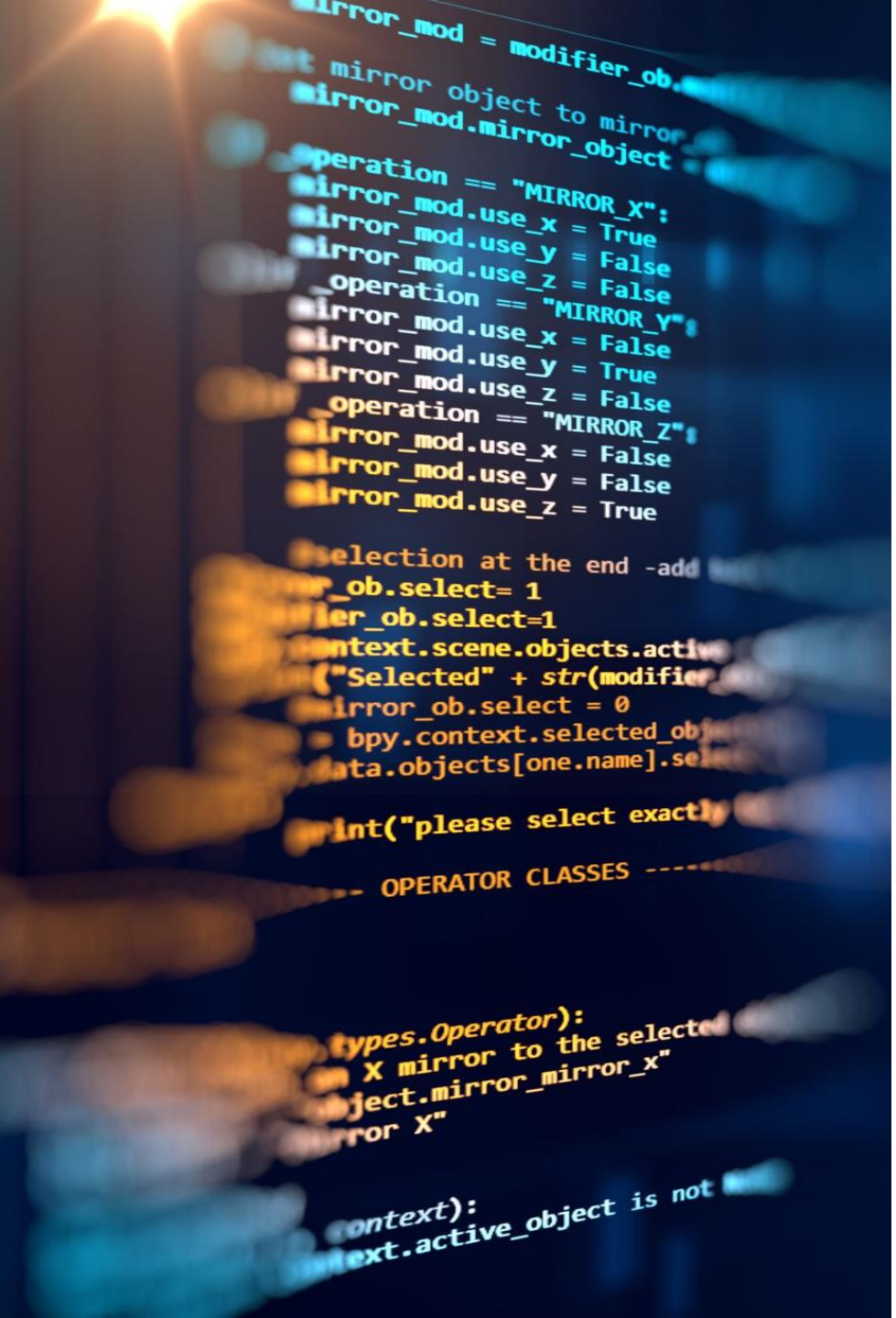
100Cyber-3: Cybersecurity Foundation

Dr. Mohammed Alshahrani
moaalshahrani@nu.edu.sa

Second Lecture

Sunday, Sep. 29 2024



Today…

- مفاهيم بالأمن السيبراني
- الفرق بين أمن المعلومات والأمن السيبراني
- أهداف الأمن السيبراني
- ابرز مخاطر الأمن السيبراني
- انواع الهجمات في الأمن السيبراني
- اسالِيب هجمات الإختراق السيبراني
- اجراءات الوقاية من الإختراق السيبراني
- مخاطر الفضاء السيبراني على الأطفال خصوصا و الشباب
- وصايا للحفاظ على صغار السن من الفضاء السيبراني
- وصايا حول اختيار كلمة المرور
- كيف تحمي بيانات المؤسسة من الاختراق السيبراني

