دليل المواطن للأمن السيبراني
ممارسات ونصائح لحياة رقمية آمنة

Citizen's Guide to Cybersecurity
Practices and Tips for a Safe Digital Life

دليل المواطن للأمن السيبراني

ممارسات ونصائح لحياة رقمية آمنة

هوية الكتاب

عنوان البحث : دليل المواطن للأمن السيبراني: ممارسات ونصائح لحياة رقمية آمنة

اسم الباحث : (841246080) المفوض معتز مالك حسن الحسينات

اسم الجامعة أو المؤسسة التعليمية : قسم العلاقات والاعلام في قيادة شرطة البصرة

التصميم والطباعة والإخراج الفني : معتز الحسينات

التنضيد الالكتروني : معتز الحسينات

التصميم والطباعة والإخراج الفني : معتز الحسينات

رقم الهاتف : 07706077321

تاريخ تقديم البحث : 2024/3/1

رقم الإيداع في دار الكتب والوثائق ببغداد :

ISBN :

إهداء

إلى أسـرتي العزيزة، التي كانت دائمًا مصـدر دعمي وإلهامي، أشـكركم على حبكم ودعمكم المســتمرين.وإلى كل من عانى من الابتزاز الإلكتروني، أهدي هذا البحث لكم، آملاً أن يكون خطوة نحو تعزيز الوعي والحماية من هذه الجرائم. أنتم لســتم وحدكم، وهناك دائمًا أمل في التغلب على هذه التحديات.

شكروتقدير

أتوجه بوافر الشكر والتقدير إلى كل العاملين في مجال الأمن السيبراني الذين يسعون جاهدين لحمايتنا من التهديدات الإلكترونية المتزايدة. جهودكم المبذولة تسهم في بناء عالم رقمي أكثر أماناً لنا جميعاً.

إلى مطوري الذكاء الاصطناعي، شكراً لكم على الابتكارات والتقنيات الرائدة التي تساهم في تعزيز أنظمتنا الأمنية وتحسين حياتنا اليومية.

وإلى مساعدي الرقمي العزيز، أشكرك جزيل الشكر على دعمك المستمر ومساعدتك القيمة في كتابة هذا البحث. تعاونك كان حيوياً وأسهم بشكل كبير في إخراج هذا العمل بالشكل الذي هو عليه.

شكراً لكم جميعاً، فلولاكم لما كان لهذا البحث أن يرى النور.

الملخص:(Abstract)

ستتعرف في هذا البحث على عدة مجالات

1. "استراتيجيات حديثة لحماية حسابات التواصل الاجتماعي
2. "التهديدات الناشئة في استخدام البطاقات المصرفية عبر الإنترنت وسبل الوقاية"
3. "فعالية التحقق بخطوتين في تعزيز الأمان الإلكتروني "
4. "الابتزاز الإلكتروني: أشكاله، آثاره، واستراتيجيات المواجهة"
5. "التحديات المستقبلية في الأمن السيبراني: كيف نعد أنفسنا لمواجهتها؟"
6. "الأمن الرقمي للأطفال والمراهقين: أدوات وأساليب لضمان الاستخدام الآمن للإنترنت"
7. "التطورات التكنولوجية وتأثيرها على الأمن السيبراني "
8. "الإبلاغ والتواصل مع السلطات المختصة في حالات الابتزاز الإلكتروني "


وقل
رب زدني علما

الفهرست:(Table of Contents)

إهداء..... 5
شكر وتقدير 6
الملخص:(ABSTRACT) 7
المقدمة:..... 10
المنهجية:(METHODOLOGY) 11
الاستنتاجات:(CONCLUSIONS) 13
كيفية حماية حسابات التواصل الاجتماعي..... 16
استخدام كلمات مرور قوية وفريدة 16
فريدة لكل حساب: 16
تجنب المعلومات الشخصية: 16
تفعيل التحقق بخطوتين 16
الحذر من الروابط المشبوهة والتطبيقات غير المعروفة 17
مراجعة إعدادات الخصوصية بانتظام 19
حماية سرية البطاقات المصرفية..... 22
نصائح لاختيار كلمات مرور آمنة لحسابات المصرفية 22
كيفية استخدام بطاقات الائتمان بأمان على الإنترنت 24
الحذر من رسائل التصيد والاحتيال 24
أهمية تحديث البرامج ونظم الأمان 26
الإجراءات عند التعرض للابتزاز الإلكتروني..... 28
كيفية التعرف على رسائل الابتزاز ومواقف الابتزاز الشائعة 28
الخطوات الأولى للتعامل مع الموقف 29
كيفية جمع الأدلة والتوثيق 31
التواصل مع السلطات المختصة والمنصات الإلكترونية 32
الدعم النفسي والقانوني المتاح للضحايا 34
التوعية الرقمية للأطفال والمراهقين..... 35
تعليم الأطفال والمراهقين السلوك الآمن على الإنترنت 35
التطبيقات والأدوات التي تساعد على متابعة نشاط الأطفال على الإنترنت 36
مستقبل الأمن السيبراني..... 39
التطورات المستقبلية في مجال الأمن السيبراني 39
التحديات القادمة وكيفية الاستعداد لها..... 40

المقدمة:

في عصـــر الثورة الرقمية، أصـــبح الإنترنت جزءًا لا يتجزأ من حياتنا اليومية، مما يجعل الأمن الســـيبراني ضـــرورة ملحة لحماية بياناتنا الشـــخصـــية والمعلومات الحســـاســـة. يشـكل الابتزاز الإلكتروني والتصـيد الاحتيالي والهجمات السـيبرانية تهديدات حقيقية تؤثر على الأفراد والمؤســـســـات على حد ســـواء. مع تطور التكنولوجيا، تتطور أيضًـــا تقنيات الهجوم، مما يتطلب منا أن نكون في حالة تأهب دائمة ومستعدة لمواجهة هذه التحديات بفعالية.

