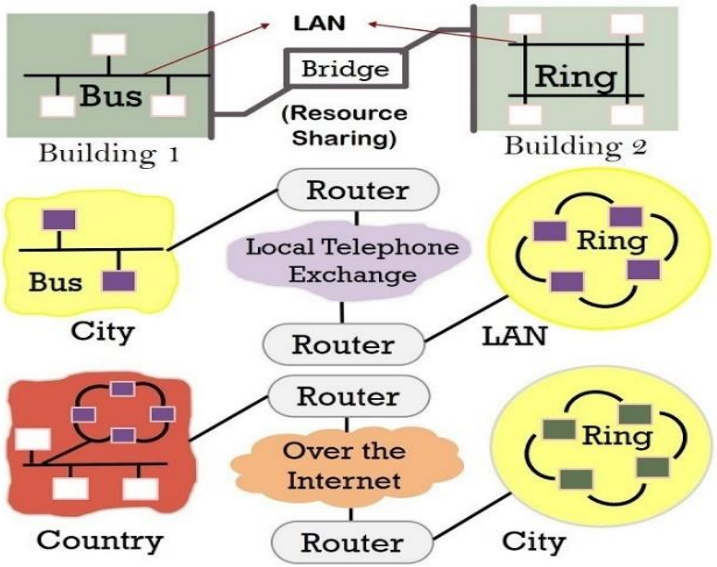
أنواع الشبكات

- هنالك ثلاثة أنواع رئيسية من الشبكات :
  1. الشبكات الواسعة WIDE AREA NETWORKS (WAN)
  2. الشبكات المحلية LOCAL AREA NETWORKS (LAN)
  3. الشبكات العنكبوتية MEDIUM AREA NETWORKS (MAN)

LAN

MAN

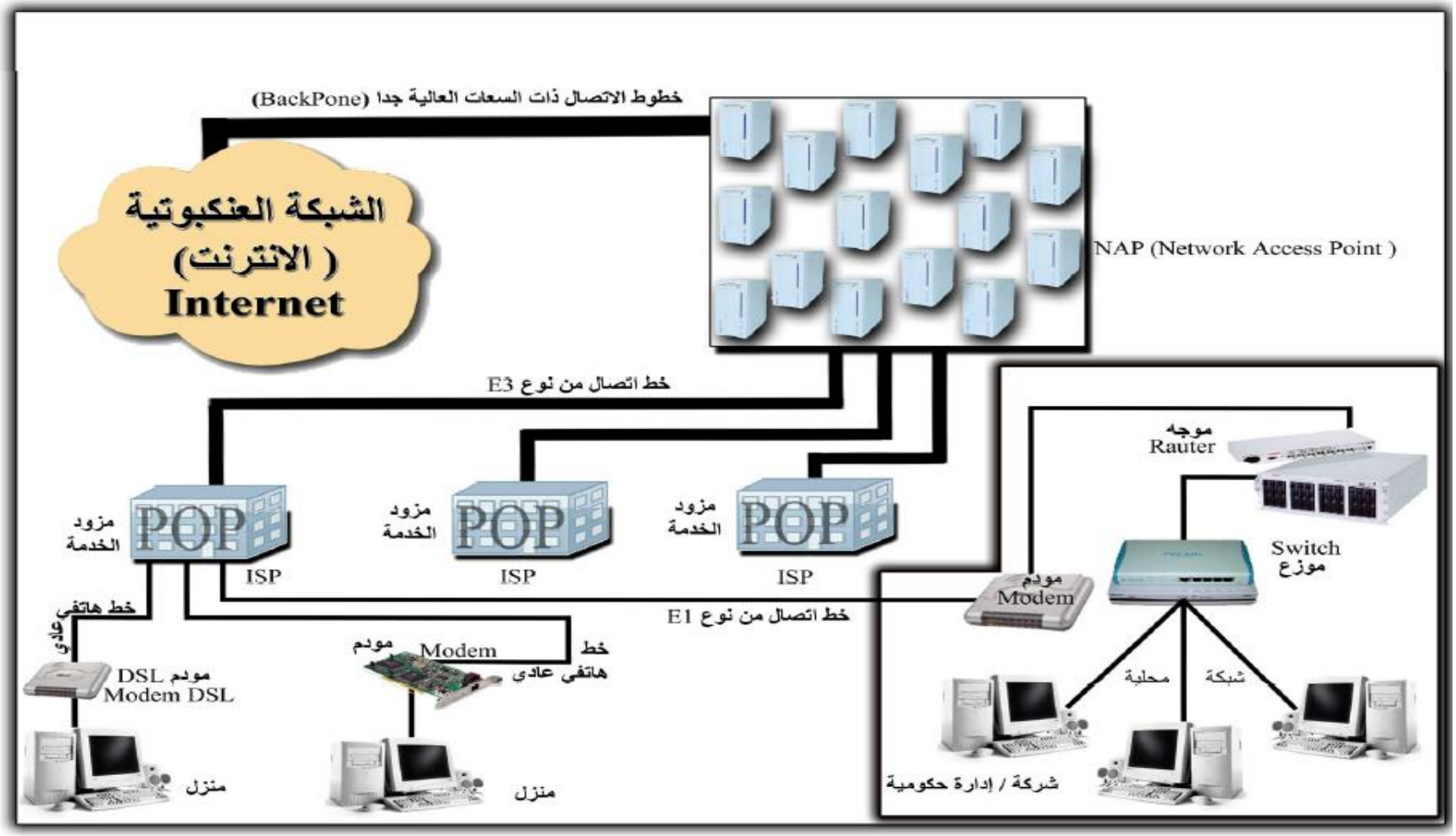
WAN



شبكة الحاسبات

- مجموعة من الحاسبات التي تتوزع على مواقع مختلفة و تربط بينها وسائل الاتصالات المختلفة و تقوم بجمع و تبادل البيانات الرقمية و الاشتراك في المصادر المرتبطة بها .
- و من هنا يتضح لنا أن شبكة الحاسب تقوم بارسال البيانات الرقمية من اجهزة الحاسبات إلى وحداتها الطرفية و بين اجهزة الحاسبات بعضها البعض باستخدام وسائل الاتصال المختلفة كالاقمار الصناعية و الكيابل المحورية و الاسلاك الهاتفية.