اجراءات الوقاية من الاختراق السيبراني

هناك العديد من الإجراءات التي يمكن اتخاذها للوقاية من الاختراقات السيبرانية. تعتمد هذه الإجراءات على تقنيات متعددة ونهج شامل يشمل تعزيز أمان الأنظمة والشبكات والبيانات، بالإضافة إلى توعية المستخدمين وتحسين العمليات. فيما يلي أهم **إجراءات الوقاية من الاختراق السيبراني**:

اجراءات الوقاية من الاختراق السيبراني

1. **استخدام كلمات مرور قوية وآمنة**

- **تجنب كلمات المرور الشائعة** مثل "123456" أو "password".
- **استخدام كلمات مرور معقدة** تحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز.
- **استخدام مدير كلمات المرور** لتخزين كلمات المرور بأمان وإنشاء كلمات مرور قوية وفريدة لكل حساب.

اجراءات الوقاية من الاختراق السيبراني

2. تفعيل المصادقة متعددة العوامل (Multi-Factor Authentication - MFA)

- إضافة طبقة حماية إضافية بجانب كلمة المرور، مثل رمز يتم إرساله إلى الهاتف المحمول أو استخدام تطبيق مصادقة مثل Google Authenticator.
- يساعد ذلك في منع الدخول غير المصرح به حتى إذا تم اختراق كلمة المرور.

3. تحديث البرمجيات والأنظمة بانتظام

- تطبيق تحديثات الأمان والإصدارات الجديدة لأنظمة التشغيل والبرامج بانتظام، بما في ذلك تحديثات المتصفحات والبرامج المضادة للفيروسات.
- سد الثغرات الأمنية المعروفة التي يمكن أن يستغلها المهاجمون.

اجراءات الوقاية من الاختراق السيبراني

4. استخدام برامج مكافحة الفيروسات والجدران النارية (Firewalls)

- تثبيت برامج مكافحة الفيروسات وتحديثها بانتظام للكشف عن البرمجيات الخبيثة وإزالتها.
- تفعيل الجدران النارية (Firewalls) لحماية الشبكة من الوصول غير المصرح به.

5. تشفير البيانات (Data Encryption)

- تشفير البيانات أثناء النقل والتخزين، سواء كانت على أجهزة محلية أو على السحابة.
- استخدام بروتوكولات التشفير الآمنة مثل HTTPS لتأمين الاتصالات عبر الإنترنت.

اجراءات الوقاية من الاختراق السيبراني

6. التوعية والتدريب الأمني للمستخدمين

- تدريب الموظفين والمستخدمين على أفضل ممارسات الأمن السيبراني مثل التعرف على رسائل التصيد الاحتيالي والتعامل مع البيانات الحساسة.
- إجراء حملات توعية دورية لتحديث المعلومات حول أحدث التهديدات وأساليب الهجوم.

7. إجراء النسخ الاحتياطي للبيانات (Data Backup)

- إجراء نسخ احتياطي منتظم للبيانات الهامة على وسائط منفصلة مثل الأقراص الصلبة الخارجية أو السحابة.
- التأكد من أن النسخ الاحتياطية محمية وغير متصلة بالشبكة لمنع تلفها أو الوصول إليها في حال حدوث هجوم ببرمجيات الفدية.

اجراءات الوقاية من الاختراق السيبراني

8. تطبيق سياسات إدارة الوصول (Access Management)

- تحديد صلاحيات الوصول بناءً على الحاجة الوظيفية (Need to Know) لمنع الوصول غير المصرح به إلى المعلومات الحساسة.
- مراجعة وإلغاء صلاحيات الوصول للمستخدمين الذين لم يعودوا بحاجة إليها، مثل الموظفين الذين غادروا الشركة.

9. استخدام الشبكات الافتراضية الخاصة (VPN)

- استخدام شبكة افتراضية خاصة (VPN) لتأمين الاتصالات عبر الإنترنت، خاصة عند الاتصال من شبكات غير آمنة مثل شبكات Wi-Fi العامة.
- تشفير حركة البيانات بين الجهاز والشبكة لتقليل فرص التنصت والتجسس.