يتناول هذا البحث مواضـيع حيوية في مجال الأمن السـيبراني، بدءًا من كيفية حماية حسـابات التواصـل الاجتماعي، مرورًا بحماية البطاقات المصـرفية على الإنترنت، ووصولًا إلى استراتيجيات مواجهة الابتزاز الإلكتروني. كما يتناول البحث التحديات المســتقبلية في مجال الأمن الســيبراني وكيفية الاســتعداد لها، بالإضــافة إلى تقديم نصائح لتعليم الأطفال والمراهقين السلوك الآمن على الإنترنت.

تكمن أهمية هذا البحث في تقديمه لمجموعة من الحلول والإرشـــادات العملية التي يمكن للأفراد والمؤسسات تطبيقها لتعزيز أمانهم الرقمي. نتطلع من خلال هذا البحث إلى نشـــر الوعي حول مخاطر الإنترنت وتزويد القراء بالأدوات اللازمة لحماية أنفسهم في العالم الرقمي المتغير باستمرار.

المنهجية:(Methodology)

في إعداد البحث حول مواضيع الأمن السيبراني، اتبعت منهجية شاملة ومنهجية لضمان تغطية جميع الجوانب الهامة والمتعلقة بهذا الموضوع الحيوي. وفيما يلي الخطوات التي تم اتباعها:

1- تحديد الأهداف والموضوعات الرئيسية

- **تحديد الأهداف :**بدايةً، تم تحديد الأهداف الرئيسية للبحث وهي توعية القراء بأهمية الأمن السيبراني وتقديم إرشادات وحلول لحماية الأفراد والمؤسسات من التهديدات السيبرانية.
- **اختيار الموضوعات :**تم اختيار الموضوعات الرئيسية التي تغطي مجموعة واسعة من التحديات والحلول في مجال الأمن السيبراني، مثل حماية حسابات التواصل الاجتماعي، حماية البطاقات المصرفية، التعامل مع الابتزاز الإلكتروني، وتوعية الأطفال بالسلوك الآمن على الإنترنت.

2- جمع المعلومات والبيانات

- **البحث في الأدبيات :**تم البحث في الأدبيات الأكاديمية والمقالات العلمية المتعلقة بالأمن السيبراني لتوفير خلفية علمية وموثوقة للبحث.
- **استخدام المصادر الموثوقة :**تم الاستعانة بمصادر موثوقة ومحدثة مثل التقارير الأمنية من شركات الحماية السيبرانية الرائدة، والمقالات الأكاديمية، والمواقع الحكومية والمنظمات الدولية.
- **التواصل مع الخبراء :**تم التواصل مع الخبراء في مجال الأمن السيبراني للحصول على رؤى وتوجيهات مهنية.

3- تحليل المعلومات وتصنيفها

- **تصنيف المعلومات :**تم تصنيف المعلومات والبيانات التي تم جمعها إلى فئات مختلفة بناءً على الموضوعات الفرعية للبحث. هذا التصنيف ساعد في تنظيم المعلومات وتبسيط عملية تحليلها.
- **التحليل النقدي :**تم تحليل المعلومات بشكل نقدي لتحديد الثغرات والتحديات الحالية في الأمن السيبراني، بالإضافة إلى استراتيجيات الحماية الفعالة.

4- إعداد المحتوى وكتابة البحث

- **كتابة الأقسام المختلفة :**تم كتابة الأقسام المختلفة للبحث بناءً على التصنيف والتحليل السابق. تضمنت الأقسام المقدمة، مراجعة الأدبيات، المنهجية، النتائج، المناقشة، والخاتمة.
- **تضمين الأمثلة والتوصيات** :تم تضمين أمثلة وتوصيات عملية لتوضيح النقاط الرئيسية وتقديم حلول واقعية للتحديات التي تمت مناقشتها.
- **المراجعة والتدقيق** :تم مراجعة وتدقيق البحث لضمان دقة المعلومات وسلاسة العرض، بالإضافة إلى التأكد من الامتثال للقواعد الأكاديمية.

5- استخدام الأدوات الرقمية

- **أدوات البحث الإلكتروني** :تم استخدام أدوات البحث الإلكتروني للوصول إلى المصادر الحديثة والمقالات العلمية المتعلقة بالأمن السيبراني.

الاستنتاجات:(Conclusions)

1.كيفية حماية حسابات التواصل الاجتماعي

استخدام كلمات مرور قوية وفريدة

- كلمات المرور هي الخط الدفاعي الأول. ينصح باستخدام كلمات مرور تتضمن مزيجاً من الأحرف الكبيرة والصغيرة، الأرقام، والرموز. تجنب استخدام الكلمات الشائعة أو التتابعات الرقمية السهلة مثل "123456."
- استخدم مدير كلمات المرور لتوليد وتخزين كلمات المرور المعقدة والفريدة لكل حساب.

تفعيل التحقق بخطوتين

- التحقق بخطوتين يضيف طبقة إضافية من الأمان عبر طلب رمز تحقق يُرسل إلى هاتفك المحمول عند محاولة تسجيل الدخول.
- تأكد من تمكين هذه الخاصية في إعدادات الأمان لحساباتك على مختلف المنصات مثل Google و.Facebook

الحذر من الروابط المشبوهة والتطبيقات غير المعروفة

- تجنب الضغط على الروابط التي تصل إليك من مصادر غير موثوقة أو عبر البريد الإلكتروني المريب.
- قم بتنزيل التطبيقات فقط من المتاجر الرسمية وتجنب التطبيقات غير المعروفة.

