الأمن السيبراني
Cyber Security

أجندة الكورس
Course Agenda

- Cyber Security Definition and Importance
- Cyber Security Types
- Cyber Capes
- Cyber Information VS Cyber Security
- Cyber crimes
- Cyber Attacks protection tips

- تعريف الأمن السيبراني ومدى أهميته
- أنواع الأمن السيبراني
- الفضاء السيبراني
- الفرق بين أمن المعلومات والأمن السيبراني
- الجرائم الإلكترونية
- كيف تحمي نفسك من الهجمات الإلكترونية

أهداف الكورس
Course Goals

- التعرف على ماهية الفضاء السيبراني أو الواقع الافتراضي البديل للواقع التقليدي الذي نعيش فيه الآن، والذي سوف يكون مليئاً بالمخاطر في صورة هجمات سيبرانية إلكترونية تهدد حياتك الشخصية والعملية.
- التعرف على ماهية وأشكال وصور هذه الجرائم السيبرانية.
- التعرف على المجرم المعلوماتي وأساليبه التي يقوم من خلالها بتلك الجرائم؛ حتى تكون أكثر حذراً من التعامل مع أشخاص مبهمين خلال شبكات الإنترنت.
- تعلم كيفية حماية بياناتك الشخصية ومعلوماتك الهامة سواء كنت فرداً، أو كنت مؤسسة أعمال خاصة أو عامة، تعتمد في طياتها على السجلات الرقمية في ظل التحول الرقمي من خلال معرفتك بالأمن السيبراني وسبل التصدي للهجمات الإلكترونية.

المحاضرة الأولى

ماهية وتعريف الأمن السيبراني

Cyber security concept

أجندة المحاضرة
Lecture Agenda

- Cyber Capes
- Cyber Security Definition
- Cyber Information VS Cyber Security
- The Importance of Cyber Security
- Types of cyber security

- الفضاء السيبراني
- تعريف الأمن السيبراني
- الفرق بين أمن المعلومات والأمن السيبراني
- أهمية الأمن السيبراني
- أنواع الأمن السيبراني

تعريف الفضاء السيبراني
Cyber Capes

أصبح الفضاء الإلكتروني مجالاً جديداً للبحث الجغرافي في عصر المعلومات، فعلى خلفية المنافسة الدولية الشرسة على الفضاء السيبراني، كانت هناك حاجة ملحة لتعزيز البحث بين مجالات الجغرافيا والأمن السيبراني، مما أدى إلى ابتكارات نظرية ومنهجية خلقت فرعاً فرعياً لجغرافيا الفضاء السيبراني.

توسع جغرافيا الفضاء السيبراني البحث الجغرافي من المساحات الحقيقية إلى المساحات الافتراضية، وأساسها النظري هو تطور نظرية العلاقة الجغرافية التقليدية بين الإنسان والأرض إلى نظرية العلاقة بين الإنسان والموقع الافتراضي.

تعريف الفضاء السيبراني
Cyber Capes

يعد الفضاء الإلكتروني عالماً مكانياً جديداً من الأنشطة التي تشمل البشر والبيانات على حد سواء، وقد أصبح حجر الزاوية للأمن القومي لكل بلد، ويعد المفهوم العلمي للفضاء السيبراني ضرورياً لتحليل حوادث الفضاء السيبراني، وإدارة الفضاء السيبراني، وضمان الأمن السيبراني.

تعريف الأمن السيبراني
Cyber Security Definition

- الأمن السيبراني هو عملية حماية واستعادة الشبكات والأجهزة والبرامج من أي نوع من الهجمات الإلكترونية، تماماً مثل الأمن المادي الذي يهدف إلى حماية الممتلكات المادية والأشخاص من النشاط الإجرامي أو الضرر العرضي، فيحمي الأمن السيبراني أنظمة الكمبيوتر والأنظمة الخلفية وتطبيقات المستخدم النهائي End User Applications ومستخدمي تلك الأنظمة والبيانات التي يخزنونها.
- كما أنه يهدف الأمن السيبراني إلى منع مجرمي الإنترنت Internet criminals أو المطلعين الضارين Hackersأو غيرهم من الوصول إلى أنظمة وتطبيقات تكنولوجيا المعلومات، أو إلحاق الضرر بها أو تعطيلها أو تعديلها.

أهمية الأمن السيبراني
Cyber Security Importance

- مع تحول المجتمع البشري إلى عالم رقمي، يتم تسهيل جميع جوانب حياتنا من خلال الشبكات والكمبيوتر والأجهزة الإلكترونية الأخرى وتطبيقات البرامج.
- تستخدم البنية التحتية الحيوية -بما في ذلك الرعاية الصحية والمؤسسات المالية والحكومات والتصنيع- أجهزة الكمبيوتر أو الأجهزة الذكية كجزء أساسي من عملياتها، والغالبية العظمى من هذه الأجهزة متصلة بالإنترنت.
- يمتلك الفاعلون المهددون حافزاً أكبر من أي وقت مضى لإيجاد طرق لاختراق أنظمة الكمبيوتر هذه؛ لتحقيق مكاسب مالية أو ابتزاز أو دوافع سياسية أو اجتماعية (تُعرف باسم القرصنة) أو لمجرد التخريب.