اجراءات الوقاية من الاختراق السيبراني

10. إجراء اختبارات الاختراق والتقييمات الأمنية (Penetration Testing)

- إجراء اختبارات اختراق دورية لتحديد نقاط الضعف في الأنظمة والشبكات وتصحيحها قبل أن يستغلها المهاجمون.
- استخدام فرق مختصة لتقييم أمان الشبكة والتأكد من تنفيذ الضوابط الأمنية بفعالية.

11. تطبيق سياسات التحديث التلقائي والتصحيح (Patch Management)

- تطبيق تصحيحات الأمان والتحديثات بشكل تلقائي أو بشكل منتظم على جميع الأنظمة والبرمجيات المستخدمة.
- التأكد من أن جميع الأنظمة، بما في ذلك الأجهزة والبرمجيات، محدثة بشكل مستمر لتفادي الاستغلال.

اجراءات الوقاية من الاختراق السيبراني

12. تطبيق آليات المراقبة والكشف (Monitoring & Detection)

- استخدام أنظمة مراقبة الشبكات والأنظمة للكشف المبكر عن الأنشطة المشبوهة أو التهديدات المحتملة.
- تحليل سجلات الأنشطة (Logs) بانتظام للكشف عن الأنشطة غير الطبيعية وإجراء التحقيقات اللازمة.

13. إنشاء خطة استجابة للحوادث (Incident Response Plan)

- وضع خطة واضحة ومفصلة للتعامل مع الحوادث السيبرانية، تشمل كيفية تحديد الحادث، احتوائه، معالجته، واستعادة الأنظمة.
- تدريب الفريق المختص على كيفية التعامل مع الحوادث وإجراء تمارين محاكاة بانتظام.

اجراءات الوقاية من الاختراق السيبراني

14. استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي

- استخدام أدوات متقدمة تعتمد على الذكاء الاصطناعي والتعلم الآلي لتحليل الأنماط السلوكية وكشف الهجمات المعقدة مثل التهديدات المتقدمة المستمرة (APT).
- تكامل هذه الأدوات مع أنظمة الكشف عن التسلل (IDS) وأنظمة منع التسلل (IPS) لتحسين مستوى الأمان.

15. تقييد استخدام الأجهزة الشخصية (BYOD Policies)

- وضع سياسات واضحة لاستخدام الأجهزة الشخصية في بيئة العمل، مثل الهواتف المحمولة أو الأجهزة اللوحية.
- استخدام أدوات إدارة الأجهزة المحمولة (MDM) لتأمين البيانات والتحكم في الوصول إليها من خلال هذه الأجهزة.

اجراءات الوقاية من الاختراق السيبراني

الخلاصة:

- هذه الإجراءات الوقائية تشكل جزءًا من استراتيجية شاملة للأمن السيبراني. يجب على المؤسسات والأفراد العمل معًا لتطبيق هذه التدابير وتعزيز الوعي الأمني باستمرار لضمان حماية الأنظمة والمعلومات من الاختراقات السيبرانية.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

مخاطر الفضاء السيبراني على الأطفال والشباب تعتبر من القضايا الهامة التي تحتاج إلى اهتمام وتوعية. مع زيادة استخدام الأطفال والشباب للإنترنت ووسائل التواصل الاجتماعي، تزداد احتمالية تعرضهم للعديد من المخاطر السيبرانية التي قد تؤثر على سلامتهم النفسية والجسدية وحتى الاجتماعية. فيما يلي أبرز هذه المخاطر:

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

1. التنمر الإلكتروني (Cyberbullying)

- **التنمر الإلكتروني** هو استخدام الإنترنت، وسائل التواصل الاجتماعي، أو الرسائل النصية للإساءة، التهديد، أو مضايقة الآخرين.
- **أمثلة:**
  - إرسال رسائل مؤذية أو تهديدات.
  - نشر إشاعات أو معلومات شخصية محرجة على الإنترنت.
  - إنشاء حسابات وهمية للاستهزاء أو السخرية من الآخرين.
- **الآثار:** يمكن أن يؤدي التنمر الإلكتروني إلى مشكلات نفسية خطيرة مثل القلق، الاكتئاب، وحتى التفكير في الانتحار.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

2. التحرش والاستغلال الجنسي (Online Predation)