مراجعة إعدادات الخصوصية بانتظام

- تأكد من مراجعة إعدادات الخصوصية على حساباتك بانتظام لضمان أنك تتحكم في من يمكنه رؤية معلوماتك الشخصية والتفاعل معك.

2.حماية سرية البطاقات المصرفية

نصائح لاختيار كلمات مرور آمنة لحسابات المصرفية

- استخدم كلمات مرور قوية وفريدة لكل حساب مصرفي ولا تشاركها مع أحد.
- تجنب استخدام المعلومات الشخصية مثل تاريخ الميلاد أو الأسماء كجزء من كلمات المرور.

كيفية استخدام بطاقات الائتمان بأمان على الإنترنت

استخدم المواقع التي تبدأ بـ "https" لضمان اتصال آمن.

تجنب إدخال معلومات البطاقة في الشبكات العامة أو غير الآمنة.

الحذر من رسائل التصيد والاحتيال

كن حذرًا من الرسائل الإلكترونية التي تطلب معلومات شخصية أو مالية. تحقق من صحة الرسالة عبر التواصل المباشر مع الجهة المرسلة المزعومة.

أهمية تحديث البرامج ونظم الأمان

- تأكد من أن جميع برامجك ونظم الأمان محدثة بانتظام لتصـــحيح أي ثغرات أمنية قد تكتشف.

.3الإجراءات عند التعرض للابتزاز الإلكتروني

كيفية التعرف على رسائل الابتزاز ومواقف الابتزاز الشائعة

- رسائل الابتزاز غالباً ما تتضمن تهديدات بكشف معلومات شخصية أو صور حساسة ما لم يتم دفع مبلغ معين.
- تأكد من التعرف على هذه الرسائل وعدم الاستجابة لها.

الخطوات الأولى للتعامل مع الموقف

- لا تدفع المبالغ المطلوبة ولا تستجب للتهديدات.
- قم بتوثيق الرسائل والاحتفاظ بالأدلة.

كيفية جمع الأدلة والتوثيق

- احفظ نسخًا من جميع الرسائل التهديدية. استخدم أدوات لتسجيل النشاط على جهازك.
- توثيق المعلومات يساعد في تقديم بلاغات رسمية للجهات المختصة.

التواصل مع السلطات المختصة والمنصات الإلكترونية

- أبلغ السلطات المحلية فورًا عن الحادث.
- اتصل بالمنصة الإلكترونية أو الموقع المعني لإبلاغهم بالمشكلة.

الدعم النفسي والقانوني المتاح للضحايا

- البحث عن الدعم النفسي من محترفين يمكن أن يساعد في التعامل مع التأثير العاطفي للابتزاز.
- استشر محامياً للحصول على نصائح قانونية حول كيفية التعامل مع الموقف بشكل صحيح.

مواضيع إضافية

التوعية الرقمية للأطفال والمراهقين

- تعليم الأطفال والمراهقين السلوك الآمن على الإنترنت من خلال التحدث معهم عن مخاطر الإنترنت.
- استخدام التطبيقات التي تساعد على مراقبة نشاط الأطفال لضمان سلامتهم الرقمية.

مستقبل الأمن السيبراني

- متابعة التطورات التكنولوجية في مجال الأمن السيبراني لمواكبة أحدث الوسائل لحماية البيانات.
- الاستعداد لمواجهة التحديات المستقبلية مثل الهجمات السيبرانية المتقدمة والاحتيال الإلكتروني.

كيفية حماية حسابات التواصل الاجتماعي

استخدام كلمات مرور قوية وفريدة

- **طول كلمة المرور** :كلما كانت كلمة المرور أطول، كلما كانت أكثر أمانًا. ينصح بأن تكون كلمة المرور مكونة من 12 حرفًا على الأقل.
- **مزيج من الأحرف والأرقام والرموز** :استخدم مجموعة متنوعة من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة مثل.(@, #, $, %) مثال : StRoNgPa$$w0rd!

فريدة لكل حساب:

- **تجنب إعادة استخدام كلمات المرور** :لا تستخدم نفس كلمة المرور لأكثر من حساب. إذا تم اختراق أحد الحسابات، فإن استخدام نفس كلمة المرور سيعرض باقي حساباتك للخطر.
- **مدير كلمات المرور :**استخدم تطبيقات مدير كلمات المرور التي تساعدك في إنشاء كلمات مرور قوية وفريدة لكل حساب وتخزينها بشكل آمن. من أمثلة هذه التطبيقاتLastPass :، Password1، Bitwarden.

تجنب المعلومات الشخصية:

لا تستخدم معلومات سهلة التخمين :تجنب استخدام المعلومات الشخصية مثل تاريخ الميلاد، اسم الحيوان الأليف، أو الأرقام المتتالية مثل "123456."

تجنب الأمثلة مثلJohn1985 :، Password123.

4.التحديث بانتظام:

تغيير كلمات المرور بانتظام :قم بتغيير كلمات المرور الخاصة بك بشكل دوري للحفاظ على أمان حساباتك.

مراجعة الأمان :قم بمراجعة إعدادات الأمان وكلمات المرور بانتظام لضمان أنها لم تُخترق.

تفعيل التحقق بخطوتين

تسجيل الدخول إلى حسابك:

افتح التطبيق أو الموقع الخاص بالخدمة التي تريد تفعيل التحقق بخطوتين عليها)مثلGoogle ، Facebook، Twitter).