طرق الاتصال بشبكة الإنترنت

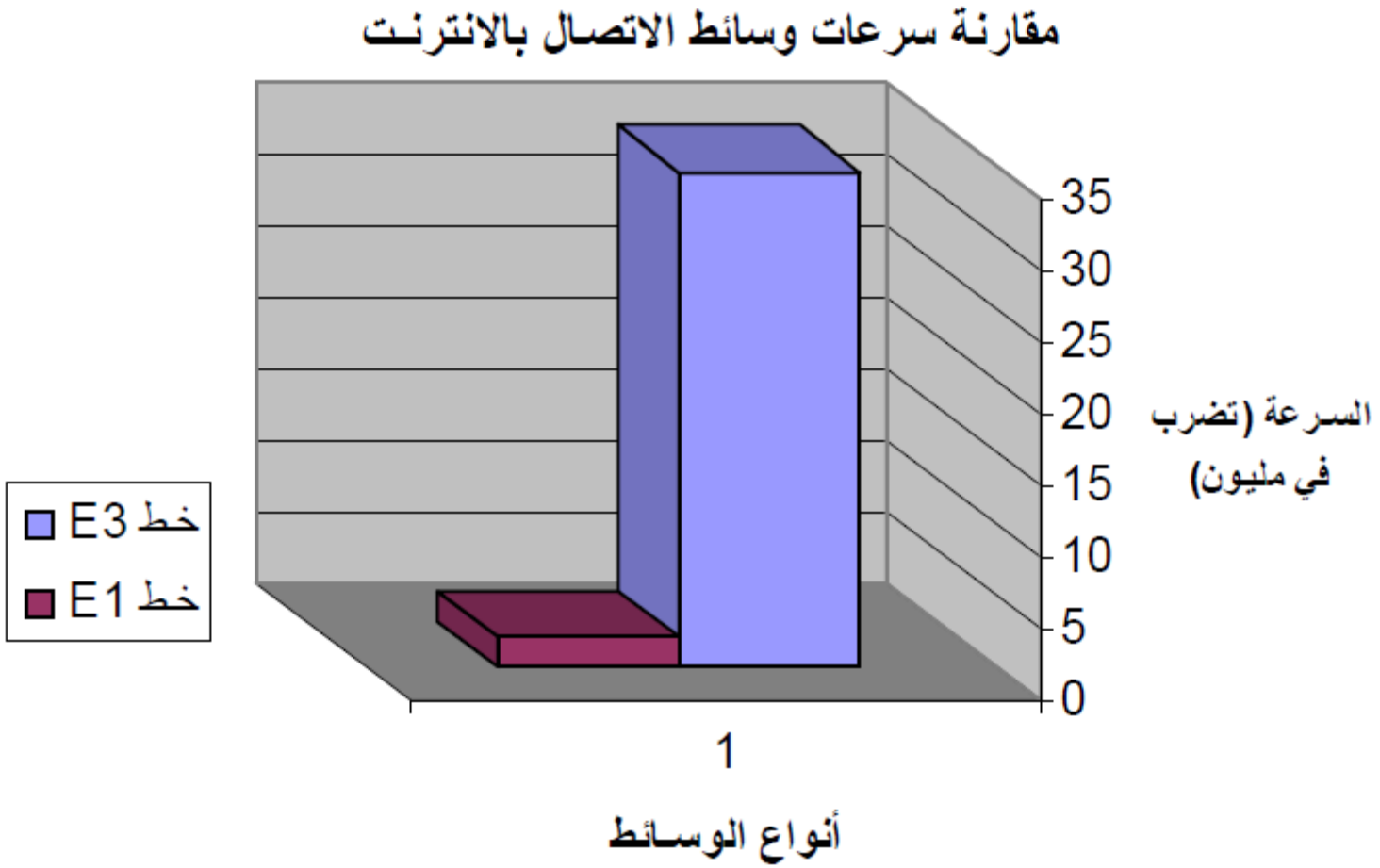


طرق للاتصال بشبكة الانترنت

طرق الاتصال بشبكة الإنترنت

- كما هو موضح بالشكل السابق فأن طرق الاتصال بشبكة الإنترنت ما أن يكون باستخدام جهاز مودم وخط هاتفي، وهذا النوع أقل أنواع الاتصال كلفة، لكنه أبطؤها، فقط تصل سرعته إلى (56 ألف نبضة في الثانية) كحد أقصى، وإما أن يكون باستخدام تقنية DSL التي تستخدم فيها أجهزة خاصة تسمى DSL Modem عندها القدرة على نقل البيانات بسرعات عالية (تتراوح بين 64 ألفا إلى 52 مليون نبضة في الثانية)، على خطوط الهاتف نفسها، وفي كلتا الطريقتين يكون مزود الخدمة بوابتك التي تلج منها إلى عالم الإنترنت.
- أما الشركات، والدوائر الحكومية فإنها غالبا ما تمتلك شبكات داخلية ترتبط بمزود الخدمة بواسطة خطوط اتصال خاصة تتميز بسرعة نقل كبيرة . ومن أمثلة هذه الخطوط ما يعرف باسم E1 الذي يعطي سرعة تصل إلى (2 مليون نبضة في الثانية)، و E3 الذي يعطي سرعة تصل إلى (34,4 مليون نبضة في الثانية) كما في الشكل التالي وهذه الخطوط السريعة تتصل بمزود الخدمة الذي يصلها بدوره بشبكة الإنترنت.

طرق الاتصال بشبكة الإنترنت



أمن شبكات المعلومات

- الإنترنت سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى جهازك. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات.
- إن المعلومات أو الأنظمة التي يحتفظ بها تكون عرضة للهجوم من جبهتين مختلفتين : الجبهة الداخلية والجبهة الخارجية، ولشدة خطر الأولى فإننا سنناقشها أولاً.

أمن شبكات المعلومات

- أولاً: المهاجمون من الداخل:
- لعله من المناسب أن نحدد ما نعني بالمهاجمين من الداخل، إنهم أولئك الأفراد الذين ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية إلى حماية أنظمة المعلومات التي تستخدمها تلك الجهة. والمهاجمون من الداخل كانوا دوماً الخطر الذي تواجهه أي جهة، مهما كانت، سواء كانت تلك الجهة شركة أو منظمة أو حتى دولة. ولقد فاقم اختراع الحاسوب والتقنيات التي ظهرت إلى الوجود بعد ذلك الخطر الناجم عن الهجمات التي قد يشنها العدو الداخلي ضد الجهة التي ينتمي إليها ظاهراً.
- يظهر تقرير صدر في الولايات المتحدة الأمريكية عام 2003م أن 7.36 من الجهات التي شملتها دراسة مسحية أجراها مكتب التحقيق الفيدرالي FBIمشاركة مع معهد أمن الحاسوب Computer Security Institute، أو ما يعرف اختصارا باسم CSI، يعتبر المستخدمين من داخل تلك الجهات خطرا حقيقيا على أنظمة المعلومات التي تستخدمها تلك الجهات.

أمن شبكات المعلومات

- ولكن بسبب الضجة الإعلامية التي تثار عادة عندما يكون الهجوم على جهة ما قادما من خارجها مثل الإنترنت، فإن الشركات والدوائر الحكومية تولي جل اهتمامها لتحصين أنظمة معلوماتها ضد الهجمات القادمة من الخارج ، وغالبا ما يكون هذا على حساب الاستعداد لصد الخطر القادم من الداخل الذي يحدث غالبا دمارا باهظ التكاليف.
وبحسب تقديرات معهد أمن الحاسوب CSI، فإن معدل تكاليف الهجوم القادم من الداخل هو 2.7 مليون دولار للهجوم الواحد ، بينما لا يزيد معدل الهجوم الواحد القادم من الخارج عن 57 ألف دولاراً.
- دوافع الهجوم من الداخل: هناك أسباب عديدة قد تدفع الإنسان لشن هجوم ضد أنظمة معلومات الجهة التي يعمل فيها، ومن أهم هذه الأسباب ما يلي:

أمن شبكات المعلومات

- عدم الرضا: أيا كانت مسببات عدم الرضا هذا، إلا أن الواقع يشهد أن التقنية الحديثة جعلت من مهاجمة نظم المعلومات أمرا يشعر بالانتقام للذات، ويبعث البهجة في نفس الشخص الذي نفذ الهجوم.
- إثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم إلكتروني : هناك طائفة عريضة من الناس يداخلهم الشعور بالفخر إذا تمكنوا من اختراق مواقع على شبكة الإنترنت، أو وصلوا إلى قواعد بيانات محمية، ويجدون في ذلك أمرا يباهون به أقرانهم. والحقيقة أن كثيرا من هؤلاء قد لا يملكون المعرفة الحقيقية لشن الهجمات الإلكترونية، ولكن هناك مواقع على شبكة الإنترنت أمن المعلومات بلغة ميسرة توفر برامج يمكن استخدامها في مهاجمة أنظمة المعلومات، ولا يتطلب استعمالها كبير معرفة بالحاسوب أو الشبكات.
- تحقيق المكاسب المالية: قد يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها السرقة معلومات سرية يستخدمها لاحقا لابتزاز الجهة لدفع فدية مالية.

أمن شبكات المعلومات

- حجم التهديد الداخلي: إن الهجوم من الداخل يمكن أن يخل بأي من مكونات أمن المعلومات التي تحدثنا عنها سابقا، أي أنه يمكن أن يلحق الضرر بسرية المعلومات أو سلامتها، أو يعيق الوصول إلى المعلومات أو يمنعه. وأسوأ من هذا أن المهاجم من الداخل إذا كان ماهراً فإنه بمقدوره أن يطمس أي آثار تدل على ارتكابه اللهجوم .
وأهم جوانب الأخطار التي تأتي من الهجوم الداخلي هي :

1. مهاجمة الشبكة الداخلية للمنشأة التي يعمل فيها.
2. مهاجمة المعلومات بالسرقة أو التغيير أو الحذف.
3. فتح ثغرات في أنظمة الحماية التي وضعتها الجهة التحصين أنظمة المعلومات فيها.

أمن شبكات المعلومات

- ثانياً: المهاجمون من الخارج:
- نظراً لحجم التغطية الإعلامية التي تعقب الهجمات من الخارج فإننا نفترض أنكم قد سمعتم كثيراً مما قيل وكتب عن هذا الصنف، و بعض بواعث هذا النوع من الهجمات مماثلة للصنف السابق، كما أن هناك بواعث أخرى، منها: سعي المهاجم من الخارج لتحقيق أهداف سياسية أو دينية أو تجارية. ومن بواعث هذا النوع من الهجمات التجسس الصناعي أو التخريب.