أهمية الأمن السيبراني
Cyber Security Importance

- وعلى مدى العقدين الماضيين تم شن هجمات إلكترونية ضد البنية التحتية الحيوية في جميع الدول المتقدمة، وتكبد عدد لا يحصى من الشركات خسائر فادحة.
- فهناك أكثر من 2000 انتهاك مؤكد للبيانات على مستوى العالم كل عام، ومع كل خرق يكلف أكثر من 3.9 مليون دولار في المتوسط (8.1 مليون دولار في الولايات المتحدة)

منذ عام 2000 سرق مجرمو الإنترنت معلوماتهم الخاصة أكثر من 3.5 مليار شخص، أي نصف سكان العالم.

أهمية الأمن السيبراني
Cyber Security Importance

- في الغالبية العظمى من هذه الأنظمة تعد مواقع الويب وتطبيقات الويب بوابة للمهاجمين.
- كما إنهم معرضون للإنترنت العام، ومتصلون بشكل عام بأنظمة خلفية حساسة، مما يمثل رابطاً ضعيفاً في استراتيجية أمان المؤسسة.
- سواء كانت مؤسستك شركة من أي حجم، أو موقع ويب يتلقى حركة مرور كبيرة، أو مؤسسة أو منظمة غير ربحية تخدم المصلحة العامة؛ فإن التحضير والدفاع ضد تهديدات الأمن السيبراني يجب أن يكون أحد أهم اهتماماتك.

أنواع الأمن السيبراني
Types of cyber security

أمن الحوسبة السحابية
Cloud computing security

منع فقدان البيانات
Data loss

أمن المعلومات
Information Security

أمن البنية التحتية
Critical infrastructure

أمن الشبكات
Network security

تعليم المستخدم النهائي
User awareness

أمن التطبيقات
Application security

أمن البنية التحتية الحرجة
Critical infrastructure

البنية التحتية الحرجة Critical infrastructure هي الأنظمة المادية والإلكترونية والأصول التي تعتبر حيوية جداً للدولة، بحيث يكون لعجزها أو تدميرها تأثير مدمر على أمن الدولة المادي أو الاقتصادي أو الصحة العامة أو السلامة، كما توفر البنية التحتية الحرجة للدولة الخدمات الأساسية التي يقوم عليها المجتمع.

أمن المعلومات
Information Security

يحمي كل من البيانات المادية والرقمية -بشكل أساسي البيانات بأي شكل- من الوصول غير المصرح به أو الاستخدام أو التغيير أو الكشف أو الحذف أو أي أشكال أخرى من المعلومات الخبيثة Malicious information.

أمن الشبكات
Network security

- يحمي الشبكات الداخلية من المتطفلين من خلال تأمين البنية التحتية.
- تتضمن أمثلة أمان الشبكة تنفيذ المصادقة الثنائية Two-factor authentication

وكلمات مرور جديدة وقوية New and strong passwords.

أمن التطبيقات
Application security

- يستخدم البرامج والأجهزة للدفاع ضد التهديدات الخارجية التي قد تطرح نفسها في مرحلة تطوير التطبيق.
- كما تتضمن أمثلة أمان التطبيقات برامج مكافحة الفيروسات Anti Virus وجدران الحماية Firewall والتشفير Encryption.

الحوسبة السحابية
Cloud computing

أداة قائمة على البرامج تحمي بياناتك وتراقبها في السحابة Cloud computing

للمساعدة في التخلص من المخاطر المرتبطة بالهجمات المحلية.

منع فقدان البيانات
Preventing Information Loss

- يتألف من تطوير سياسات وعمليات لمعالجة ومنع فقدان البيانات، وتطوير سياسات الاسترداد في حالة حدوث خرق للأمن السيبراني.
- يتضمن ذلك تعيين أذونات الشبكة والسياسات لتخزين البيانات.

تعليم المستخدم النهائي
Educating the end-user

يتضمن تعليم المستخدم النهائي تعليم المستخدمين -الذين يستخدمون التكنولوجيا الحديثة- اتباع أفضل الممارسات، مثل عدم النقر على روابط غير معروفة أو تنزيل مرفقات مشبوهة في رسائل البريد الإلكتروني - مما قد يسمح بدخول البرامج الضارة وأشكال أخرى من البرامج الضارة Malware.