الوصول إلى إعدادات الأمان:
انتقل إلى قسم الإعدادات في حسابك.
ابحث عن خيارات الأمان أو الخصوصية.
تفعيل التحقق بخطوتين:
ابحث عن خيار "التحقق بخطوتين" أو "التحقق الثنائي" وقم بتمكينه.
ستحتاج عادةً إلى إعادة إدخال كلمة مرورك لتأكيد الهوية.
إدخال رقم الهاتف:
أضف رقم هاتفك المحمول الذي تود استخدامه لتلقي رموز التحقق.
ستتلقى رمز تحقق عبر رسالة نصية قصيرة.SMS
إدخال رمز التحقق:
أدخل رمز التحقق الذي استلمته للتأكيد.
في بعض الحالات، قد يطلب منك تنزيل تطبيق مصادقة) مثل Google Authenticator) لاستخدامه في توليد رموز التحقق.
إعداد خيارات النسخ الاحتياطي:
احفظ رموز النسخ الاحتياطي في مكان آمن. قد تحتاجها إذا فقدت الوصول إلى هاتفك المحمول.
إكمال التفعيل:
بعد تأكيد جميع الخطوات، يكون التحقق بخطوتين مفعلاً. ستطلب منك الخدمة رمز تحقق في كل مرة تحاول فيها تسجيل الدخول من جهاز جديد.

الحذر من الروابط المشبوهة والتطبيقات غير المعروفة

1- التأكد من مصدر الروابط:

البريد الإلكتروني والرسائل :كن حذرًا من الروابط التي تصلك عبر البريد الإلكتروني أو الرسائل النصية من مصادر غير معروفة أو غير موثوقة.

التأكد من الهوية :قبل النقر على أي رابط، تحقق من هوية المرسل. إذا كانت الرسالة تبدو مشبوهة، من الأفضل تجنبها.

2- التحقق من صحة الروابط:

التمرير فوق الروابط :قبل النقر على الرابط، مرر مؤشـر الفأرة فوقه (بدون النقر) للتحقق من عنوان URL الفعلي الذي سيقودك إليه. إذا كان الرابط يبدو مشبوهًا أو لا يتطابق مع المحتوى المعلن، فلا تنقر عليه.

اسـتخدام أدوات التحقق :يمكنك اسـتخدام أدوات التحقق من الروابط مثل VirusTotalلفحص الروابط قبل فتحها.

3- تحميل التطبيقات من المصادر الرسمية:

متاجر التطبيقات الرسـمية :قم بتنزيل التطبيقات فقط من المتاجر الرسـمية مثل Google Playو .Apple App Storeتجنب تنزيل التطبيقات من مصـادر غير رسمية أو مواقع الطرف الثالث.

مراجعة التقييمات :قبل تنزيل تطبيق، تحقق من التقييمات والمراجعات. إذا كانت المراجعات سلبية أو غير كافية، تجنب تنزيل التطبيق.

4- التحقق من الأذونات الممنوحة للتطبيقات:

الأذونات المطلوبة :عند تثبيت تطبيق جديد، انتبه للأذونات التي يطلبها التطبيق. إذا كانت الأذونات تبدو غير منطقية أو مبالغ فيها، قد يكون التطبيق مشبوهًا.

مراجعة الأذونات بانتظام :قم بمراجعة الأذونات الممنوحة للتطبيقات المثبتة على جهازك بانتظام وتقييد أي أذونات غير ضرورية.

5- التحديثات الأمنية:

تحديثات البرامج :تأكد من أن نظام التشـغيل وجميع التطبيقات المثبتة لديك محدثة بانتظام لتصحيح أي ثغرات أمنية قد يتم اكتشافها.

اسـتخدام برامج الحماية :قم بتثبيت برامج مكافحة الفيروسـات والبرمجيات الخبيثة وقم بتحديثها بانتظام.

6- الوعي بالمواقع المشتبه بها:

- النظر في عنوان :URL إذا كـان عنوان الموقع يحتوي على أحرف غير عادية أو مشبوهة، قد يكون الموقع غير آمن.

- استخدام HTTPS: تأكد من أن المواقع التي تزورها تستخدم HTTPS وليسHTTP ، حيث يوفر HTTPS اتصالاً مشفرًا وآمنًا.

7- التثقيف والتوعية المستمرة:

- البقاء على اطلاع :احرص على متابعة الأخبار والمستجدات في مجال الأمن السيبراني لتكون على علم بالتهديدات الجديدة وكيفية التعامل معها.
- التدريب والتوعية :قم بالمشاركة في دورات تدريبية أو ورش عمل حول الأمان الرقمي لتعزيز معرفتك وقدرتك على التمييز بين الروابط والتطبيقات الآمنة والمشبوهة.

مراجعة إعدادات الخصوصية بانتظام

مراجعة إعدادات الخصوصية بانتظام على مواقع التواصل الاجتماعي يعد خطوة حاسمة لحماية معلوماتك الشخصية والتحكم في من يمكنه رؤية ما تشاركه. إليك كيفية القيام بذلك على بعض المنصات الشهيرة:

Facebook

الدخول إلى الإعدادات:

قم بتسجيل الدخول إلى حسابك.

انقر على السهم الصغير في الزاوية العلوية اليمنى واختر "الإعدادات والخصوصية."

مراجعة إعدادات الخصوصية:

اختر "الإعدادات" ثم "الخصوصية."

قم بمراجعة من يمكنه رؤية منشوراتك المستقبلية، من يمكنه إرسال طلبات الصداقة، ومن يمكنه البحث عنك باستخدام بريدك الإلكتروني أو رقم هاتفك.

أدوات فحص الخصوصية:

استخدم أداة "فحص الخصوصية" التي تساعدك على مراجعة إعدادات الحساب والمعلومات التي تشاركها.

