تأمين المعلومات في عصر السيبرانيه

م. شوق حمود العنزي
ماجستير العلوم في الامن السيبراني

المحاور:

01 مقدمه عن المعلومات.

02 امن المعلومات والامن السيبراني.

03 اسس امن المعلومات.

04 امن البريد الالكتروني.

05 التعريف بالمخاطر والتهديدات الامنية وتقليل اثرها.

06 تأمين المعلومات في عصر الامن السيبراني.

07 التعرف على دور الموظف في حماية معلومات المنظمه وانظمتها.

ماهي المعلومات؟

البيانات التي تمت معالجتها واصبحت ذات معنى/ قيمة

مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها عبر الشبكة اصبح النظر لأمن المعلومات امر مهم للغاية

ماهو امن المعلومات

هو مجموعة من السياسات والتقنيات التي تهدف إلى حماية المعلومات من أي تهديدات قد تؤدي إلى تسريبها، تدميرها، أو تعديلها بدون إذن.

ماهو الامن السيبراني

هو مجموعة من التدابير والإجراءات التي يتم اتخاذها لحماية الأنظمة الرقمية، مثل الشبكات، الحواسيب، التطبيقات، و البيانات، من الهجمات التي قد تأتي عبر الإنترنت أو أي بيئة رقمية أخرى.

اسس امن المعلومات

السرية

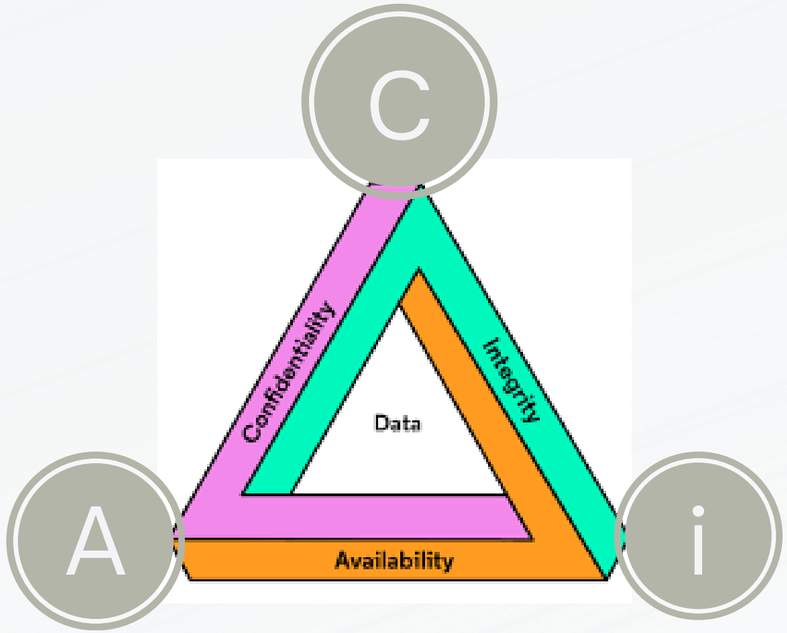
حماية المعلومات الهامة
وصلاحيات الاطلاع

التوافر والاتاحة

الحفاظ على توفر المعلومات مع امكانية
الحصول عليها

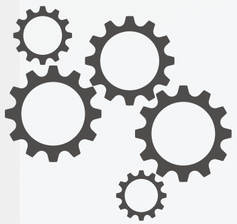
سلامة المعلومات

التأكد من ان المعلومة لم يتم
التعديل او اضافة او حذف جزء منها



مالذي يهدد امن المعلومات؟

- **الهجمات السيبرانية**: مثل الاختراقات، والفيروسات، وهجمات "برامج الفدية".



- **الهندسة الاجتماعية**: مثل التصيد الاحتيالي الذي يخدع الموظفين لكشف معلومات حساسة.

- **فقدان الأجهزة والكوارث الطبيعية:** مثل فقدان أو سرقة الأجهزة أو التأثيرات الناتجة عن الكوارث.

- **التسريبات الداخلية**: سواء من خلال إهمال الموظفين أو خيانة الثقة.