الفرق بين أمن المعلومات والأمن السيبراني
Information Security VS Cyber security

- أمن المعلومات هو في الأساس ممارسة لمنع الوصول غير المصرح به أو الاستخدام أو الإفشاء أو التعطيل أو التعديل أو الفحص أو التسجيل أو إتلاف المعلومات.
- ويمكن أن تكون المعلومات مادية أو إلكترونية، كما يمكن أن تكون المعلومات أي شيء مثل التفاصيل الخاصة بك، أو يمكننا أن نقول ملفك الشخصي على وسائل التواصل الاجتماعي، وبياناتك في الهاتف المحمول، والقياسات الحيوية الخاصة بك Bio-metrics وما إلى ذلك.
- وبالتالي فإن أمن المعلومات يمتد إلى العديد من مجالات البحث مثل التشفير Encryption، والحوسبة المتنقلة Mobile Computing، والطب الشرعي الإلكتروني Digital forensics، ووسائل التواصل الاجتماعي عبر الإنترنت Social Media،.. إلخ.

مواطن التميز والتفرقة بين الأمن السيبراني وأمن المعلومات
Information Security VS Cyber security

الأمن السيبراني	أمن المعلومات
يختص الأمن السيبراني بأمن كافة الموجود على السايبر	أمن المعلومات لا يختص بأمن كافة الموجود على السايبر
الأمن السيبراني لا يختص بأمن المعلومات الفيزيائية	يختص أمن المعلومات بأمن المعلومات الفيزيائية أي الورقية
الأمن السيبراني مفهوم أوسع وأشمل من أمن المعلومات، حيث يتضمن تأمين كافة البيانات والمعلومات التي يتم تداولها من خلال الشبكات الداخلية والخارجية على حدٍ سواء، والتي يتم تخزينها في الخوادم servers داخل أو خارج الشركة من أي اختراق	أمن المعلومات هو الذي يهتم بحماية المعلومات أو أنظمة المعلومات من أي نفاذ غير مسموح به أو غير مصرح به، أو من أي سرقة أو تحرير أو تعديل أو تشهير، وذلك بهدف حفظ السرية والخصوصية للعملاء وإبقاء المعلومات محفوظة

ويمكن أن تؤثر الانتهاكات والتهديدات الأمنية على أي نظام تقريباً، بما في ذلك:

قطاع الاتصالات

الحكومات الإلكترونية

قطاع التعليم

الرعاية الصحية

المحاضرة الثانية

الجرائم الإلكترونية

Cyber Crimes

أجندة المحاضرة
Lecture Agenda

- Cyber Crimes
- How to commit Cyber crimes
- Types of cyber Crimes
- Cyber attacks and its types

- ماهية وتعريف الجرائم الإلكترونية
- كيفية ارتكاب الجرائم الإلكترونية
- أنواع الجرائم الإلكترونية
- التهديدات السيبرانية وأنواعها

تعريف الجرائم الإلكترونية
Cyber Crimes

- الجريمة الإلكترونية هي أي نشاط إجرامي يشمل جهاز كمبيوتر أو شبكة أو جهاز متصل بشبكة.
- بينما يتم تنفيذ معظم الجرائم الإلكترونية من أجل تحقيق ربح لمجرمي الإنترنت، يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة مباشرة لإتلافها أو تعطيلها، بينما يستخدم البعض الآخر أجهزة الكمبيوتر أو الشبكات لنشر برامج ضارة Malware أو معلومات غير قانونية أو صور أو مواد أخرى.

الفئات الثلاثة للجريمة الإلكترونية
Cybercrime’s 3 categories

- الجرائم التي يكون فيها الجهاز الحاسوبي هو الهدف، مثل الوصول إلى الشبكة.
- الجرائم التي يتم فيها استخدام الكمبيوتر كسلاح، مثل شن هجوم قطع الخدمة.
- الجرائم التي يتم فيها استخدام الكمبيوتر كبرنامج ملحق لجريمة، مثل استخدام جهاز كمبيوتر لتخزين البيانات التي تم الحصول عليها بشكل غير قانوني.

والنشاط الإجرامي السيبراني يمكن أن يقوم به أفراد أو مجموعات صغيرة بمهارات تقنية قليلة نسبياً، أو من قبل جماعات إجرامية عالمية عالية التنظيم قد تشمل مطورين مهرة وآخرين من ذوي الخبرة ذات الصلة لزيادة تقليل فرص الاكتشاف والمقاضاة، غالباً ما يختار مجرمو الإنترنت العمل في بلدان ذات قوانين ضعيفة أو غير موجودة بشأن الجرائم الإلكترونية.