- يواجه الأطفال خطر التعرض للتحرش الجنسي أو الاستغلال من قبل أشخاص يتظاهرون بأنهم أصدقاء أو شركاء.
- **أمثلة:**
  - التواصل مع الأطفال عبر وسائل التواصل الاجتماعي أو الألعاب الإلكترونية لمحاولة كسب ثقتهم والحصول على صور أو معلومات شخصية.
  - طلب اللقاءات الشخصية بعد فترة من بناء علاقة ثقة مزيفة.
- **الآثار:** قد يتعرض الطفل لمواقف خطيرة تتعلق بالتحرش الجنسي أو الاستغلال، مما يؤثر على سلامته النفسية والجسدية.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

3. الوصول إلى محتوى غير مناسب (Inappropriate Content)

- الإنترنت يحتوي على كميات هائلة من المحتوى غير المناسب للأطفال، مثل المحتوى العنيف، الإباحي، أو المحرض على الكراهية.
- **أمثلة:**
  - مشاهدة مقاطع فيديو تحتوي على مشاهد عنف أو إيذاء للنفس.
  - الوصول إلى مواقع تحتوي على محتوى إباحي أو تعليمي خاطئ.
- **الآثار:** قد يؤثر التعرض لمثل هذا المحتوى على تطور الطفل العقلي والنفسي، مما يؤدي إلى سلوكيات غير لائقة أو مشكلات اجتماعية.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

4. الإدمان على الإنترنت والألعاب الإلكترونية (Internet and Gaming Addiction)

- يقضي الأطفال والشباب ساعات طويلة على الإنترنت أو الألعاب الإلكترونية، مما قد يؤدي إلى الإدمان.
- **أمثلة:**
  - قضاء ساعات طويلة في لعب الألعاب الإلكترونية دون التفاعل مع العائلة أو الأصدقاء.
  - إهمال الدراسة أو الأنشطة اليومية بسبب التعلق بالإنترنت أو الألعاب.
- **الآثار:** الإدمان على الإنترنت قد يؤدي إلى مشكلات صحية مثل ضعف النظر، السمنة، والعزلة الاجتماعية، وكذلك التأثير على الأداء الأكاديمي.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

5. التصيد والاحتيال الإلكتروني (Phishing and Scams)

- يمكن للأطفال والشباب أن يكونوا أهدافًا سهلة لهجمات التصيد الاحتيالي والاحتيال عبر الإنترنت.
- **أمثلة:**
  - تلقي رسائل بريد إلكتروني أو رسائل على وسائل التواصل الاجتماعي تحتوي على روابط خبيثة.
  - استغلال الأطفال للحصول على معلومات شخصية أو مالية من خلال مواقع ومسابقات مزيفة.
- **الآثار:** قد يتم سرقة معلومات شخصية أو مالية، مما يعرض الأطفال وعائلاتهم لمشكلات مالية وقانونية.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

6. سرقة الهوية والانتحال (Identity Theft and Impersonation)

- يمكن للمهاجمين استخدام المعلومات الشخصية للأطفال لإنشاء حسابات مزيفة أو القيام بأنشطة غير قانونية.
- **أمثلة:**
  - سرقة بيانات الدخول لحسابات الألعاب أو وسائل التواصل الاجتماعي.
  - انتحال هوية الطفل لطلب المال أو القيام بأعمال غير قانونية باسمهم.
- **الآثار:** يمكن أن يؤدي ذلك إلى مشكلات قانونية وتشويه سمعة الطفل وعائلته.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

7. تحديات الإنترنت الخطيرة (Online Challenges and Dares)

- هناك تحديات تنتشر على الإنترنت بين الأطفال والشباب، تشجعهم على القيام بأعمال خطيرة أو غير قانونية.
- **أمثلة:**
  - تحديات مثل "تحدي الحوت الأزرق" الذي يتطلب من المشاركين القيام بأعمال مؤذية لأنفسهم.
  - تحديات ترويج العنف أو التحديات التي تتطلب منهم القيام بأعمال خطيرة لتصويرها ونشرها.
- **الآثار:** يمكن أن يؤدي اتباع هذه التحديات إلى إصابات جسدية، مشكلات نفسية، أو حتى الموت.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

8. المخاطر النفسية والاجتماعية (Psychological and Social Risks)