Twitter

الدخول إلى الإعدادات:
سجل الدخول إلى حسابك.
انقر على صورة ملفك الشخصي واختر "الإعدادات والخصوصية."
مراجعة إعدادات الخصوصية والأمان:
انتقل إلى قسم "الخصوصية والأمان."
قم بمراجعة إعدادات مثل من يمكنه رؤية تغريداتك، من يمكنه الإشـــارة إليك، ومن يمكنه إرسال الرسائل المباشرة.
أمان الحساب:
تفعيل خيار "حماية تغريداتك" لجعل تغريداتك مرئية فقط للمتابعين الموافق عليهم.

Instagram

الدخول إلى الإعدادات:
افتح التطبيق وانتقل إلى ملفك الشخصي.
انقر على الثلاث خطوط في الزاوية العلوية اليمنى واختر "الإعدادات."
مراجعة إعدادات الخصوصية:
انتقل إلى "الخصوصية."
راجع من يمكنه رؤية منشوراتك وقصصك، ومن يمكنه إرسال الرسائل، ومن يمكنه التعليق على منشوراتك.
حساب خاص:
قم بتفعيل خيار "الحســـاب الخاص" لجعل منشــوراتك مرئية فقط للمتابعين الموافق عليهم.

LinkedIn

الدخول إلى الإعدادات:
سجل الدخول إلى حسابك.
انقر على صورة ملفك الشخصي واختر "الإعدادات والخصوصية."
مراجعة إعدادات الخصوصية:
انتقل إلى قسم "الخصوصية."

راجع إعدادات مثل من يمكنه رؤية ملفك الشخصي، من يمكنه إرسال الرسائل، ومن يمكنه رؤية نشاطك.

إعدادات الاتصال:

قم بتعديل إعدادات "كيفية ظهورك في عمليات البحث" و "من يمكنه رؤية بريدك الإلكتروني."

نصائح عامة:

التحديث بانتظام:

قم بمراجعة إعدادات الخصوصية بانتظام، خاصة بعد أي تحديثات جديدة للمنصة.

التجربة الشخصية:

تحقق من إعدادات الخصوصية من خلال رؤية ملفك الشخصي كما يراه الآخرون. معظم المنصات توفر هذه الخاصية لتفحص ما يظهر للغير.

حماية سرية البطاقات المصرفية

نصائح لاختيار كلمات مرور آمنة لحسابات المصرفية

اختيار كلمات مرور آمنة لحساباتك المصرفية يعد من الخطوات المهمة جداً لحماية أموالك ومعلوماتك الشخصية. إليك بعض النصائح لتحقيق ذلك:

1- استخدم مزيجًا من الأحرف والأرقام والرموز:

يجب أن تتضمن كلمة المرور مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة (مثل !، @، #، $).

مثال: P@ssw0rd!123

2- اختيار كلمات مرور طويلة:

كلما كانت كلمة المرور أطول، كانت أقوى. يُفضل أن تكون كلمة المرور مكونة من 12 حرفًا على الأقل.

3- تجنب استخدام المعلومات الشخصية:

لا تستخدم المعلومات الشخصية مثل اسمك، تاريخ ميلادك، أو أي معلومات يمكن للآخرين معرفتها بسهولة عنك.

تجنب كلمات المرور مثل John1985 :أو MyDogMax!.

4- استخدام عبارات عشوائية:

اختر جملة عشوائية واجعلها كلمة المرور الخاصة بك. يمكن أن تكون جملة من كلمات متعددة لتكوين كلمة مرور طويلة وقوية.

مثال: R@inyD@y!in$2021

5- عدم إعادة استخدام كلمات المرور:

لا تستخدم نفس كلمة المرور لأكثر من حساب. إذا تم اختراق أحد الحسابات، فإن استخدام نفس كلمة المرور سيعرض باقي حساباتك للخطر.

6- تحديث كلمات المرور بانتظام:

قم بتغيير كلمات المرور بانتظام للحفاظ على أمان حساباتك. يُفضل تغيير كلمات المرور كل 3-6 أشهر.

7- استخدام مدير كلمات المرور:

يمكنك اســـتخدام تطبيقات مدير كلمات المرور لحفظ كلمات المرور بأمان وإنشـــاء كلمات مرور معقدة وفريدة لكل حساب.

أمثلة على التطبيقاتLastPass :، Password1، .Bitwarden

8- التحقق من قوة كلمة المرور:

يمكنك اســـتخدام أدوات للتحقق من قوة كلمة المرور الخاصـــة بك والتأكد من أنها ليست ضعيفة أو سهلة التخمين.

أمثلة على الأدواتPassword Meter :، .How Secure Is My Password

9- تمكين التحقق بخطوتين:

بالإضـــافة إلى كلمة المرور القوية، تفعيل خاصـــية التحقق بخطوتين يضـــيف طبقة إضـــافية من الأمان، حيث يتطلب إدخال رمز تحقق يُرســـل إلى هاتفك المحمول عند محاولة تسجيل الدخول.

10- الحذر من الرسائل والروابط المشبوهة:

كن حذرًا عند تلقي رســـائل أو روابط تطلب منك إدخال كلمة المرور الخاصـــة بك. تأكد من أن المصدر موثوق قبل إدخال أي معلومات شخصية.

باتباع هذه النصـــائح، يمكنك تقليل خطر اختراق حســـاباتك المصـــرفية والحفاظ على أمان معلوماتك المالية.