كيفية ارتكاب الجرائم الإلكترونية
How to commit a cybercrime

- يمكن أن تبدأ هجمات الجرائم الإلكترونية حيثما توجد بيانات رقمية وفرصة للمجرم ودوافع لارتكابها.
- يستخدم مجرمو الإنترنت موجهات هجوم مختلفة لتنفيذ هجماتهم الإلكترونية ويبحثون باستمرار عن أساليب وتقنيات جديدة لتحقيق أهدافهم، مع اتخاذ كافة الإجراءات الاحترازية لعدم الوصول إليهم.
- غالباً ما ينفذ مجرمو الإنترنت أنشطتهم باستخدام البرامج الضارة Malware وأنواع أخرى من البرامج، لكن الهندسة الاجتماعية Social engineering غالباً ما تكون مكوناً مهماً لتنفيذ معظم أنواع الجرائم الإلكترونية.
- تعد رسائل البريد الإلكتروني للتصيد الاحتيالي مكوناً مهماً آخر للعديد من أنواع الجرائم الإلكترونية، ولكن بشكل خاص بالنسبة للهجمات المستهدفة، مثل اختراق البريد الإلكتروني للأعمال، حيث يحاول المهاجم انتحال شخصية صاحب عمل عبر البريد الإلكتروني لإقناع الموظفين بدفع فواتير مزيفة.

أنواع الجرائم الإلكترونية
Types of cybercrime

هناك العديد من أنواع الجرائم الإلكترونية المختلفة، يتم تنفيذ معظم الجرائم الإلكترونية مع توقع المهاجمين تحقيق مكاسب مالية، على الرغم من أن الطرق التي يهدف بها مجرمو الإنترنت للحصول على أموال قد تختلف، وتتضمن بعض الأنواع المحددة.

أنواع الجرائم الإلكترونية
Types of cybercrime

أهم الجرائم الإلكترونية

التجسس
الإلكتروني
Cyber Spying

سرقات بطاقات
الائتمان
Credit Card Theft

الابتزاز
الإلكتروني
Blackmail

قرصنة
البرامج
Hacking

سرقة الهوية
Identity
Theft

الابتزاز الإلكتروني
Blackmail

- هي جريمة تنطوي على هجوم أو تهديد بهجوم مقترن بالمطالبة بالمال لوقف الهجوم.
- ويعد هجوم برامج الفدية Ransom ware أحد أشكال الابتزاز الإلكتروني، فيحصل المهاجم على إمكانية الوصول إلى أنظمة المؤسسة، ويقوم بتشفير مستنداتها وملفاتها -أي شيء ذي قيمة محتملة- مما يجعل الوصول إلى البيانات غير ممكن حتى يتم دفع الفدية.
- عادة ما يكون هذا في شكل من أشكال العملة المشفرة، مثل البيتكوين.

سرقات بطاقات الائتمان
Credit Card Theft

- هجوم يحدث عندما يتسلل المتسللون إلى أنظمة تجار التجزئة للحصول على بطاقة الائتمان أو المعلومات المصرفية لعملائهم.
- يمكن شراء بطاقات الدفع المسروقة وبيعها بكميات كبيرة في أسواق الشبكة المظلمة، حيث سرقت مجموعات القرصنة كميات كبيرة من أرباح بطاقات الائتمان عن طريق البيع لمجرمي الإنترنت من المستوى الأدنى الذين يربحون من خلال الاحتيال على بطاقات الائتمان ضد الحسابات الفردية.

التجسس الإلكتروني
Cyber spying

- جريمة تنطوي على مجرم إلكتروني يقوم باختراق أنظمة أو شبكات للوصول إلى المعلومات السرية التي تحتفظ بها حكومة أو منظمة أخرى.
- قد يكون الدافع وراء الهجمات هو الربح أو الأيديولوجية، كما يمكن أن تشمل أنشطة التجسس الإلكتروني كل نوع من أنواع الهجمات الإلكترونية لجمع البيانات أو تعديلها أو تدميرها، بالإضافة إلى استخدام الأجهزة المتصلة بالشبكة ، مثل كاميرات الويب أو كاميرات الدوائر التلفزيونية المغلقة، للتجسس على فرد أو مجموعات مستهدفة ومراقبة الاتصالات، بما في ذلك رسائل البريد الإلكتروني والرسائل النصية والرسائل الفورية.

سرقة الهوية
Identity theft

- هجوم يحدث عندما يقوم شخص ما بالوصول إلى جهاز كمبيوتر للحصول على معلومات شخصية للمستخدم، والتي يستخدمها بعد ذلك لسرقة هوية هذا الشخص أو الوصول إلى حساباته القيمة، مثل البنوك وبطاقات الائتمان.
- يشتري مجرمو الإنترنت ويبيعون معلومات الهوية في أسواق الشبكة المظلمة، ويقدمون حسابات مالية، بالإضافة إلى أنواع أخرى من الحسابات.
- كما تعد المعلومات الصحية الشخصية هي هدف آخر متكرر للصوص الهوية.

قرصنة البرامج
Hacking

- هجوم يتضمن نسخ البرامج وتوزيعها واستخدامها بشكل غير قانوني بقصد استخدام تجاري أو شخصي.
- غالباً ما ترتبط انتهاكات العلامات التجارية وانتهاكات حقوق النشر وانتهاكات براءات الاختراع بهذا النوع من الجرائم الإلكترونية.