- التعرض المستمر للمحتوى السلبي، العزلة الاجتماعية، أو التفاعل السلبي على الإنترنت يمكن أن يؤدي إلى مشكلات نفسية واجتماعية.
- **أمثلة:**
  - الشعور بالقلق أو الاكتئاب بسبب المقارنة الدائمة مع الآخرين.
  - الإحساس بالوحدة أو العزلة بسبب قضاء الكثير من الوقت على الإنترنت.
- **الآثار:** يمكن أن تؤدي هذه المشكلات إلى تدهور الصحة النفسية والانسحاب الاجتماعي.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

9. مخاطر الألعاب الإلكترونية (Online Gaming Risks)

- الألعاب الإلكترونية التفاعلية قد تكون مكانًا لاستدراج الأطفال من قبل غرباء أو التعرض للتنمر.
- **أمثلة:**
  - تعرض الأطفال للغة غير لائقة أو سلوكيات عدوانية من قبل لاعبين آخرين.
  - استدراج الأطفال لكشف معلومات شخصية أثناء اللعب.
- **الآثار:** يمكن أن تؤثر هذه المخاطر على الصحة النفسية للطفل، وتزيد من مخاطر الاستغلال أو التحرش.

مخاطر الفضاء السيبراني على الأطفال خصوصا والشباب

الخلاصة:

- حماية الأطفال والشباب من مخاطر الفضاء السيبراني تتطلب تعاونًا بين الأهل، المدرسة، والمجتمع. من خلال التوعية والمراقبة المستمرة، يمكن تقليل هذه المخاطر وضمان بيئة آمنة لهم للاستفادة من الإنترنت بشكل إيجابي وآمن.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

مجموعة من الوصايا والإرشادات للحفاظ على صغار السن من مخاطر الفضاء السيبراني، وهي تهدف إلى توجيه الآباء والأمهات والمعلمين لتوفير بيئة آمنة للأطفال عند استخدامهم للإنترنت:

وصايا للحفاظ على صغار السن من الفضاء السيبراني

1. التواصل المفتوح والمستمر

- تحدث مع الأطفال بانتظام حول أنشطتهم عبر الإنترنت. اسألهم عن المواقع التي يزورونها، والأشخاص الذين يتواصلون معهم، وما إذا كانوا قد تعرضوا لأي شيء غير مريح.
- شجع الأطفال على الشعور بالراحة في التحدث إليك إذا واجهوا أي شيء مشبوه أو مخيف.

2. تحديد القواعد والحدود

- ضع قواعد واضحة لاستخدام الإنترنت، بما في ذلك الأوقات المسموح بها لاستخدام الأجهزة والمواقع والتطبيقات التي يمكنهم الوصول إليها.
- حدد فترة زمنية محددة للاستخدام اليومي للإنترنت والألعاب الإلكترونية لتجنب الإدمان.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

3. استخدام أدوات الرقابة الأبوية

- استخدم برامج الرقابة الأبوية ((Parental Controlالتي تتيح لك مراقبة نشاط الأطفال عبر الإنترنت وتحديد المواقع التي يمكنهم الوصول إليها.
- تفعيل ميزات الأمان على الأجهزة التي يستخدمها الأطفال، مثل حظر المواقع غير المناسبة وتقييد التطبيقات.

4. تعليم الأطفال أساسيات الأمان السيبراني

- علّم الأطفال كيفية إنشاء كلمات مرور قوية وعدم مشاركتها مع أي شخص.
- توعية الأطفال بعدم مشاركة معلوماتهم الشخصية (مثل الاسم، العنوان، المدرسة) عبر الإنترنت، حتى مع من يزعمون أنهم أصدقاء.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

5. تحذيرهم من مخاطر الغرباء عبر الإنترنت

- حذر الأطفال من التحدث مع الغرباء على الإنترنت أو مشاركة الصور والمعلومات الشخصية معهم.
- شجعهم على عدم قبول طلبات الصداقة أو الرسائل من أشخاص لا يعرفونهم بشكل شخصي.

6. مراقبة استخدام وسائل التواصل الاجتماعي

- راقب حسابات الأطفال على وسائل التواصل الاجتماعي مثل فيسبوك، إنستغرام، تيك توك، وتأكد من أنهم لا يشاركون محتوى غير مناسب أو يتفاعلون مع أشخاص مشبوهين.
- قم بإعداد إعدادات الخصوصية للحسابات الاجتماعية لضمان عدم مشاركة المحتوى إلا مع الأصدقاء والعائلة فقط.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

7. تشجيع الاستخدام الآمن والهادف للتكنولوجيا

- وجه الأطفال نحو استخدام الإنترنت لأغراض تعليمية، مثل البحث عن المعلومات المفيدة أو المشاركة في الأنشطة التعليمية عبر الإنترنت.
- شجعهم على ممارسة الأنشطة البدنية والهوايات بعيدًا عن الشاشات، مثل الرياضة أو القراءة.