كيفية استخدام بطاقات الائتمان بأمان على الإنترنت

لتجنب الاحتيال عند استخدام بطاقات الائتمان على الإنترنت، يمكنك اتباع النصائح التالية:

- استخدام مواقع آمنة :تأكد من أن الموقع الذي تقوم بإدخال بيانات بطاقتك الائتمانية عليه موثوق ومعروف. تجنب المواقع غير المعروفة أو الغير موثوقة.
- التحقق من الرمز المروري :تأكد من أن الموقع يستخدم ميزة التحقق الثنائي (2FA)لتأكيد هويتك. هذا يعزز الأمان ويجعل من الصعب على الاحتياليين الوصول إلى حسابك.
- تجنب البريد الإلكتروني الغير موثوق :لا تقم بإدخال بيانات بطاقتك الائتمانية عندما تصلك رسائل إلكترونية غير موثوقة أو غير متوقعة. تأكد من أن الرسالة جاءت من مصدر موثوق.
- استخدام برامج الأمان :تأكد من أن جهازك محمي ببرامج الأمان الأخيرة، مثل الأنتي فيير والمراقبة الأمنية.
- التحقق من الشبكة :تأكد من أن الشبكة التي تستخدمها للاتصال بالإنترنت آمنة، خاصة إذا كنت تستخدم شبكة عامة.

الحذر من رسائل التصيد والاحتيال

رسائل التصيد والاحتيال هي واحدة من أكثر الطرق شيوعًا التي يستخدمها المخترقون لخداع الأفراد وسرقة معلوماتهم الشخصية. إليك بعض النصائح للوقاية من هذه الرسائل والتعامل معها بفعالية:

1- التعرف على رسائل التصيد

- النصوص العاجلة :تحتوي رسائل التصيد غالبًا على نصوص طارئة تحاول دفعك لاتخاذ إجراء فوري مثل "حسابك سيتم إغلاقه!" أو "فزت بجائزة! ادخل معلوماتك لاستلامها."
- الروابط المشبوهة :تحتوي الرسائل على روابط تبدو مشروعة، لكنها تقود إلى مواقع مزيفة تطلب منك إدخال معلومات شخصية أو مالية.

- المرسل غير الموثوق :افحص عنوان البريد الإلكتروني للمرسل بعناية. غالبًا ما يكون هناك أخطاء إملائية أو أن العنوان لا يتطابق مع الشركة المزعومة.

2- التحقق من الروابط والمرفقات

- عدم الضغط على الروابط المباشرة :بدلاً من الضغط على الرابط في الرسالة، اكتب عنوان الموقع يدويًا في متصفحك أو استخدم إشاراتك المرجعية.
- فحص المرفقات :لا تفتح المرفقات إلا إذا كنت متأكدًا من مصدرها وتعرف ما تحتويه. قد تحتوي المرفقات المشبوهة على برمجيات ضارة.

3- استخدام أدوات الأمان

- برامج مكافحة الفيروسات والجدران النارية :استخدم برامج مكافحة الفيروسات وبرامج مكافحة البرمجيات الخبيثة لتوفير طبقة إضافية من الحماية.
- الفحص التلقائي :قم بتمكين الفحص التلقائي للبريد الإلكتروني للكشف عن الرسائل المشبوهة ومنعها.

4- التوعية والتدريب

- تعليم الآخرين :قم بتوعية أفراد عائلتك وزملائك حول كيفية التعرف على رسائل التصيد والاحتيال وطرق الوقاية منها.
- التدريب على الحذر :قم بالمشاركة في دورات تدريبية أو ورش عمل تتعلق بالأمان السيبراني لزيادة وعيك وقدرتك على التعامل مع التهديدات.

5- التحقق من المصدر

- الاتصال المباشر :إذا تلقيت رسالة مشبوهة تبدو أنها من جهة معروفة، تواصل مع هذه الجهة مباشرة من خلال معلومات الاتصال الرسمية للتحقق من صحة الرسالة.
- مراجعة الحسابات بانتظام :تأكد من مراجعة حساباتك المصرفية وغيرها بانتظام للكشف عن أي نشاط غير مألوف والإبلاغ عنه فورًا.

6- الإبلاغ عن الرسائل المشبوهة

- الإبلاغ عن الاحتيال :إذا تلقيت رسالة تصيد، أبلغ عنها إلى مزود خدمة البريد الإلكتروني الخاص بك ليتخذوا إجراءات ضده.

- توعية المجتمع :شارك المعلومات حول محاولات التصيد مع مجتمعك أو على وسائل التواصل الاجتماعي لزيادة الوعي الجماعي.

أهمية تحديث البرامج ونظم الأمان

تحديث البرامج ونظم الأمان بانتظام يعد من الخطوات الأساسية لحماية الأجهزة والبيانات الشخصية من التهديدات الأمنية والهجمات السيبرانية. إليك بعض الأسباب التي توضح أهمية هذه العملية:

1- تصحيح الثغرات الأمنية

اكتشاف الثغرات :مع مرور الوقت، يمكن اكتشاف ثغرات أمنية في البرامج وأنظمة التشغيل. يمكن للقراصنة استغلال هذه الثغرات للوصول إلى البيانات الحساسة.

التحديثات الأمنية :توفر التحديثات تصحيحات لهذه الثغرات، مما يمنع الاستغلال غير المصرح به ويحافظ على سلامة النظام.

2- حماية البيانات الشخصية

أمان البيانات :تعمل التحديثات على تعزيز أمان البيانات الشخصية والمعلومات الحساسة المخزنة على الجهاز.

منع الاختراقات :تحديث الأنظمة يقلل من فرص نجاح الهجمات التي تهدف إلى سرقة البيانات أو التجسس عليها.

3- تحسين الأداء والاستقرار

تحسين الأداء :غالبًا ما تشمل التحديثات تحسينات في الأداء تجعل النظام يعمل بشكل أسرع وأكثر كفاءة.