التهديدات السيبرانية وأنواعها
Cyber Attack

هناك العديد من أنواع التهديدات السيبرانية التي يمكن أن تهاجم أجهزتك وشبكاتك، لكنها تقع عموماً في ثلاث فئات:

- الهجمات على التوافر Availability Attack
- الاعتداء على النزاهة Integrity Attack
- الاعتداء على السرية confidentiality Attack

التهديدات السيبرانية وأنواعها
Cyber Attack

الهجمات على التوافر Availability Attack

- الهدف من هذا النوع من الهجمات الإلكترونية هو منع المستخدمين من الوصول إلى بياناتهم الخاصة حتى يدفعوا رسوماً أو فدية، عادةً ما يتسلل مجرم الإنترنت إلى الشبكة والأطراف المخولة من الوصول إلى البيانات المهمة، ويطالبون بدفع فدية.

التهديدات السيبرانية وأنواعها
Cyber Attack

الاعتداء على النزاهة Integrity Attack

- تتكون هذه الهجمات من التخريب الشخصي أو التخريب المؤسسي، وغالباً ما تسمى عمليات التسريب.
- سوف يصل المجرم الإلكتروني إلى معلومات حساسة ويطلقها بغرض كشف البيانات والتأثير على الجمهور لفقد الثقة في شخص أو مؤسسة.

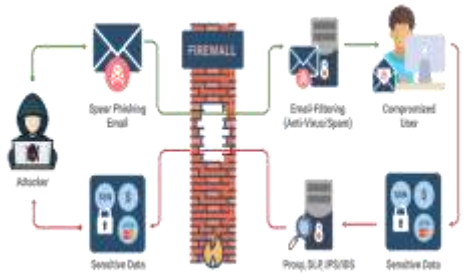
الاعتداء على السرية Confidentiality Attack

- يمكن تصميم هذه الهجمات لسرقة معلومات التعريف الشخصية الخاصة بك وحسابك المصرفي أو معلومات بطاقة الائتمان الخاصة بك.
- بعد هذه الهجمات يمكن بيع معلوماتك أو تداولها على الويب المظلم للآخرين لشرائها واستخدامها.

التهديدات السيبرانية وأنواعها
Cyber Attack

وفيما يلي بعض أنواع التهديدات الإلكترونية التي تقع ضمن الفئات الثلاث المذكورة أعلاه:

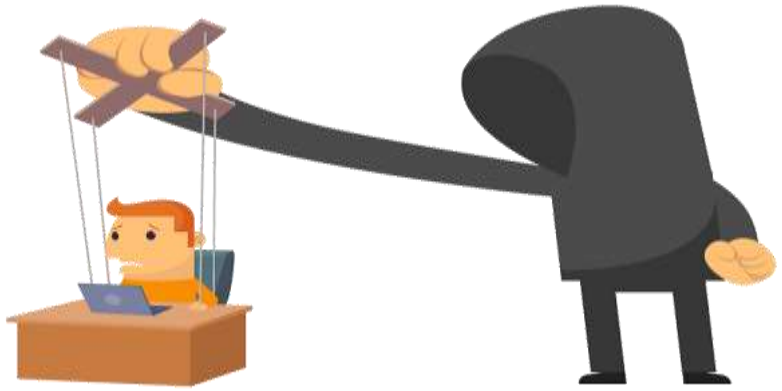
البرامج
الضارة
Malware



هجمات
التصيد
Phishing

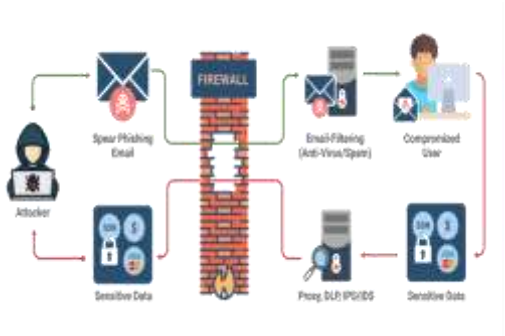
الهندسة الاجتماعية
Social
engineering

الهندسة الاجتماعية
Social engineering



نوع من الهجوم على السرية، هي عملية التلاعب النفسي بالناس لأداء الإجراءات أو التخلي عن المعلومات.

هجمات التصيد
Phishing



هي الشكل الأكثر شيوعاً للهندسة الاجتماعية، وعادة ما تأتي هجمات التصيد الاحتيالي في شكل بريد إلكتروني مخادع بهدف خداع المتلقي لتقديم معلومات شخصية.