8. التحذير من مخاطر التنمر الإلكتروني (Cyberbullying)

- علم الأطفال كيفية التعامل مع التنمر الإلكتروني: لا يردوا على الرسائل المسيئة، ويخبروا شخصًا بالغًا إذا تعرضوا للتنمر.
- احرص على تعليمهم ألا يشاركوا أو ينشروا أي محتوى مسيء أو محرج لغيرهم.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

9. إعداد الأجهزة بطرق آمنة

- تأكد من أن جميع الأجهزة تحتوي على برامج مكافحة الفيروسات محدثة وجدران نارية (Firewalls) لتجنب التهديدات الأمنية.
- تثبيت متصفح آمن، واستخدام محركات بحث مخصصة للأطفال مثل *Kiddle* أو *SafeSearchKids* لضمان تجربة تصفح آمنة.

10. توعية الأطفال حول مخاطر التحديات الخطيرة

- تحدث مع الأطفال عن التحديات الخطيرة المنتشرة على الإنترنت مثل "تحدي الحوت الأزرق" أو "تحدي كيكي"، وكيفية تجنب المشاركة في مثل هذه الأنشطة الخطيرة.
- شجعهم على عدم الانسياق وراء التحديات التي يمكن أن تعرضهم للخطر أو تسبب لهم الأذى الجسدي أو النفسي.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

11. تشجيع الإبلاغ عن الأنشطة المشبوهة

- شجع الأطفال على الإبلاغ عن أي محتوى مشبوه أو سلوك مريب يشاهدونه على الإنترنت، سواء كان تنمرًا، تحرشًا، أو محاولات اختراق.
- أخبرهم أن التحدث معك أو مع معلمهم عن هذه الأمور لن يسبب لهم المتاعب بل يساعد في حمايتهم.

12. القدوة الحسنة في استخدام الإنترنت

- كن قدوة حسنة في استخدامك للإنترنت؛ تجنب قضاء ساعات طويلة على الإنترنت أمامهم، والتزم بممارسات الأمان السيبراني.
- تحدث عن تجربتك الشخصية في الحفاظ على الأمان عند استخدام الإنترنت، مثل عدم فتح الروابط المريبة أو تجنب مشاركة المعلومات الشخصية.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

13. توعية الأطفال بالمحتوى الإيجابي

- ساعد الأطفال في العثور على مواقع وتطبيقات تعليمية وإبداعية يمكنهم الاستفادة منها، مثل مواقع التعلم التفاعلي، الألعاب التعليمية، أو برامج تطوير المهارات.
- شاركهم في مشاهدة البرامج التعليمية والأفلام التي تناسب أعمارهم، وتحدثوا عن محتواها لتعزيز فهمهم.

14. وضع خطط للإنترنت العائلي

- اجتمع كأسرة لتحديد قواعد استخدام الإنترنت، مثل عدم استخدام الهواتف الذكية أثناء وقت الطعام أو تحديد أماكن معينة في المنزل لاستخدام الأجهزة الإلكترونية.
- تنظيم "أيام بدون إنترنت" حيث تشجع الأسرة على القيام بأنشطة مشتركة خارج الإنترنت مثل الرياضة، الرحلات، أو القراءة.

وصايا للحفاظ على صغار السن من الفضاء السيبراني

الخلاصة:

- حماية الأطفال في الفضاء السيبراني تتطلب التعاون والتواصل المستمر بين الآباء والأطفال. من خلال تطبيق هذه الوصايا، يمكنك تعزيز الأمان الرقمي لأطفالك، وتوجيههم نحو استخدام آمن وإيجابي للتكنولوجيا.

وصايا حول اختيار كلمة المرور

اختيار كلمة مرور قوية وآمنة هو أحد أهم التدابير التي يمكن اتخاذها لحماية الحسابات والبيانات الشخصية من الاختراق. إليك مجموعة من الوصايا حول كيفية اختيار وإدارة كلمات المرور بشكل آمن:

وصايا حول اختيار كلمة المرور

1. اختر كلمات مرور طويلة ومعقدة

- استخدم كلمات مرور لا تقل عن 12-16 حرفًا. كلما كانت الكلمة أطول، زادت صعوبتها في التخمين.
- استخدم مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة (مثل: !، @، #، $، %).