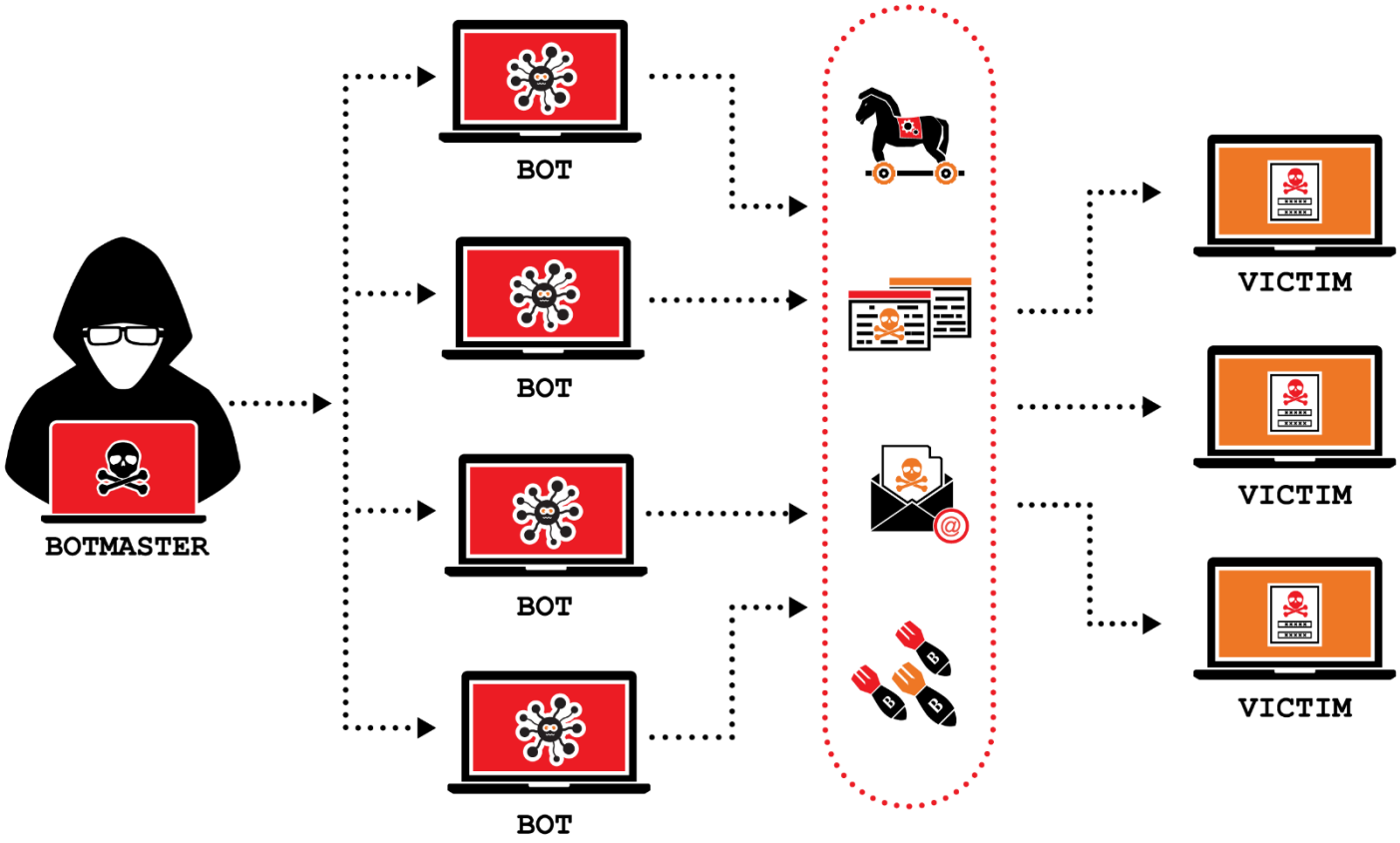
المخاطر الشبكة المختلفة وسبل الحماية منهاً

- تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة. وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.

المخاطر الشبكة المختلفة وسبل الحماية منهاً

- وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية DoS تستهدف إبطا او شل حركة مرور البيانات عبر الشبكة.
- كما أنه من خلال الهجمات الإغراقية الموزعة DDoS، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي سيطر عليها للهجوم على كمبيوتر أو كمبيوترات أخرى. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة DDoS في أحد أجهزة الكمبيوتر مستخدماً حساباً مسروقاً. إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

المخاطر الشبكة المختلفة وسبل الحماية منهاً



سبل الحماية أمن الشبكات

- إن الفوائد والخدمات التي جاءت بها شبكة الإنترنت لم تأت خلوا من المنغصات، فراجت سوق الطفيليين Hackers الذين لا هم لهم سوى التلصص على معلومات الآخرين. كما ظهر أناس يستمتعون بإلحاق الأذى بالآخرين، إما بحذف وثائقهم المهمة، أو العبث بمحتوياتها ، أو نشر البرامج السيئة Malware مثل الديدان ، والفيروسات ، وأحصنة طروادة وغيرها.
- والمقاومة تلك الأخطار والحد منها ظهرت تقنيات ومفاهيم متعددة ، من أكثرها انتشارا جدران الحماية Firewalls التي تسمى أيضا الجدران النارية. و لتقريب المعنى للأذهان نقول إن جدار الحماية نظام مؤلف من برنامج software يجري في حاسوب ، وهذا الحاسوب قد يكون حاسوبا عاديا ، مثل الحاسبات الشخصية ، أو حاسوبا بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية . وفكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس، وتمنع مرور آخرين، بناء على تعليمات مسبقة.

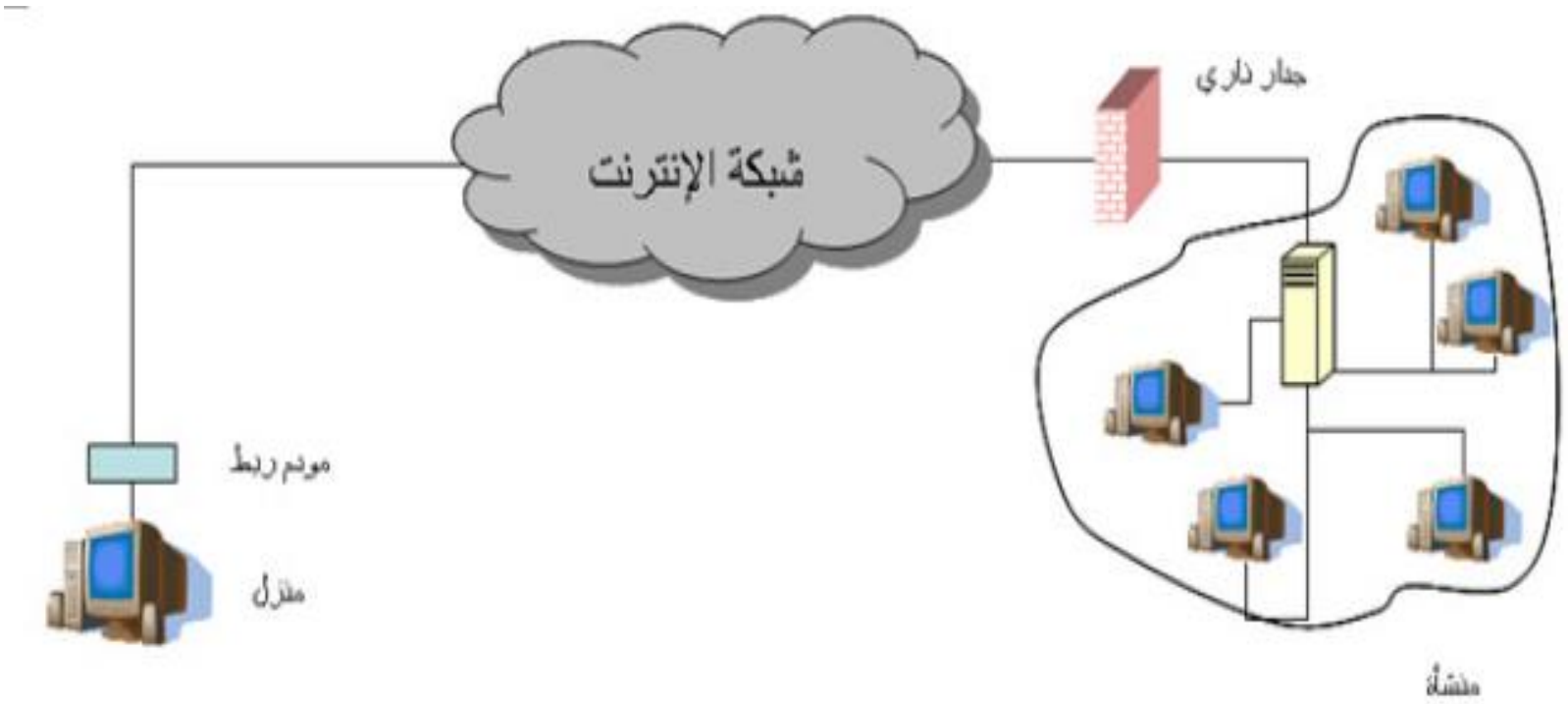
سبل الحماية أمن الشبكات

- الحصول على جدار حماية ناري Firewall
- جدار الحماية الناري من الإنترنت هو برنامج أو جهاز يقوم بفرز وتصفية الفيروسات والديدان والمتسللين والمعتدين الذين يحاولون الوصول إلى جهازك عبر الإنترنت. ويعتبر تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الكمبيوتر لديك هو القيام بتركيب جدار حماية ناري قبل الدخول إلى الإنترنت للمرة الأولى والإبقاء عليه عاملاً في كافة الأوقات.
- يمكنك الحصول على جدار حماية ناري لجهازك من محلات الكمبيوتر أو من خلال الإنترنت. علما أن بعض أنظمة التشغيل مثل ويندوز إكس بي مع الحزمة الخدمية/الإصدار-2 Service Pack2 ونظام التشغيل ماكنتوش MacOS X يوجد من ضمنها جدار حماية ناري.

سبل الحماية أمن الشبكات

- ولتوفير بعض الحماية لنفسها تقوم المنشآت بوضع جدار حماية لعزل شبكتها الداخلية عن شبكة الإنترنت ، كما يوضح الشكل التالي. بيد أن هذا العزل لا يمكن أن يكون كليا ؛ وذلك للسماح للجمهور بالاستفادة من الخدمات المقدمة، وفي الوقت ذاته منع الطفيليين والمخربين من الدخول، وتتاح من خلال البرنامج الموجود في جدار الحماية مراقبة المعلومات بين الشبكة الداخلية للمنشأة والعالم الخارجي. ولتحقق الغاية من جدار الحماية فإنه لا بد من وضعه في موقع استراتيجي يضمن ألا تخرج المعلومات أو تدخل إلى الشبكة الداخلية إلا عن طريقه.