البرامج الضارة
Malware

- هي نوع من الهجوم على التوافر، ويشير إلى البرنامج المصمم للوصول إلى جهاز كمبيوتر أو إتلافه دون علم المالك، ويمكن للبرامج الضارة أن تفعل كل شيء بدءاً من سرقة معلومات تسجيل الدخول الخاصة بك واستخدام جهاز الكمبيوتر الخاص بك لإرسال رسائل غير مرغوب فيها إلى تعطل نظام الكمبيوتر الخاص بك.
- وتتضمن عدة أنواع شائعة من البرامج الضارة برامج التجسس وبرامج تسجيل المفاتيح والفيروسات الحقيقية، وما يسمى بفيروس الفدية Ransom ware وهو أشهرها على الإطلاق.

فيروس الفدية
Ransom ware

- وتعد برامج الفدية Ransom ware -وهي شكل آخر من البرامج الضارة- نوعاً من الهجوم على التوافر، هدفه قفل وتشفير بيانات جهاز الكمبيوتر أو الجهاز -بشكل أساسي الاحتفاظ بملفاتك كرهينة- ثم طلب فدية لاستعادة الوصول.

  يجب على الضحية عادة دفع الفدية في غضون فترة زمنية محددة أو المخاطرة بفقدان الوصول إلى المعلومات إلى الأبد.
- تشمل الأنواع الشائعة من فيروسات الفدية Ransom Ware Virus برامج التشفير الخبيثة Ransomware.

المحاضرة الثالثة

سبل حماية الأمن السيبراني

Ways to protect cyber security

أجندة المحاضرة
Lecture Agenda

- كيفية اكتشاف الهجمات السيبرانية
- تدابير حماية الأمن السيبراني
- بعض النصائح الإرشادية لحماية نفسك من الهجمات الإلكترونية

- Cyber Security Breach Detection
- Cyber Security Precautions
- Cyber Attacks Protection Tips

كيفية اكتشاف الهجمات السيبرانية
Cyber security breach detection

- ليس من السهل دائماً معرفة ما إذا كان عملك قد تعرض لخرق في الأمن السيبراني، فيستخدم المهاجمون مجموعة متنوعة من الطرق لتجنب الاكتشاف والبقاء في نظامك لفترة كافية لجمع أكبر قدر ممكن من البيانات.
- في بعض الأحيان قد يستغرق الأمر شهوراً -وغالباً لفترة أطول- لإدراك حدوث هجوم، وبحلول هذه المرحلة قد يكون المهاجمون قد تسببوا بالفعل في أضرار جسيمة لعملك أو عملائك.

كيفية اكتشاف الهجمات السيبرانية
Cyber security breach detection

ويعد اكتشاف الهجمات الإلكترونية تحدياً حتى بالنسبة للخبراء، ولكن قد تشير بعض علامات التحذير إلى حدوث اختراق أو اختراق إلكتروني.

على سبيل المثال

- نشاط الشبكة المشبوه (مثل عمليات نقل الملفات الغريبة أو محاولات تسجيل الدخول).
- تغييرات مفاجئة في البنية التحتية الحيوية Vital Infrastructure أو كلمات مرور النظام Passwords والحسابات.
- الملفات المشبوهة في نظامك، والتي ربما تم تشفيرها أو لم يتم تشفيرها.
- الأنشطة والمعاملات المصرفية المشبوهة.

كيفية اكتشاف الهجمات السيبرانية
Cyber security breach detection

ويعد اكتشاف الهجمات الإلكترونية تحدياً حتى بالنسبة للخبراء، ولكن قد تشير بعض علامات التحذير إلى حدوث اختراق أو اختراق إلكتروني.

على سبيل المثال

- فقدان غير مبرر للوصول إلى شبكتك أو بريدك الإلكتروني أو حساباتك على وسائل التواصل الاجتماعي.
- تسرب بيانات العملاء أو قوائم العملاء أو أسرار الشركة.
- اتصالات الإنترنت بطيئة بشكل غير عادي والوصول المتقطع للشبكة.
- علامات الخطأ أو التحذيرات في المتصفحات أو أدوات مكافحة الفيروسات أو مكافحة البرامج الضارة التي تنبهك إلى الإصابات.

كيفية اكتشاف الهجمات السيبرانية
Cyber security breach detection

وإذا كان لديك موقع ويب خاص بالعمل؛ فيجب عليك مراقبته بحثاً عن أي حالات شاذة قد تشير إلى احتمال وجود هجوم قيد التقدم.

على سبيل المثال:

- التناقضات غير المبررة أو الإضافات المشكوك فيها في التعليمات البرمجية الخاصة بك.
- مشاكل تتعلق بتسجيل الدخول الإداري أو الوصول إلى وظائف الإدارة.
- تغييرات غير مبررة في حجم حركة المرور (مثل الانخفاض المفاجئ والحاد).
- تغييرات غير مبررة في تصميم أو تخطيط أو محتوى موقعك.
- مشكلات الأداء التي تؤثر على توفر موقع الويب الخاص بك وإمكانية الوصول إليه.