2. تجنب استخدام المعلومات الشخصية

- لا تستخدم المعلومات الشخصية في كلمات المرور مثل اسمك، تاريخ ميلادك، اسم أفراد عائلتك، أو رقم هاتفك.
- تجنب استخدام الكلمات الشائعة أو السهلة مثل "password"، "123456"، أو "qwerty".

وصايا حول اختيار كلمة المرور

3. لا تعيد استخدام كلمات المرور نفسها

- لا تستخدم نفس كلمة المرور لأكثر من حساب. إذا تم اختراق أحد الحسابات، فقد يؤدي ذلك إلى اختراق جميع حساباتك الأخرى.
- استخدم كلمة مرور فريدة لكل حساب، خصوصًا للحسابات الحساسة مثل البريد الإلكتروني أو الحسابات المصرفية.

4. استخدم جملة سرية (Passphrase)

- بدلاً من كلمة مرور تقليدية، يمكنك استخدام جملة سرية تتكون من كلمات عشوائية لكنها سهلة التذكر. على سبيل المثال: "RainySky!Orange2021"."
- يمكنك استخدام كلمات عشوائية وإضافة رموز وأرقام لجعلها أكثر أمانًا، مثل: "Tree#Happy7Moon!"."

وصايا حول اختيار كلمة المرور

5. تجنب الأنماط المتكررة أو المتوقعة

- تجنب استخدام الأنماط المتكررة مثل " "aaa111أو الكلمات المتتالية مثل "."abcd1234
- لا تستخدم التكرار مثل " "PasswordPasswordأو "123123".

6. استخدام مدير كلمات المرور (Password Manager)

- استخدم برامج إدارة كلمات المرور لتخزين وإنشاء كلمات مرور قوية وفريدة لكل حساب. هذه البرامج تحفظ كلمات المرور بشكل آمن وتسمح لك بالوصول إليها عند الحاجة.
- من أمثلة برامج إدارة كلمات المرور: LastPass، 1Password، Bitwarden.

وصايا حول اختيار كلمة المرور

7. قم بتغيير كلمات المرور بانتظام

- قم بتغيير كلمات المرور للحسابات المهمة بشكل دوري، خاصة إذا كنت تشك في أن كلمة مرورك قد تكون مكشوفة أو مخترقة.
- حدد فترات زمنية لتغيير كلمات المرور، مثل كل 3-6 أشهر للحسابات الحساسة.

8. استخدم المصادقة متعددة العوامل (MFA)

- قم بتفعيل المصادقة الثنائية (Two-Factor Authentication) أو متعددة العوامل (Multi-Factor Authentication) كلما أمكن ذلك. تضيف هذه الطبقة الإضافية من الأمان عن طريق طلب رمز تحقق إضافي يتم إرساله إلى هاتفك أو توليده بواسطة تطبيق.
- حتى لو تمت سرقة كلمة مرورك، سيكون من الصعب على المهاجم الوصول إلى حسابك دون رمز المصادقة الثاني.

وصايا حول اختيار كلمة المرور

9. تجنب استخدام كلمات المرور في الأماكن العامة

- تجنب إدخال كلمات المرور الخاصة بك على أجهزة كمبيوتر عامة أو شبكات Wi-Fi غير آمنة.
- كن حذرًا من الأشخاص المحيطين بك عند إدخال كلمة المرور، وتأكد من عدم تمكنهم من رؤيتها.

10. لا تشارك كلمات المرور مع الآخرين

- تجنب مشاركة كلمات المرور مع أي شخص، حتى مع الأصدقاء المقربين أو أفراد العائلة. إذا كان يجب مشاركة كلمة مرور، استخدم وسائل آمنة مثل تطبيقات الرسائل المشفرة، وتغييرها بعد الاستخدام.
- إذا كنت تعمل في بيئة جماعية، تجنب مشاركة حسابات مشتركة بكلمات مرور واحدة.

وصايا حول اختيار كلمة المرور

11. لا تحفظ كلمات المرور في المتصفح

تجنب حفظ كلمات المرور في المتصفح، حيث يمكن الوصول إليها بسهولة إذا تم اختراق جهازك.

استخدم مدير كلمات مرور منفصل وأكثر أمانًا لحفظ كلمات المرور.