الأخطاء الأكثر شيوعًا في أمن المعلومات تشمل:

be secure

- **استخدام كلمات مرور ضعيفة**: مثل الكلمات السهلة أو المتكررة، مما يسهل على المهاجمين اختراق الحسابات.
- **عدم تحديث البرمجيات:** تجاهل التحديثات الأمنية للبرمجيات والأنظمة، مما يترك ثغرات يمكن استغلالها.
- **عدم الوعي الأمني**: غياب التدريب والتوعية بين الموظفين حول ممارسات الأمان الأساسية، مما يؤدي إلى تصيد احتيالي أو سوء استخدام المعلومات.
- **البيانات غير المشفرة**: تخزين أو نقل بيانات حساسة دون تشفير، مما يزيد من خطر التعرض للسرقة.
- **الإفراط في الوصول**: منح الموظفين صلاحيات وصول أكثر من اللازم، مما يزيد من فرص التسريبات أو الاستخدام غير المصرح به.
- **عدم وجود نسخ احتياطية:** عدم القيام بنسخ احتياطية للبيانات، مما يؤدي إلى فقدان المعلومات في حالة حدوث هجوم أو فشل النظام.
- **استخدام شبكات غير آمنة**: الاتصال بشبكات Wi-Fi عامة دون استخدام وسائل أمان مثل VPN، مما يسهل على المهاجمين اعتراض البيانات.

اثر هذه الاخطاء على الشركة

الاثر	داخلي	خارجي
المشكلة	احتواء المشكلة والتحقيق في الحادث	تأثير سلبي على سمعة الشركة
الخسائر المالية	تكاليف التحقيق والإصلاح	فقدان العملاء وتراجع المبيعات
التداعيات القانونية	دفع غرامات نتيجة عدم الامتثال للسياسات	دعاوى قانونية من العملاء.
فقدان البيانات	فقدان معلومات حساسة داخل الشركة	تسرب البيانات إلى المنافسين
تأثير على العمليات	توقف بعض العمليات أثناء معالجة المشكلة	تأثير سلبي على ثقة العملاء

دورك في امن معلومات الشركه

- اتباع السياسات الأمنية الالتزام بالقواعد والإجراءات المحددة من قبل الشركة.
- اختيار كلمات مرور صعبة وتغييرها بشكل دوري.
- الحذر من الرسائل المشبوهة عدم فتح مرفقات أو النقر على روابط من مصادر غير موثوقة.
- عدم ترك الأجهزة غير مؤمنة أو مفتوحة في أماكن عامة.
- الإبلاغ عن المشكلات و أي حوادث أو مواقف غير طبيعية على الفور.
- التعامل بحذر مع البيانات الحساسة وعدم مشاركتها مع غير المعنيين.

امن البريد الالكتروني

يعتبر البريد الإلكتروني أحد أهم وسائل الاتصال في بيئة العمل الحديثة، حيث يسهل تبادل المعلومات بين الموظفين والعملاء والشركاء.

90%

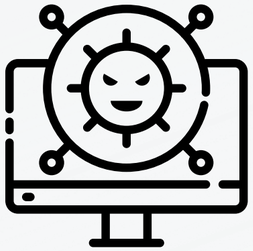
من الهجمات الإلكترونية تبدأ عبر البريد الإلكتروني، مما يجعله وسيلة شائعة للاختراق.

مصادر التهديد الامني في البريد الالكتروني

مرفقات البريد الإلكتروني الضارة

التصيد الاحتيالي (Phishing)

البرمجيات الخبيثة (Malware)



الرسائل المزعجة (Spam)

مرفقات البريد الإلكتروني الضارة

مرفقات البريد الإلكتروني الضارة هي ملفات يتم إرسالها عبر البريد الإلكتروني تحتوي على برمجيات خبيثة تهدف إلى إلحاق الضرر بجهاز الكمبيوتر أو سرقة المعلومات الحساسة. تعتبر هذه المرفقات واحدة من أبرز وسائل الهجوم التي يعتمد عليها القراصنة، وتأتي في أشكال متعددة.

- أرشيفات مضغوطة
- ملفات PDF
- مستندات معالجة الكلمات
- ملفات التنفيذ (EXECUTABLE FILES)

التصيد الاحتيالي (PHISHING)

التصيد الاحتيالي هو نوع من الهجمات الإلكترونية يُستخدم للحصول على معلومات حساسة مثل كلمات المرور، أرقام بطاقات الائتمان، والبيانات الشخصية من الأفراد. تعتمد هذه التقنية على خداع الضحايا ليعتقدوا أنهم يتعاملون مع جهة موثوقة.

التصيد عبر الشبكات الاجتماعية

التصيد عبر الرسائل النصية SMISHING

التصيد عبر الهاتف VISHING

التصيد المستهدف (SPEAR PHISHING)

البرمجيات الخبيثة (MALWARE)

البرمجيات الخبيثة، أو malware، هي مصطلح يشمل جميع أنواع البرمجيات المصممة لإلحاق الضرر بنظام الكمبيوتر، أو سرقة المعلومات، أو التسبب في أي نوع من الأذى. يُعتبر malware تهديدًا خطيرًا للأفراد والشركات على حد سواء.