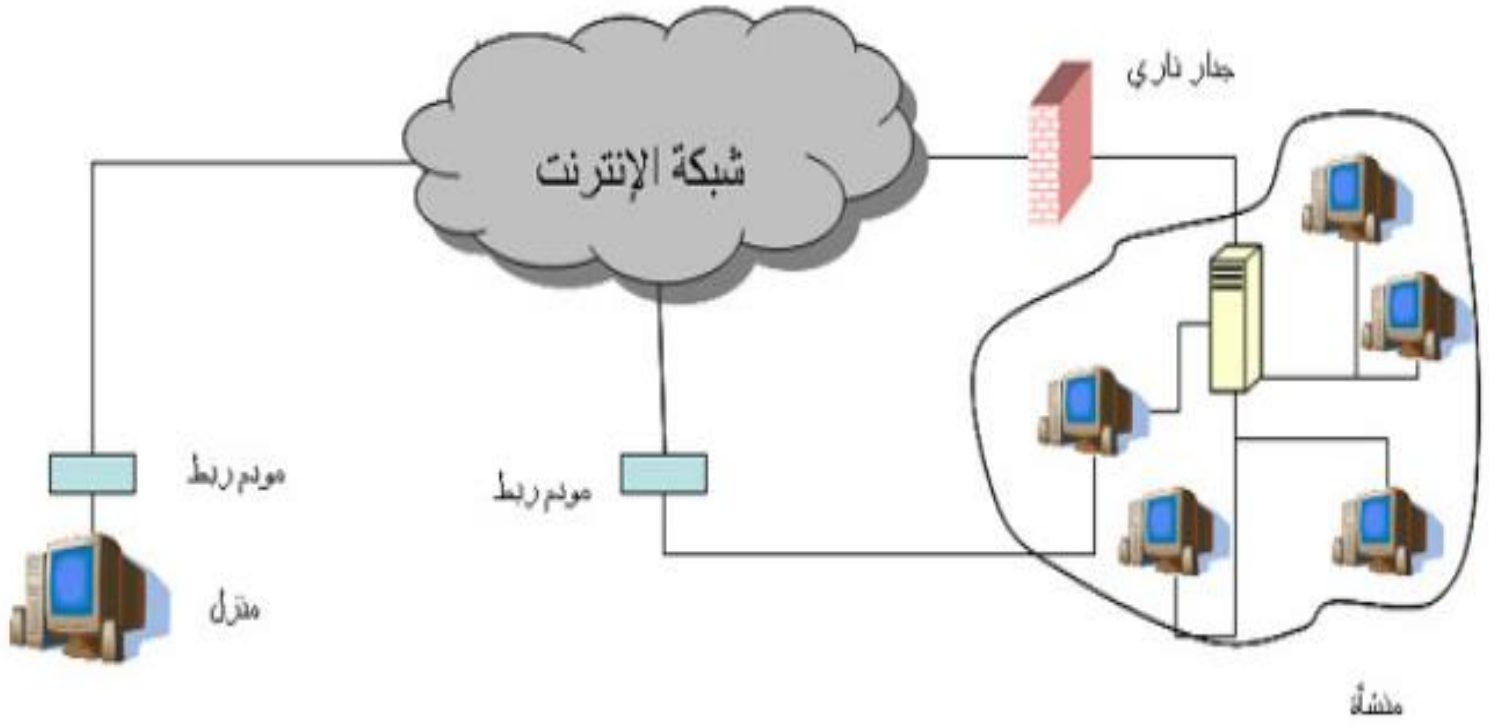
سبل الحماية أمن الشبكات



سبل الحماية أمن الشبكات

- ولذلك فإن الوضع الموضح في الشكل التالي غير مقبول عند المختصين في مجال أمن المعلومات ؛ لأن الوصول للشبكة الداخلية ممكن عن طريق الاتصال بجهاز المودم الذي يشكل في هذه الحالة بوابة خلفية يلج المتطفلون والمخربون عبرها.

سبل الحماية أمن الشبكات



سبل الحماية أمن الشبكات

- برامج مراقبة بيانات الشبكة Packet Sniffers
- طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

أنواع جدران الحماية

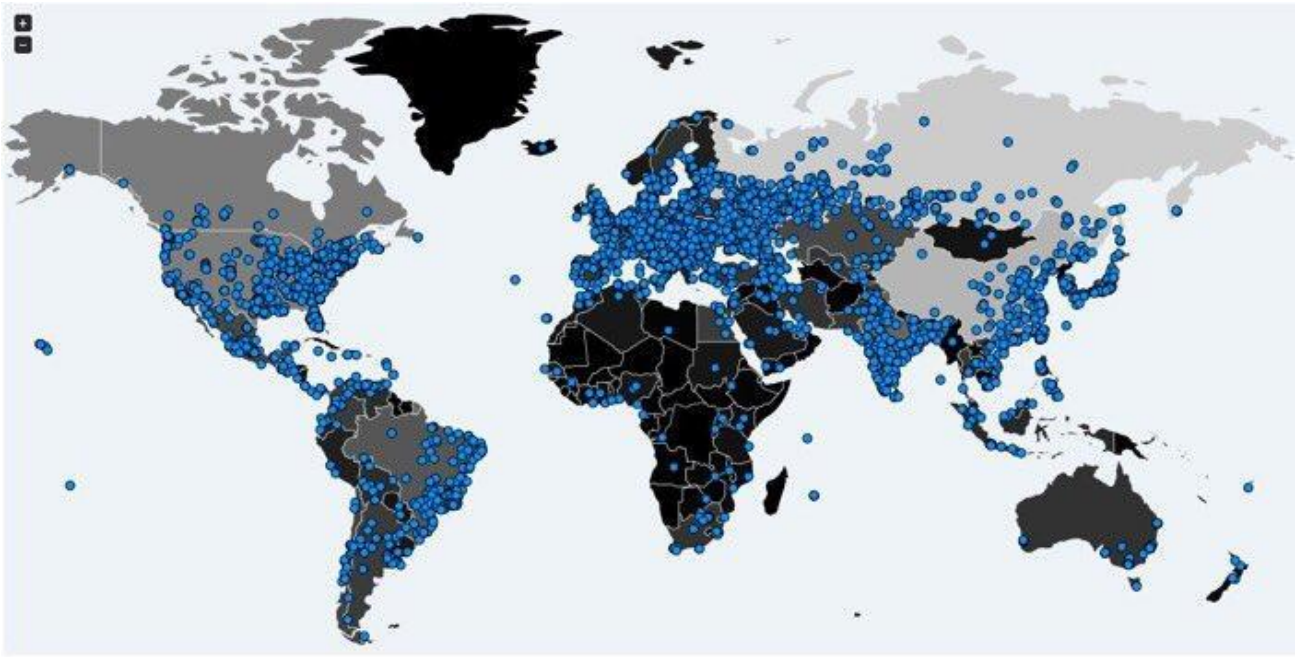
- يمكن تصنيف جدران الحماية من حيث الجهة المستفيدة منها إلى ما يلي :
- أولاً: جدران نارية لحماية المنشآت الكبيرة: وهذا النوع توفره شركات كبرى متخصصة مثل CISCO و Nortel و Symantec وغالبا ما توفر الشركة المصنعة أنواع متعددة من جدران الحماية تتفاوت من حيث سرعتها والخدمات التي تقدمها. وهذا النوع من جدران الحماية يتميز بما يلي:
  - إن جدار الحماية يكون غالبا- في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة ، أي أنه ليس مجرد برنامج يعمل في جهاز حاسوب عادي.
  - تعدد الخدمات التي يقدمها جدار الحماية، مثل: غربلة المظاريف ، والحماية ضد الفيروسات، وحماية البريد الإلكتروني، والتشفير.
  - تشغيل جدار الحماية يحتاج إلى مهارات فنية متقدمة.
  - ارتفاع كلفة الشراء والتشغيل.

أنواع جدران الحماية

- ثانياً: جدران نارية لحماية المنشآت الصغيرة : و هذا النوع يشبه سابقه في كونه جهازا مخصصا قائما بذاته ، إلا أنه لا يجاريه من حيث سرعة معالجة البيانات، أو تعدد الخدمات المقدمة، ولهذا فإنه أقل سعرة. من سابقه.
- ثالثاً: جبران نارية لحماية الأجهزة الشخصية : جدران الحماية هذه في أغلبها ما هي إلا برامج تحمل في الحاسوب الشخصي، بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب أو الداخلة إليه. وفي هذا المجال أيضا يتنافس عدد من الشركات على السوق الكبير لجدران الحماية الشخصية.