تدابير حماية الأمن السيبراني
Cyber Security Measures

استخدام كلمات مرور
قوية

التحكم في
الوصول

استخدام برامج
الأمان

وضع جدار
حماية

مراقبة
التسلل

حماية مواقع الويب

حماية أمن
الخوادم

رفع مستوى الوعي
الرقمي

استخدام كلمات مرور قوية
Use Strong Passwords

تعد كلمات المرور القوية أمراً حيوياً للأمان الجيد عبر الإنترنت.

اجعل كلمة مرورك صعبة التخمين من خلال:

- استخدام مجموعة من الأحرف الكبيرة والصغيرة والأرقام والرموز مما يجعل طولها يتراوح بين ثمانية و 12 حرفاً.
- تجنب استخدام البيانات الشخصية.
- تغييره بانتظام.
- عدم استخدامه لحسابات متعددة.
- استخدام المصادقة الثنائية Two-factor authentication.

التحكم في الوصول
Control access

تأكد من أن الأفراد يمكنهم الوصول إلى البيانات والخدمات المصرح لهم بها فقط.

على سبيل المثال، يمكنك:

- التحكم في الوصول المادي إلى شبكة المباني وأجهزة الكمبيوتر.
- تقييد الوصول إلى المستخدمين غير المصرح لهم.
- تقييد الوصول إلى البيانات أو الخدمات من خلال ضوابط التطبيق.
- تقييد ما يمكن نسخه من النظام وحفظه في أجهزة التخزين.
- تقييد إرسال واستلام أنواع معينة من مرفقات البريد الإلكتروني.

ستساعدك أنظمة التشغيل وبرامج الشبكة الحديثة على تحقيق معظم ذلك، ولكنك ستحتاج إلى إدارة تسجيل المستخدمين وأنظمة مصادقة المستخدم Authentication - مثل كلمات المرور.

استخدام برامج الأمان
Use security software

- يجب عليك استخدام برامج الأمان، مثل برامج مكافحة التجسس والبرامج الضارة وبرامج مكافحة الفيروسات، للمساعدة في اكتشاف التعليمات البرمجية الضارة Malware وإزالتها إذا انزلقت إلى شبكتك.
- يجب عليك تحديث البرامج والأنظمة بانتظام فتحتوي التحديثات على ترقيات أمان حيوية تساعد في الحماية من الأخطاء ونقاط الضعف المعروفة، وتأكد من تحديث برامجك وأجهزتك باستمرار لتجنب الوقوع فريسة للمجرمين.

وضع جدار حماية
Put up a firewall

- تعد جدران الحماية firewall بمثابة حراس بوابات فعالة بين جهاز الكمبيوتر والإنترنت، وهي أحد العوائق الرئيسية التي تحول دون انتشار التهديدات السيبرانية مثل الفيروسات والبرامج الضارة Malware.
- تأكد من إعداد أجهزة جدار الحماية بشكل صحيح، وتحقق منها بانتظام للتأكد من تثبيت آخر تحديثات البرامج، أو أنها قد لا تكون فعالة تماماً.

مراقبة التسلل
Intrusion control

يمكنك استخدام أجهزة كشف التسلل لمراقبة النظام وأنشطة الشبكة غير العادية.

إذا اشتبه نظام الكشف في وجود خرق أمني محتمل، فيمكنه إصدار إنذار، مثل تنبيه عبر البريد الإلكتروني، بناءً على نوع النشاط الذي حدده.

حماية أمن الخوادم
Server security

الخوادم Servers عبارة عن أجهزة كمبيوتر قوية توفر خدمة واحدة أو أكثر (مثل البريد الإلكتروني أو الويب أو خوادم الملفات File servers) للمستخدمين على شبكة معينة، كثيراً ما يستهدف مجرمو الإنترنت الخوادم بسبب طبيعة البيانات الحساسة التي يحتفظون بها غالباً.

حماية أمن الخوادم
Server security

يركز أمن الخادم Server security على حماية البيانات والموارد الموجودة على الخوادم،
وهي تشتمل على أدوات وتقنيات تساعد في منع عمليات التطفل والقرصنة والإجراءات الضارة الأخرى.

- قد يتطلب تأمين Servers الكبيرة والمعقدة مهارات متخصصة، ومع ذلك يجب على أي شركة تستخدم Server أن تكون على دراية بالمخاطر -على الأقل- أن تستخدم تدابير الأمان الإلكترونية الأساسية.
- يمكن أن تساعدك الممارسات الإدارية الجيدة في تحسين أمان الشبكة والخادم الخاص بشركتك.

حماية أمن الخوادم
Server security

وإذا كنت لا تستخدم مركز بيانات آمن لاستضافة الخوادم الخاصة بك؛ فيجب عليك:

- ابقهم مقفلين.
- مراقبة وتقييد الوصول إليها.
- مراقبة تقارير الخادم، مثل سجلات الأمان.
- تقييم بيئتهم لمخاطر أخرى، مثل درجة الحرارة والنار.
- الحفاظ على مصدر طاقة مستقر.