أنواع البرمجيات الخبيثة

- الفيروسات (Viruses)
- الديدان (Worms)
- البرمجيات الفدية (Ransomware)
- Trojan Horses (الخيل الطروادة)
- Spyware (برامج التجسس)
- Adware (برامج الإعلانات)
- Rootkits

الرسائل المزعجة (SPAM)

الرسائل المزعجة، أو spam، هي رسائل بريد إلكتروني غير مرغوب فيها تُرسل عادةً بكميات كبيرة إلى مجموعة كبيرة من الأشخاص. غالبًا ما تكون هذه الرسائل تجارية أو تحتوي على محتوى غير مهم، وقد تشمل روابط ضارة أو معلومات مضللة.

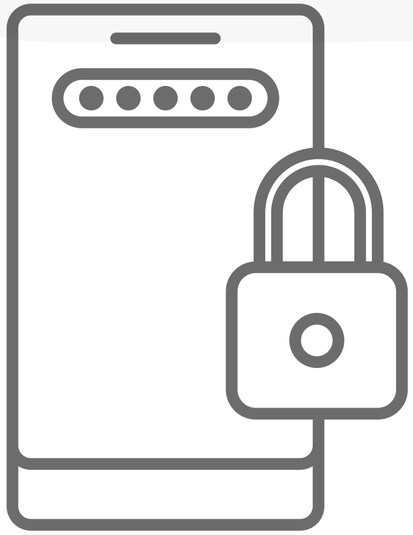
أنواع الرسائل المزعجة

- الإعلانات التجارية
- الرسائل الاحتيالية
- البرامج الضارة
- التصيد الاحتيالي (Phishing)

التعامل مع تهديدات البريد الإلكتروني

1. توفير برامج تدريبية دورية للموظفين
2. برامج مكافحة الفيروسات
3. المصادقة الثنائية (2FA)
4. تحديثات الأمان
5. استخدام كلمات مرور قوية
6. تغيير كلمات المرور بشكل دوري

نصائح لكلمة مرور قوية



- يجب أن تكون كلمة المرور طويلة، حيث من الأفضل أن تتكون من 12 حرفًا على الأقل.
- استخدم مزيجاً من الأحرف الكبيرة والصغيرة والأرقام والرموز.
- لا تقم أبداً بإعادة استخدام نفس كلمة المرور فى عدة مواقع، وحدد كلمة مرور مختلفة لكل حساب.
- لا تستخدم بدائل الرموز، مثل الرمز @ للحرف A فهذا الأمر ليس نافعاً حيث يمكن تخمينه بسهولة من خلال أدوات القرصنة التى تجرب هذه الأنواع من البدائل تلقائياً.
- لا تستخدم كلمات أو عبارات شائعة، أو لها أهمية شخصية بالنسبة لك مثل أسماء أفراد العائلة، أو تاريخ ميلادك، حيث يمكن الوصول إلى كلمة السر فى هذه الحالة بسهولة.

تأمين المعلومات في عصر الأمن السيبراني

1. أهمية تأمين المعلومات

- حماية البيانات الحساسة
- حماية السمعة المؤسسية
- منع سرقة الهوية
- الامتثال للقوانين

تأمين المعلومات في عصر الأمن السيبراني

2. التحديات التي تواجه تأمين المعلومات في العصر السيبراني

الهجمات المتطورة

التهديدات الداخلية

التقنيات الحديثة

الاستجابة السريعة للحوادث

تأمين المعلومات في عصر الأمن السيبراني

3. استراتيجيات تأمين المعلومات

أ. الحماية على مستوى الشبكات

- جدران الحمايه
- انظمة كشف التسلل \ انظمة منع التسلل
- التشفير
- التوثيق متعدد العوامل

ب. الحماية على مستوى الأجهزة

- برامج مكافحة الفيروسات
- التحديثات الدورية لنظام

ج. الحماية على مستوى التطبيقات

- اختبارات الامان
- التشفير داخل التطبيقات
- تحليل كود المصدر

د. التدريب والتوعية الأمنية

- التدريب على كيفية التعرف على رسائل التصيد الاحتيالي
- التدريب على استخدام كلمات مرور قوية
- التوعية بأهمية تحديث البرامج

دور الموظف في حماية معلومات المنظمة وأنظمتها

1. الالتزام بسياسات الأمان
2. التفاعل مع البريد الإلكتروني والتقنيات الرقمية بحذر
3. الحذر عند استخدام الأجهزة الشخصية (BYOD)
4. تطبيق المبادئ الأساسية للأمن السيبراني
5. التدريب والتوعية الأمنية المستمرة
6. الإبلاغ عن الأنشطة المشبوهة
7. مشاركة المسؤولية الجماعية في حماية المعلومات

شكراً لإستماعكم

الاجابه على اسئلتكم

معلومات التواصل:

شوق حمود العنزي

shoog1417hmood@gmail.com

shouq210