تمرين

- برأيك هل توجد دول تتعرض للاختراق الآن؟
- قم بزيارة هذا الرابط أدناة



Kaspersky Cyberthreat real-time map: https://cybermap.kaspersky.com/

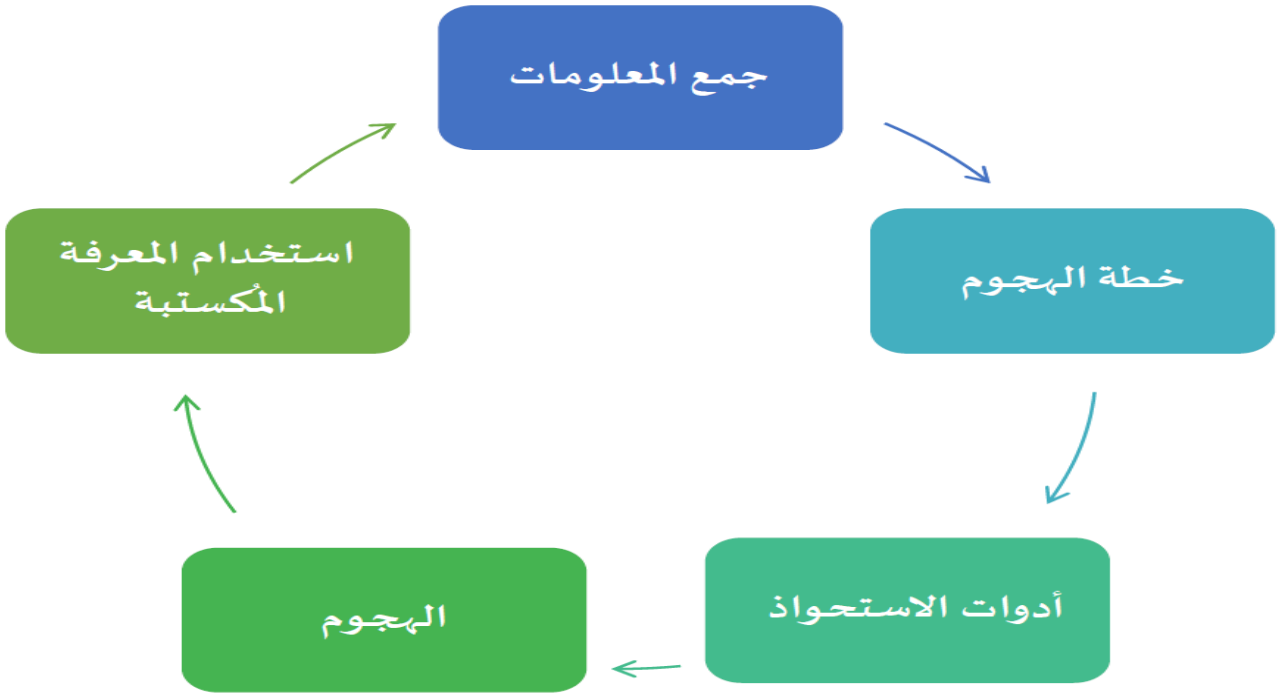
استـراحــة

الهندسة الاجتماعية

- استعرضت بعض الدراسات والأبحاث موضوع الهندسة الاجتماعية كعلم يتعرض إلى بيان كيفية تأثيره على عقول البشر وتغير بعض المفاهيم لديهم والتغريرهم من خلال استخدام أدوات ووسائل عدة.وتم تعريفها من قبل البعض تعريفا اجتماعية وتعريفة أمنية كالتالي:
- تعرف الهندسة الاجتماعية اجتماعية على أنها التأثير على مجمل السلوك الاجتماعي، ونمط الحياة والتفكير للمجتمع برمته، حيث يسعى المهندس الاجتماعي في هذه الحالة إلى تغيير سلوك الأفراد وطريقة تصرفهم، وأسلوب تفكيرهم، من اجل الوصول إلى الهدف الذي يرنو إليه.
- أمنيا: يشير مصطلح الهندسة الاجتماعية أمنية إلى التأثير على الآخرين، والتلاعب بهم لغرض دفعهم للكشف عن معلومات شخصية، ومثل هذا الاستخدام للهندسة الاجتماعية يندرج تحت ما يعرف بخدعة أو حيلة
- كما عرفت انها: فن الوصول إلى المباني أو الأنظمة، أو البيانات عن طريق استغلال علم النفس البشري بدلا من اختراق أو استخدام تقنيات القرصنة التقنية.
- ما المهندس الاجتماعي فإنه يعيش بقدرته على التعامل مع الناس في القيام بالأشياء التي تساعده على تحقيق هدفه، ولكن النجاح في هذا الأمر يتطلب غالباً قدرا كبيرا من المعرفة والمهارة في التعامل مع أنظمة الكمبيوتر وشبكات الهاتف.

الهندسة الاجتماعية

- كيف تعمل الهندسة الاجتماعية:
- يقوم عمل الهندسة الاجتماعية على ما يلي:

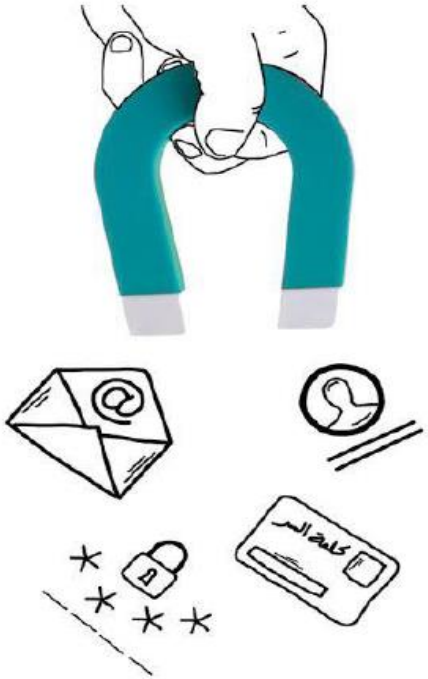


الهندسة الاجتماعية

- البرامج والتقنيات التي تساعد الأشخاص الذين يسعون للحصول على المعلومات وبث الإشاعات للوصول إلى المعلومة التي يريدون استغلالها ومن أمثلة ذلك:
  - الاحتيال الإلكتروني (Phishing)
  - الاحتيال الصوتي (Vising)
  - الرسائل الاقتحامية المزعجة (Spam)

الهندسة الاجتماعية

- الأساليب التي يتم استخدامها في الهندسة الاجتماعية يفكر المهاجمون وبشكل مستمر بأساليب جديدة لخداع الضحايا ومن أشهر الأساليب المتبعة في مثل هذا النوع من الاختراق ما يلي:
  - الهاتف.
  - البحث في المهملات.
  - الهندسة الاجتماعية.
  - استغلال الشائعات.
  - استغلال عواطف الضحية وطباعه الشخصية.
  - استغلال المواضيع الساخنة.
  - استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية.
  - انتحال الشخصي.
  - استغلال الشمعة الجيدة لتطبيقات معينة.
  - التصيد الاحتيالي



الهندسة الاجتماعية

- كيف نحمي أنفسنا من الهندسة الاجتماعية؟
- لحماية أنفسنا من الهندسية الاجتماعية، علينا اتباع ما يلي:
  - انظر دائما للعنوان URL : حينما تفتح صفحة وتوشك على كتابة كلمة مرورك تأكد دائما من عنوان الصفحة، عليك أن تفهم بنية العناوين الإلكترونية لتتأكد أنك على الموقع الصحيح والرسمي. أمثلة على روابط مسممة: facebook.co.com موقع مشبوه، الموقع الحقيقي هو facceboook.com
  - هل تلقيت بريدا إلكترونيا من شركة معروفة؟ تأكد أنه من العنوان الرسمي. استخدم المخترقون في عملية نايل فيش عناوين بريد إلكتروني تنتهي بـ@gmail.com على سبيل المثال dropbox.noreply@gmail.com وبالطبع فإن موقع دروب بوكس لن يرسل لك رسالة من بريد إلكتروني نطاقه gmail، ولكنه سيرسل من noreply@dropbox.com

الهندسة الاجتماعية

- لن يرسل لك فيس بوك رسالة لتغيير كلمة سرك عبر فيسبوك ماسنجر.
- عدم مشاركة أي معلومات أو أي بيانات شخصية مع أي جهة.
- عدم فتح مرفقات البريد الإلكتروني من أشخاص غير معروفين.
- العمل على تأمين الهاتف الذكي أو الحاسب المحمول.
- حذف أي شخص يطلب الحصول على معلومات مالية أو كلمات مرور.
- رفض طلبات المساعدة أو عروض المساعدة.
- تأمين أجهزة الكمبيوتر الخاصة بك: تثبيت برامج مكافحة الفيروسات.

جوانب الهجمات بأسلوب الهندسية الاجتماعية

- يرى بعض الباحثين أن الهجمات باستخدام أسلوب الهندسية الاجتماعية يمكن أن تشن على عدة أصعدة ، هي:
- أولاً: الصعيد الحسي يكون التركيز على موضع الهجوم والبيئة المحيطة به؛ ويدخل ضمن هذا :
  - مكان العمل : يدخل المهاجم مكان العمل متظاهرا بأنه أحد الموظفين، أو المتعاقدين مع جهة العمل، أو عمال النظافة أو الصيانة. وإذا تمكن المهاجم من الدخول فإنه يطوف بالمكاتب لجمع ما يمكنه جمعه من كلمات المرور التي قد تكون مكتوبة على أوراق ملصقة بشاشة الحاسوب ، أو لوحة المفاتيح.