12. تأكد من أمان الأسئلة الأمنية

عند إعداد أسئلة الأمان، اختر أسئلة يصعب على الآخرين تخمين إجابتها. تجنب استخدام أسئلة يمكن العثور على إجاباتها بسهولة، مثل "ما اسم مدرستك الابتدائية؟".

يمكنك استخدام إجابات عشوائية أو غير حقيقية وتخزينها في مدير كلمات المرور لتجنب كشفها.

وصايا حول اختيار كلمة المرور

13. اختبار قوة كلمة المرور

- استخدم أدوات اختبار قوة كلمات المرور (Password Strength Checkers) للتحقق من مدى قوة كلمة المرور التي اخترتها.
- تجنب مشاركة كلمة المرور مع هذه الأدوات، ولكن يمكنك استخدامها لإرشادك في اختيار كلمة مرور قوية.

14. احذر من برامج التسجيل (Keyloggers)

- تأكد من أن جهازك محمي ببرنامج مكافحة الفيروسات لتجنب الإصابة ببرامج تسجيل لوحة المفاتيح (Keyloggers) التي يمكنها تسجيل كل ما تكتبه، بما في ذلك كلمات المرور.
- قم بإجراء فحص دوري لجهازك للكشف عن أي برمجيات ضارة.

وصايا حول اختيار كلمة المرور

15. احفظ كلمة المرور في مكان آمن

- إذا كنت بحاجة إلى كتابة كلمة المرور لعدم القدرة على تذكرها، احتفظ بها في مكان آمن وغير مكشوف، مثل خزانة مغلقة.
- تجنب حفظ كلمات المرور على ورقة ملصقة على جهاز الكمبيوتر أو في محفظتك.

وصايا حول اختيار كلمة المرور

الخلاصة:

- اتباع هذه الوصايا يمكن أن يساعدك في إنشاء وإدارة كلمات مرور قوية وآمنة، مما يقلل من خطر تعرض حساباتك للاختراق. الأمان يبدأ بكلمة مرور جيدة وإدارتها بحذر، لذا احرص على الالتزام بهذه الإرشادات لتعزيز حماية بياناتك.

كيف تحمي بيانات المؤسسة من الاختراق السيبراني

حماية بيانات المؤسسة من الاختراق السيبراني تتطلب اتباع استراتيجية شاملة تتضمن سياسات وإجراءات تقنية وبشرية وإدارية. فيما يلي مجموعة من الإجراءات التي يمكن أن تساعد في حماية بيانات المؤسسة من التهديدات السيبرانية:

كيف تحمي بيانات المؤسسة من الاختراق السيبراني

1. تطوير سياسة أمنية شاملة ((Comprehensive Security Policy
2. تطبيق إدارة الوصول والتحكم ((Access Control Management
3. تفعيل المصادقة متعددة العوامل ((Multi-Factor Authentication - MFA
4. تشفير البيانات ((Data Encryption
5. التحديثات الأمنية المنتظمة ((Regular Security Updates
6. استخدام جدران الحماية ((Firewallsوأنظمة كشف التسلل ((IDS
7. التدريب والتوعية الأمنية ((Security Awareness Training
8. إجراء النسخ الاحتياطي الدوري ((Regular Data Backup

كيف تحمي بيانات المؤسسة من الاختراق السيبراني

9. تحديد وتطبيق بروتوكولات الاستجابة للحوادث ((Incident Response Protocols
10. تقييم واختبار الأمان بانتظام ((Regular Security Assessments
11. استخدام حلول أمان البريد الإلكتروني ((Email Security Solutions
12. تطبيق إدارة الأجهزة المتنقلة ((Mobile Device Management - MDM
13. تحديد سلوك الشبكة العادي ومراقبة الأنشطة غير الطبيعية (Network Behavior Analysis)
14. تقليل الاعتماد على المستخدمين الفرديين ((Single Points of Failure
15. إدارة سجلات الأنشطة ((Log Management
16. استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي ((AI & ML

كيف تحمي بيانات المؤسسة من الاختراق السيبراني

الخلاصة:

- تأمين بيانات المؤسسة يتطلب نهجًا متعدد الطبقات يشمل التكنولوجيا، السياسات، والتدريب.
يجب على المؤسسة تبني استراتيجيات دفاعية شاملة ومتكاملة للتعامل مع التهديدات السيبرانية المستمرة، والتأكد من أن جميع الموظفين والمكونات التقنية يساهمون في الحفاظ على الأمان السيبراني.