رفع مستوى الوعي الرقمي
Raise awareness

- تحمل موظفوك مسؤولية المساعدة في الحفاظ على أمان عملك.
- تأكد من فهمهم لدورهم وأي سياسات وإجراءات ذات صلة.
- عليك تزويدهم بالتوعية والتدريب المنتظمين في مجال الأمن السيبراني.

بعض النصائح الإرشادية
لحماية نفسك من الهجمات الإلكترونية
Cyber attacks Protection Tips

بعض النصائح الإرشادية لحماية نفسك من الهجمات الإلكترونية
Cyber attacks Protection Tips

يمكن تقليل مخاطر الجرائم الإلكترونية باتباع الخطوات التالية:

- تطوير سياسات وإجراءات واضحة للأعمال والموظفين.
- وضع خطط إدارة الاستجابة لحوادث الأمن السيبراني لدعم هذه السياسات والإجراءات.
- تحديد التدابير الأمنية المطبقة حول كيفية حماية الأنظمة وبيانات الشركة.
- استخدام تطبيقات المصادقة الثنائية Two-factor authentication أو مفاتيح الأمان المادية.
- تفعيل المصادقة الثنائية Two-factor authentication على كل حساب عبر الإنترنت عندما يكون ذلك ممكناً.
- التحقق شفهياً من صحة طلبات إرسال الأموال من خلال التحدث إلى مدير مالي.
- إنشاء قواعد نظام الكشف عن التطفل (IDS) التي تحدد رسائل البريد الإلكتروني ذات الامتدادات المشابهة لرسائل البريد الإلكتروني للشركة.

بعض النصائح الإرشادية لحماية نفسك من الهجمات الإلكترونية
Cyber attacks Protection Tips

- التدقيق بعناية في جميع طلبات البريد الإلكتروني الخاصة بتحويل الأموال لتحديد ما إذا كانت الطلبات خارجة عن المألوف.
- تدريب الموظفين باستمرار على سياسات وإجراءات الأمن السيبراني وما يجب القيام به في حالة حدوث انتهاكات أمنية.
- الحفاظ على تحديث مواقع الويب وأجهزة نقطة النهاية والأنظمة بجميع تحديثات أو تصحيحات إصدارات البرامج، ونسخ البيانات والمعلومات احتياطياً بشكل منتظم لتقليل الضرر في حالة حدوث هجوم فدية أو خرق للبيانات.
- كما يمكن أيضاً بناء أمن المعلومات ومقاومة هجمات الجرائم الإلكترونية عن طريق تشفير جميع الأقراص الثابتة المحلية وأنظمة البريد الإلكتروني الخاصة بأجهزة الكمبيوتر، وذلك باستخدام شبكة افتراضية خاصة (VPN) وباستخدام خادم نظام مجال آمن (DNS).

بعض النصائح الإرشادية لحماية نفسك من الهجمات الإلكترونية
Cyber attacks Protection Tips

ومن الناحية الشخصية عليك اتباع الآتي:

- استخدم فقط المواقع الموثوقة عند تقديم معلوماتك الشخصية، فمن القواعد الأساسية الجيدة ا لتحقق من عنوان URL إذا كان الموقع يتضمن (https: //) فهذا يعني أنه موقع آمن.
- إذا كان عنوان URL يتضمن (http: //) لاحظ (s) المفقودة، تجنب إدخال معلومات حساسة مثل بيانات بطاقة الائتمان أو رقم الضمان الاجتماعي.
- لا تفتح مرفقات البريد الإلكتروني أو تنقر فوق الروابط في رسائل البريد الإلكتروني من مصادر غير معروفة، فمن أكثر الطرق شيوعاً التي تتعرض بها الشبكات والمستخدمون للبرامج الضارة والفيروسات من خلال رسائل البريد الإلكتروني المتخفية على أنها مرسلة من قبل شخص تثق به.

بعض النصائح الإرشادية لحماية نفسك من الهجمات الإلكترونية
Cyber attacks Protection Tips

- احرص دائماً على تحديث أجهزتك، فتحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح الثغرات الأمنية، كما يمكن للمهاجمين عبر الإنترنت أيضاً استهداف الأجهزة القديمة التي قد لا تعمل بأحدث برامج الأمان.
- قم بنسخ ملفاتك احتياطياً بانتظام للحصول على حماية إضافية في حالة حدوث هجمات أمنية على الإنترنت، فإذا كنت بحاجة إلى مسح جهازك نظيفاً بسبب هجوم إلكتروني؛ فسيساعدك تخزين ملفاتك في مكان آمن ومنفصل.
- يتطور الأمن السيبراني باستمرار، مما يجعل من الصعب مواكبة آخر المستجدات.
- يعد الإبقاء على الحذر في استخدام الإنترنت من أفضل الطرق للمساعدة في حماية نفسك وشبكاتك وأجهزتك وعملك.

شكراً لكم