جوانب الهجمات بأسلوب الهندسية الاجتماعية

- الهاتف: يستخدم بعض المهاجمين الهاتف لشن هجمات بأسلوب الهندسية الاجتماعية، وأكثر الأشخاص تعرضا لهذا النوع من الهجمات هم العاملون في مراكز تقديم الدعم الفني . فالمهاجم، مثلاً ، قد يتصل بمركز تقديم الدعم الفني هاتفياً ويطلب منه بعض المعلومات الفنية ؛ وتدريجياً يحصل على ما يريده من معلومات ، ككلمات المرور وغيرها. وبعد ذلك يستخدم هذه المعلومات التي يحصل عليها لشن هجمات على حواسيب المنشأة. ويرى الكاتبان أن هذا النوع من السهل تنفيذه ضد البنوك، و الشركات، والمؤسسات في مجتمعنا؛ بسبب تركيبتنا النفسية والاجتماعية التي تجعل عددا منا يولي ثقته بسهولة لكل أحد.
- النفايات : قد يستغرب بعضنا إذا علم أن هذه الطريقة من أكثر الطرق شعبية بين المهاجمين الذين يستخدمون الهندسة الاجتماعية، والسر في شعبيتها أن المهاجم يستطيع جمع معلومات كثيرة ومهمة دون أن يلفت انتباه أحد.

جوانب الهجمات بأسلوب الهندسية الاجتماعية

- الإنترنت: عندما يستخدم شخص ما عدة برامج أو تطبيقات يتطلب كل منها كلمة مرور مثل : Yahoo وHotmail وغيرها، فإنه غالبا ما يجنح إلى استخدام كلمة مرور واحدة لها جميعا ليسهل على نفسه تذكرها. لكن المشكلة هي أنه عندما يستطيع مهاجم ما معرفة كلمة المرور هذه فإنه يصبح من السهل عليه اختراق كل التطبيقات التي يتعامل معها صاحب كلمة المرور الأصلي. ومن وسائل المهاجمين في الحصول على كلمة المرور إلى الإنترنت، إن ينشئ المهاجم المتربص موقعا على شبكة الإنترنت يقدم خدمات معينة، مثل: تنزيل البرامج المجانية، ولكنه يشترط على الراغب في تنزيل هذه البرامج أن يدخل رقم المستخدم وكلمة المرور. ونتيجة لما أشرنا إليه آنفا من أن بعض مستخدمي الحاسوب يفضل استخدام كلمة مرور واحدة لكل التطبيقات التي يتعامل معها فإن كلمة المرور التي يدخلها في ذلك الموقع غالبا ما تكون هي كلمة المرور نفسها التي يستخدمها في تطبيقاته الأخرى. ومن هنا يحصل المهاجم على كلمة المرور للدخول على معلومات المستهدف المخزنة في التطبيقات الأخرى.

جوانب الهجمات بأسلوب الهندسية الاجتماعية

- ثانياً: الصعيد النفسي:
- هذا المستوى يعنى بالمناخ النفسي المحيط بالطريقة التي ينفذ بها الهجوم. فالمهاجم يسعى إلى خلق الأجواء النفسية المناسبة لإيهام الضحية بأن المهاجم شخص موثوق به، ولديه صلاحية الاطلاع على المعلومات الحساسة للشخص المستهدف أو المنشأة المستهدفة.

أساليب الهجوم
بإستخدام الهندسة الاجتماعية

- هناك عدة أساليب للهجوم باستخدام الهندسة الاجتماعية، وهي كما يلي:
- أولاً: أسلوب الإقناع : هذا هو أهم أساليب هذه الطريقة ؛ ولذلك سنفصل الكلام فيه. وبادئ ذي بدء نقول إن سيكولوجية الإقناع لها جوانب متعددة أهمها:

– طرق الإقناع: تدل الدراسات التي أجريت في علم النفس الاجتماعي Social Psychology أن هناك طريقتين لإقناع شخص لعمل شيء ما :

- طريقة الإقناع المباشرة: في هذه الطريقة يتذرع المهاجم بالحجج المنطقية والبراهين لحفز المستمع – في هذه الحالة الضحية - على التفكير المنطقي والوصول إلى نتيجة يرغب المهاجم في جر الضحية إليها.
- الطريقة غير المباشرة : هنا يعتمد المهاجم على الإيحاءات النفسية، والقفز فوق المنطق، وتحاشي استنفار قدرة التفكير المنطقي لدى الضحية ، وحث الضحية على قبول مبررات المهاجم دون تحليلها والتفكير فيها جدياً.

أساليب الهجوم
بإستخدام الهندسة الاجتماعية

- أساليب التأثير المستخدمة في طريقة الإقناع غير المباشرة: فيما يلي نعرض أنجح الأساليب التي يعملها المهاجم ضد خصمه عندما يستخدم الأول طريقة الإقناع غير المباشرة :

- التزيي بمظهر صاحب السلطة: إن الغالب على الناس سرعة تلبية طلبات ذي السلطة ، حتى وإن لم يكن موجودا بشخصه.
- الإغراء بامتلاك شيء نادر: إن الناس في مجملهم لديهم الرغبة في امتلاك أي شيء مهما كان إذا أحسوا أن ذلك الشيء أصبح شحيحا، أو أنه متوفر لفترة محدودة، وهذا أمر يدل عليه الواقع المعيش، كما دلت عليه الدراسات التي أجريت في مجال علم النفس الاجتماعي. كما أن رغبتهم تزداد في امتلاك ذلك الشيء متى ما شعروا أن قدرتهم على امتلاكه ستصبح محدودة في المستقبل.
- إبراز أوجه التشابه مع الشخص المستهدف: إن من خصائص النفس البشرية الميل إلى من يشبهها في العرق، أو اللون، أو الاهتمامات والطباع. وإحساسنا بوجود أوجه شبه مع شخص ما يجعلنا أقل حذرا عند التعامل معه، لأننا لا إراديا تعطل بعض قدراتنا على التحليل والتفكير المنطقي.
- رد الجميل: إن من خصائص النفس السوية رغبتها في رد الجميل إلى من أحسن إليها. وتزداد هذه الخاصية رسوخا في المجتمعات ذات الصبغة القبلية والأسرية.

أساليب الهجوم
بإستخدام الهندسة الاجتماعية

- ثانياً: أسلوب انتحال الشخصية: وتعني تقمص إنسان ما شخصية إنسان آخر، وقد يكون هذا الآخر شخصاً حقيقياً أو ومتوهماً.
- ثالثاً: أسلوب المداهنة: عند التأمل في الشخصيات التي يكثر انتحالها، وذكرناها في الفقرة السابقة ، يتضح للعيان أنها في الأعم لأناس تدعمهم سلطة قوية داخل الشركة أو التجمع.
- رابعاً: أسلوب مسايرة الركب: هذا مسلك اجتماعي يملي على الإنسان ألا يتخذ موقفا مغايرة لما عليه الآخرون تجاه مسألة ما. والمهاجم إذ يدرك هذا فإنه سيسعى جاهدة لاستغلاله .
- خامساً: أسلوب الهندسة الاجتماعية العكسية: هذه إحدى الطرق المتقدمة لكسب ثقة المستهدفين ، ومن ثم الحصول على المعلومات. وتقوم هذه الطريقة على اختلاق موقف يظهر المهاجم في صورة صاحب سلطة إدارية أو فنية ، فيتوجه إليه المستهدفون بالأسئلة ويطلبون منه المساعدة ويتلقون منه التعليمات. وتنفيذ هذه الطريقة بثلاث مراحل:
  - افتعال الموقف.
  - إبراز المهاجم نفسه على أنه الشخص ذو المعرفة أو الصلاحية اللازمة للتعامل مع الموقف.
  - تقديم المساعدة.

العامل البشري
نقطة الاختراق الأولى

٩٠٪ من الاختراقات في عام ٢٠١٥ م في العالم تمت من خلال استغلال العامل البشري.

الحل هو توعية مستخدم التقنية عن المخاطر السبرانية

الإنسان هو الهدف الأول
خمسة طرق استخدمت للاختراق

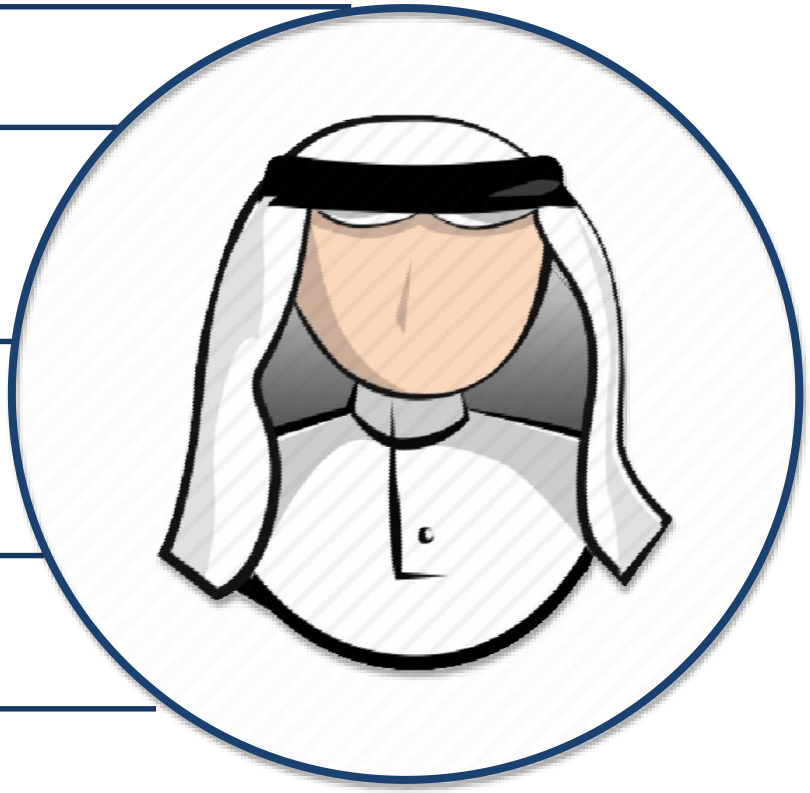
رسائل تصيد عبر شبكات التواصل الاجتماعي

مكالمات تلفونية للمستهدفين

رسائل الاصطياد الإلكتروني الموجهة (Spear Phishing)