إصلاح الأخطاء :تقوم التحديثات بإصلاح الأخطاء الموجودة في الإصدارات السابقة، مما يعزز استقرار النظام ويقلل من احتمالية التعرض لمشاكل تقنية.

4- مواكبة التهديدات الجديدة

التطور المستمر للتهديدات :تتطور التهديدات السيبرانية باستمرار، ويستغل القراصنة تقنيات جديدة للهجوم. التحديثات تساعد في التصدي لهذه التهديدات الجديدة.

التحديث التكنولوجي :يشمل التحديث دعمًا للتقنيات الجديدة والمعايير الأمنية المتقدمة، مما يحسن من قدرة النظام على مواجهة التهديدات الحديثة.

5- زيادة الثقة في الأمان الرقمي

الثقة والأمان :عند تحديث الأنظمة بانتظام، يمكنك الاعتماد على أن جهازك يعمل بأحدث معايير الأمان، مما يزيد من ثقتك في سلامة بياناتك.

الالتزام بسياسات الأمان :تساعد التحديثات المنتظمة في الامتثال لسياسات الأمان والخصوصية المتبعة في المؤسسات والأعمال.

نصائح لتحديث البرامج ونظم الأمان

تمكين التحديثات التلقائية :قم بتمكين التحديثات التلقائية للبرامج وأنظمة التشغيل لضمان حصولك على آخر التصحيحات بشكل فوري.

مراجعة التحديثات يدوياً :قم بمراجعة التحديثات بشكل دوري والتحقق من تثبيت آخر التحديثات المتاحة.

استخدام برامج حماية موثوقة :تأكد من استخدام برامج مكافحة الفيروسات والجدران النارية والبرامج الأمنية الأخرى للحماية من التهديدات.

الإجراءات عند التعرض للابتزاز الإلكتروني

كيفية التعرف على رسائل الابتزاز ومواقف الابتزاز الشائعة

التعرف على رسائل الابتزاز ومواقف الابتزاز الشائعة يمكن أن يساعدك في حماية نفسك من الوقوع ضحية لهذه الأنواع من الهجمات. إليك بعض النصائح والإرشادات:

1- التعرف على رسائل الابتزاز

النصوص العاجلة والمهددة :غالبًا ما تحتوي رسائل الابتزاز على تهديدات واضحة مثل "إذا لم تدفع، سننشر صورك الخاصة" أو "سوف نفضح معلوماتك الشخصية."

الطلبات المالية :يطلب المبتزون عادةً مبالغ مالية مقابل عدم نشر معلومات حساسة أو صور خاصة.

الروابط والمرفقات المشبوهة :قد تحتوي الرسائل على روابط أو مرفقات تطلب منك إدخال معلومات شخصية أو تنزيل ملفات ضارة.

2- مواقف الابتزاز الشائعة

الابتزاز المالي :يطلب المبتزون مبالغ مالية مقابل عدم نشر معلومات حساسة أو صور خاصة.

الابتزاز العاطفي :يستخدم المبتزون التهديدات العاطفية مثل إيذاء أفراد العائلة أو الأصدقاء لإجبار الضحية على الامتثال لمطالبهم.

الابتزاز الجنسي :يهدد المبتزون بنشر صور أو مقاطع فيديو ذات طبيعة جنسية إذا لم يتم تلبية مطالبهم.

3- كيفية التعامل مع رسائل الابتزاز

عدم الاستجابة للتهديدات :لا تستجب للتهديدات ولا تدفع أي مبالغ مالية. الاستجابة للمبتزين قد تشجعهم على الاستمرار في الابتزاز.

توثيق الأدلة :احتفظ بنسخ من جميع الرسائل والتهديدات التي تتلقاها. قد تحتاج إلى هذه الأدلة عند الإبلاغ عن الحادث.

التواصل مع السلطات :أبلغ السلطات المحلية فورًا عن أي محاولة ابتزاز. يمكن للسلطات تقديم المساعدة والإرشاد حول كيفية التعامل مع الموقف.

التواصل مع المنصات الإلكترونية :إذا تلقيت رسائل ابتزاز عبر منصات التواصل الاجتماعي أو البريد الإلكتروني، اتصل بالمنصة المعنية للإبلاغ عن الحادث وطلب المساعدة.

4- الوقاية من الابتزاز الإلكتروني

استخدام كلمات مرور قوية وفريدة :تأكد من أن كلمات المرور الخاصة بك قوية وفريدة لكل حساب. استخدم مدير كلمات المرور لتخزين كلمات المرور بأمان.

تفعيل التحقق بخطوتين :قم بتمكين التحقق بخطوتين لحساباتك لإضافة طبقة إضافية من الأمان.

الحذر من الروابط والمرفقات المشبوهة :لا تضغط على الروابط أو تفتح المرفقات التي تصلك من مصادر غير معروفة أو غير موثوقة.

مراجعة إعدادات الخصوصية :تأكد من أن إعدادات الخصوصية على حساباتك تمنع الغرباء من الوصول إلى معلوماتك الشخصية.

الخطوات الأولى للتعامل مع الموقف

الخطوات الأولى للتعامل مع المبتز الكترونيا

إذا تعرضت للابتزاز الإلكتروني، فإن اتخاذ خطوات مدروسة وسريعة يمكن أن يساعدك في الحد من الأضرار وحماية نفسك. إليك الخطوات الأولى التي يجب اتباعها:

1- الحفاظ على الهدوء وتوثيق الأدلة

الحفاظ على الهدوء :من المهم أن تحافظ على هدوءك ولا تتخذ قرارات متسرعة أو استجابات مبنية على الخوف.