اختراق مواقع موثوقة وزرع البرامج التجسسية فيها

تسلسل من البرامج الخبيثة لاختراق الجهاز المستهدف



من هم أنونيموس؟

- أنونيموس Anonymous اي المجهول وهي اسم على مسمى. ظهرت على الإنترنت منذ عام 2003، حيث يظهر الاعظاء في زي متنكر ولا يعرضون اي معلومات تفيد بهويتهم و أحيانا يتم تغير الصوت أثناء بث خبر ما. الفكرة أتت لمحاربة الأشخاص السيئين في المجتمع من خلال الإنترنت.

من هم أنونيموس؟

- فهي مجموعة من الهاكرز الخارجين عن القانون، و هي مجموعة من الناس عندما يرون أن شيئ ما غلط ،يبادرون إلى تصحيح رؤية العالم إليه ، نعم بالطبع المجموعة تحتوي كذلك على هاكرز لكن عدد الهاكرز المنتمين إلى المجموعة قليل . تهدف أنونيموس إلى ، الكشف عن المعنى الحقيقي لكلمة سينتولوجيا والتي تستند إلى الفكر العلماني خصوصا، كذلك بالنسبة لمن يؤمنون بالتعاليم الدينية والمعتقدات التي يستند إليها الفكر العلماني.
- أهم العمليات التي قامت بها جماعة أنونيموس: في المرحلة الأولى من عمر ما يمكن تسميته أنونيموس كانت جميع النشاطات تقريبا تنحصر بالطابع الساخر، حيث قام الأفراد باستهداف عدة برامج راديو متعصبة مثلا بمكالمات مخادعة ومقالب، لكن أشهر المقالب وأطولها ربما هو استهداف شبكة اجتماعية ولعبة سويدية باسم Habbo Hotel
- مع الوقت بدأ الأمر بالتطور مع استخدام شعار النازية (بوضع الشخصيات مع بعضها لتشكله معاً).

من هم أنونيموس؟

- عام 2008: مشروع Chanology وهجوم أنونيموس على كنيسة الساينتولوجي.
- كنيسة الساينتولوجي (Scientology) هي جماعة دينية أسسها كاتب قصص مصورة في منصف القرن العشرين، ومنذ تأسيسها أحاطت بها العديد من الفضائح بما يخص التهرب الضريبي والتصرفات المريبة وحتى محاولة ابتزاز هيئة الدخل الأمريكية (المسؤولة عن الضرائب)، لكن النشاط الأكثر فضائحية ربما هو الملاحقة المستمرة ومحاولة أذى الأعضاء السابقين بعد مغادرة الكنيسة وكتم أي معلومات يتم تسريبها بأي ثمن، وفي مطلع عام 2008 هذا ما حصل مع قيام الكنيسة بإجبار موقع Gawker على حذف فيديو للمثل الشهير Tom Cruise وهو يتحدث عن الكنيسة.

جرائم سيبرانية

- في عام 2013 واجهت الولايات المتحدة أكبر حملة تجسس سيبراني تحت اسم "تيتان ربين"، وقد استهدفت هذه الهجمة وكالة الأمن القومي الأميركي، وزارة الدفاع الأميركية بالإضافة لعدد من القطاعات الخاصة. وقد اتهم الكونغرس الحكومة الصينية بهذا الهجوم، وعلى إثر ذلك قامت الولايات المتحدة بعقد اتفاقية مع الصين في عام 2015 لوضع حدود العلاقات السيبرانية، ولكن الصين نقضت الاتفاقية عندما قامت بالتجسس على مكتب موظفي الحكومة الفيدرالية والذي أضر ببيانات 20 مليون شخص.

قصه الهكر المشهور كيفن

- اسم كيفن ميتنيك kevin mitnick لا يعرفه الكثيرون في عالمنا العربي والشرق الأوسط، ولكنه في أوروبا والولايات المتحدة يعتبر من أشهر الأسماء خصوصا بالنسبة إلى شركات الانترنت وعالم الحاسبات الآلية وأمن الشبكات. كيفن ميتنيك هو أشهر قرصان الكتروني ظهر على وجه الأرض وأكثر الهاكرز خطورة منذ ظهور الحاسبات الآلية إلى درجة أنه أصبح اول قرصان كمبيوتر توضع صوره من ضمن قائمة المطلوبين لدى الاف بي أي FPI الانترنت فما هي قصته؟

قصه الهكر المشهور كيفن

- وعلى الرغم من أن كيفن لم يكن من المتفوقين دراسية، إلا أنه برع في الدخول إلى بدالات مؤسسة الهاتف المحلية، وتمكن من الحصول على مكالمات هاتفية مجانية. وتطور الأمر إلى تمكنه من اقتحام عوالم الآخرين، والاستماع إلى مكالماتهم. وأصبح لديه خلال فترة وجيزة، الكثير من المعلومات والأسرار، عن أشخاص كان يختارهم من الأغنياء وذوي السلطة، مما خلق في نفسه الشعور بالقوة والتفوق. وبفضل اهتماماته في هذا المجال تعرف إلى مجموعة من الشباب لهم الاهتمام ذاته، والخبرة في اختراق شبكة الهاتف عن طريق الكمبيوتر، و شكلوا مجموعة أصبحت اجتماعاتها شبه منتظمة، للتداول في وسائل وطرق جديدة في هذا المجال. وحتى ذلك الوقت، كان كل ما قامت به المجموعة لا يتعدى المزاح لشباب راغبين في المتعة والابتعاد عن الملل، وإن كان بإزعاج الآخرين قليلا.. لكن الإزعاج ما لبث أن تحول إلى أذى، حيث قام أحد أفراد المجموعة بتدمير ملفات إحدى شركات الكمبيوتر في سان فرانسيسكو، ولم تتمكن الشرطة من معرفة الفاعل، لأكثر من عام.

قصه الهكر المشهور كيفن

- في أحد أيام العطل من عام 1981 دخل كيفن واثنان من أصدقائه خلسة، إلى المركز الرئيسي لشركة الهاتف في مدينة لوس انجلوس، ووصلوا إلى الغرفة التي تحتوي على الكمبيوتر الذي يدير عمليات الاتصال، وأخذوا كتب التشغيل الخاصة به، وقوائم وسجلات تتضمن مفاتيح السر لأقفال الأبواب، في تسعة مراكز أساسية تابعة لشركة الهاتف في المدينة. وعندما حققت الشرطة المحلية في الأمر، لم تتمكن من كشف الفاعل.. لكن، وبعد سنة، وشت بهم فتاة من أعضاء المجموعة للشرطة، الذين سارعوا لاعتقال الشبان الثلاثة. وحكم على كيفن بقضاء ثلاثة أشهر في سجن الأحداث بتهمة السرقة، وتدمير بيانات عبر شبكة كمبيوتر، كما قضت المحكمة بوضعه بعد ذلك، سنة تحت المراقبة في لوس انجلوس. من جهته، حاول مركز الخدمة الاجتماعية تقديم العون له، لتطوير خبراته في مجال الكمبيوتر، والاستفادة منها بشكل شرعي، لكن النتيجة جاءت سلبية، إذ سعى كيفن إلى تعلم أمور مختصرة، وحيل تساعده على ممارسة هوايته باختراق شبكات الكمبيوتر، وهذا ما قاده من قضية إلى أخرى. واعتقل كيفن ثانية عام 1983 من قبل شرطة جامعة شمال كاليفورنيا، بعد ضبطه يحاول استخدام شبكة كمبيوتر الجامعة للوصول من خلالها إلى البنتاغون. وحكمت المحكمة عليه بستة أشهر تدريب في إصلاحية للأحداث، في كاليفورنيا. وبعد سنوات اعتقل مرة أخرى، بتهمة العبث بكمبيوتر حسابات إحدى الشركات، والغريب في الأمر، أنه بقي رهن الاعتقال لمدة سنة كاملة من دون محاكمة، والأغرب اختفاء ملفه من مركز الشرطة، من دون أي تفسير أو شرح!

قصه الهكر المشهور كيفن

- وفي عام 1988 قبض عليه مرة ثانية بتهمة اختراق حاسبات أحدى شركات الكمبيوتر الكبرى في الولايات المتحدة مما سبب خسائر تقدر بأربعة ملايين دولار وسرقة برامج بقيمة مليون دولار. لذلك لحكم عليه في عام 89 بالسجن لمدة عام وقضى كيفن المدة. ولقد كان مجبرا على الانخراط في مركز لمعالجة الإدمان من القرصنة وذلك بحكم قضائي لمدة ستة أشهر.
- وبعد إطلاق سراحه في عام 1990 كان كيفن يحاول الاستقامة ولكنه كان يواجه صعوبة في الحصول على عمل في عالم الحاسبات الآلية نتيجة لماضيه الملوث. حتى وجد عملا في احدى الشركات المتوسطة. ولكن نتيجة لوفاة أخيه في عام 92 من جرعة مخدرات تعرض كيفن لحالة كأبة شديدة و عاد لهوايته القديمة وهي اختراق الحاسبات الآلية والقرصنة. وفي نهاية ذلك العام توجهت الى «اف.بي.أي» إلى شقة كيفن لتستجوبه حول بعض قضايا الاختراق لتجده قد فر واختفى. وظلت المتابعة مستمرة بين الاف بي أي وكيفن بين عدة مدن كان خلالها كيفن يواصل عمله في اختراق الحاسبات الآلية عن طريق حاسبه المحمول والهاتف النقال.

قصه الهكر المشهور كيفن

- في كل مرة كان كيفن يهرب بأعجوبة من أيدي عملاء FPIهذه الملاحقة صنعت من كيفن اسطورة في انحاء الولايات المتحدة واصبح مثالا يحتذى به في عالم القرصنة والهاكرز لقدرته على الاختفاء والدخول إلى أكثر الحاسبات صعوبة حتى إلى وزارة الدفاع الأميركية وأكبر الشركات في أميركا.
- ولكن في نهاية عام 94 اخترق كيفن الحاسب الرئيسي لشركة Tsutomu Shimomuraوهي شركة مشهورة متخصصة في أمن الشبكات. هذا الاختراق جعل الشركة تصمم على متابعة كيفن وملاحقته بالتعاون مع محققي الى «اف.بي.أي»، وبالفعل بعد شهرين فقط وبتاريخ 15 فبراير من عام 1995 اعتقل كيفن في شقته. وللضرر الذي ألحقه كيفن بالعديد من الشركات والأفراد ولملايين الدولارات من الخسائر ولكونه أصبح خطرا على امن الولايات المتحدة الأميركية فقد حكم عليه بالسجن لمدة أربع سنوات بالإضافة إلى دفع ...4 دولار كتعويض. وكذلك وافق كيفن على تخصيص أرباحه المستقبلية من أي كتب أو أفلام أو مقابلات متعلقة بجرائمه ستخصص لضحاياه لمدة سبع سنوات.

تخصصات الأمن السيبراني

- مهام متخصصي الأمن السيبراني:
  - يلعب متخصص والأمن السيبراني دورا رئيسيا في تأمين أنظمة المعلومات. من خلال مراقبة أحداث الأمان والكشف عنها والتحقيق فيها وتحليلها والاستجابة لها.
  - يركز متخصصو الأمن السيبراني على مجال تكنولوجيا المعلومات المكرسة لحماية سلامة شبكة وبيانات الشركة..
- كيف يمكن لعملك الاستفادة من تخصص الأمن السيبراني
  - يوفر الأمن السيبراني أكبر ميزة حيث يشكل أفضل الحلول الأمنية لأمن تكنولوجيا المعلومات .
  - يحمي الأمن السيبراني المعلومات الشخصية في واحدة من أكثر السلع قيمة في العصر الرقمي.
  - يتيح للموظفين العمل بأمان بحيث تكون أنت وموظفك معرضين دائما للخطر من أي هجوم الكتروني محتمل.

شهادات الأمن السيبرانى

- شهادة NETWORK
  - شهادة +A هي احدى شهادات شركة CompTIAوالتي تقدم الكثير من الشهادات العلمية لكل من يهتم بالعمل في المجال التقني وتعتبر شهادة + Aمعيار عالمي في مجال صناعات الكمبيوتر، وتعد أقوى شهادة في مجال الدعم الفني والصيانة الأجهزة الكمبيوتر. هذه الشهادة هي vendor-neutral
- ويجب ان يكون:
  - على دراية بطبقات النموذج OSI Model
  - وصف هيئات ووظائف الشبكات Networks
  - ويمتلك المهارات اللازمة لتثبيت وإعداد وإصلاح العيوب الأساسية الخاصة بأجهزة الشبكات والبروتوكولاتHardware and Network experience

شهادات الأمن السيبرانى

- شهادة CHC (Cyber Hacker Certified)
- التقني معتمدة من TechCampus
  - ❑ مدة صلاحيتها 3 سنوات
  - ❑ يمكن استلامها الكترونيا او نسخه ورقيه ترسل لعنوانه
  - ❑ إمكانية إعادة الاختبار في حالة عدم الاجتياز
- وهي شهادة احترافية في عالم أمن المعلومات والأمن السيبراني حيث يتم منحها للهاكر الأخلاقي المتمرس في الدفاع والهجوم المطلوب ضد الهجمات الشرسة حيث يحصل المتدرب على الشهادة موثقة ومعتمدة من شركة TechCampus للتدريب التقني وهي شركة مسجلة رسمية في الاتحاد الأوروبي، ومدة صلاحيتها 3 سنوات وتعتبر هي الأعلى من حيث الشهادات التقنية والاحترافية.
- مدخل إلى أمن المعلومات
- صيانة الحواسيب (هارد وير او سوفت وير)

المراجع العربية

- إيفانز غراهام، نوينهام جيفري. قاموس بنغوين للعلاقات الدولية. تر: مركز الخليج للأبحاث. الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004
- جبور منى الأشقر. السيبرانية هاجس العصر. بيروت: جامعة الدول العربية - المركز العربي للبحوث القانونية والقضائية 2016
- بارة سمير. "الأمن السيبراني Cyber security في الجزائر السياسات والمؤسسات". المجلة الجزائرية للأمن الانساني 2017
- بوغرارة يوسف "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري". مجلة الدراسات الإفريقية وحوض النيل 2018
- زروقة إسماعيل. "الفضاء السيبراني والتحول في مفاهيم القوة والصراع". مجلة العلوم القانونية والسياسية 2019
- الفتلاوي أحمد عبيس نعمة "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية 2016
- الطيب مصطفى. "الفرق بين أمن المعلومات والأمن السيبراني". مدونة علوم، 8 أغسطس 2019

المراجع العربية

- مرزوق عنترة، حرشاوي بن محيي الدين. "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية". ورقة بحث قدمت في الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقلة، الجزائر، 30، 31 يناير 2017
- دحماني سليم. "أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية أنموذجا، 2001-2017" جامعة محمد بوضياف المسيلة، قسم العلوم السياسية، 2018
- رغدة البي. "الردع السيبراني: المفهوم والإشكاليات والمتطلبات". موقع المركز الديمقراطي العربي. تم تصفح الموقع يوم: 10 أغسطس 2019
- الجودي ، لمياء خالد ، (2018) ، ماهي الهندسة الاجتماعية وكيف تتجنب مخاطرها ؟، مبادرة العطاء الرقمي.
- خنين ، منال خالد ، (2013) ، احذروا من هاكرز الهندسة الاجتماعية ، مركز التميز لأمن المعلومات الرياض ، المملكة العربية السعودية.
- عسكر، محمد ، والعكوز ، عبد العزيز، (2013)، الهندسة الاجتماعية فن اختراق عقول البشر، المركز العربي لابحاث الفضاء الالكتروني.

المراجع الأجنبية

- Hulme George V.& Goodchild Joan, (2017),What is social engineering? How criminals exploit human behavior
- Conteh, Nabie & Schmick, (2016) Paul J. Cyber security risks vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research, Vol 6 (23) USA.
- MITNICK, KEVIN D, & Simon, William L, (2015), THE ART OF DECEPTION Controlling the Human Element of Security, Foreword by Steve Wozniak.
- Tiwari, Aditya, (2018), What Is Social Engineering? What Are DifferKontio, Mika, (2016), SOCIAL ENGINEERING , TURKU UNIVERSITY OF APPLIED SCIENCES
- Lehto Martti, Neittaanmäk Pekka . Cyber Security: Analytics, Technology and Automation. Switzerland: Springer International Publishing,.r. 2015

المراجع الأجنبية

- Valeriano Brandon and C. Maness Ryan." international relations theory and cyber security threats conflicts and ethics in an Emergent Domain in an emergent domain" in The Oxford Handbook of International Political Theory,edited by. Brown Chris and Eckersley Robyn .united kingdom: Oxford University Press, 2018
- Griffiths, Jordan Luke. " CYBER SECURITY AS AN EMERGING CHALLENGE TO SOUTH AFRICAN NATIONAL SECURITY" . master's thesis , University of Pretoria , South Africa, 2016
- Ebert Hannes and Maurer Tim. "Cyber Security" oxford bibliographies, LAST MODIFIED: 11 JANUARY 2017
- Alharbi, A.R. and Aljaedi, A., 2019. Predicting rogue content and arabic spammers on twitter. Future Internet, 11(11), p.229.
- Alharbi, A.R., Hijji, M. and Aljaedi, A., 2021. Enhancing topic clustering for Arabic security news based on k-means and topic modelling. IET Networks.

تقييم الحقيبة

جامعة تبوك
University of Tabuk

جامعة تبوك
University of Tabuk

تم بحمد الله