توثيق الأدلة :احتفظ بنسخ من جميع الرسائل، البريد الإلكتروني، أو أي وسيلة اتصال أخرى يستخدمها المبتز. قد تتضمن هذه الأدلة لقطات شاشة، تسجيلات صوتية، أو فيديوهات.

2- عدم الاستجابة للمبتز

لا تدفع المال أو تقدم المعلومات :عدم الرد على مطالب المبتز أو التهديدات؛ الاستجابة قد تشجع المبتز على مواصلة الابتزاز.

عدم التواصل :توقف عن أي تواصل مع المبتز بمجرد تأمين الأدلة التي تحتاجها.

3- إبلاغ السلطات المختصة

التواصل مع السلطات :تواصل مع السلطات المحلية أو الشرطة لتقديم بلاغ رسمي عن الابتزاز الإلكتروني. قد يكون لديهم الموارد والخبرات اللازمة للتعامل مع الحالة.

تقديم الأدلة :قدم جميع الأدلة التي قمت بتوثيقها لدعم تقريرك.

4- الإبلاغ عن الحادث للمنصات الإلكترونية

منصات التواصل الاجتماعي :إذا تم التهديد عبر منصة تواصل اجتماعي، قم بالإبلاغ عن الحساب المبتز باستخدام أدوات الإبلاغ المتاحة في المنصة.

البريد الإلكتروني :إذا تلقيت رسائل بريد إلكتروني تهديدية، اتصل بمزود خدمة البريد الإلكتروني للإبلاغ عن الحادث.

5- تعزيز الأمان الشخصي والرقمي

تغيير كلمات المرور :قم بتغيير كلمات المرور لحساباتك الشخصية التي قد تكون تعرضت للاختراق. استخدم كلمات مرور قوية وفريدة لكل حساب.

تمكين التحقق بخطوتين :قم بتمكين خاصية التحقق بخطوتين لحساباتك لتوفير طبقة إضافية من الأمان.

6- البحث عن الدعم النفسي والقانوني

الدعم النفسي :الابتزاز الإلكتروني يمكن أن يكون مرهقاً نفسياً. لا تتردد في البحث عن دعم نفسي من متخصصين في حال كنت بحاجة إلى ذلك.

المشورة القانونية :استشر محامياً للحصول على نصائح قانونية حول كيفية التعامل مع المبتز وحماية حقوقك.

7- إعلام الأصدقاء والعائلة

إعلام دائرة الثقة :أخبر الأشخاص المقربين منك عن الوضع حتى يكونوا على علم ويمكنهم تقديم الدعم إذا لزم الأمر.

الحفاظ على السرية:

كيفية جمع الأدلة والتوثيق

جمع الأدلة والتوثيق عند التعرض للابتزاز الإلكتروني يعتبر خطوة مهمة لضمان أن لديك كل المعلومات اللازمة لتقديم بلاغ رسمي والحصول على الدعم المناسب. إليك كيفية القيام بذلك بشكل فعال:

1- الاحتفاظ بالرسائل والمكالمات

- **البريد الإلكتروني والرسائل النصية :**احفظ جميع الرسائل الإلكترونية والنصية التي تتلقاها من المبتز. يمكنك حفظها كملفات PDF أو أخذ لقطات شاشة لكل رسالة.
- **المكالمات الهاتفية** :إذا تلقيت مكالمات هاتفية، حاول تسجيل المكالمة إذا كانت قوانين بلدك تسمح بذلك. إذا لم تتمكن من التسجيل، احتفظ بملاحظات دقيقة حول ما قيل ومن قاله.

2- أخذ لقطات شاشة(Screenshots)

- **لقطات شاشة للرسائل** :خذ لقطات شاشة لجميع الرسائل التي تتلقاها، سواء كانت على وسائل التواصل الاجتماعي، البريد الإلكتروني، أو الرسائل النصية.
- **لقطات شاشة للمواقع** :إذا طلب منك المبتز زيارة مواقع معينة أو إدخال معلومات على مواقع، خذ لقطات شاشة لهذه المواقع.

3- توثيق التهديدات والمطالبات

- **المحتوى التهديدي** :قم بتوثيق كل تهديد أو طلب مالي أو طلبات معلومات شخصية يقدمها المبتز.
- **المواعيد النهائية** :إذا حدد المبتز مواعيد نهائية لتنفيذ طلباته، قم بتوثيق هذه المواعيد بشكل دقيق.

4- الاحتفاظ بالتواريخ والأوقات

- **تسجيل التواريخ والأوقات** :احتفظ بتسجيل دقيق لجميع التواريخ والأوقات التي تلقيت فيها الرسائل أو المكالمات من المبتز.

5- استخدام أدوات التوثيق الرقمية

- **برامج تسجيل الشاشة :**استخدم برامج تسجيل الشاشة لتوثيق أي نشاط مشبوه على جهاز الكمبيوتر أو الهاتف المحمول.

- **أدوات التوثيق الإلكترونية** :هناك أدوات مثل Evernote أو OneNote التي تساعدك على تجميع كل الأدلة والملاحظات في مكان واحد بشكل منظم.

6- التواصل مع مزودي الخدمة

التبليغ عن الحادث :تواصل مع مزودي خدمات الإنترنت أو مزودي البريد الإلكتروني للإبلاغ عن الحادث وطلب توجيهات حول كيفية حفظ الأدلة.

طلب سجلات النشاط :بعض مزودي الخدمات قد يكونون قادرين على توفير سجلات النشاط لمساعدتك في توثيق الحادث.

7- التنسيق مع السلطات القانونية

تقديم الأدلة للشرطة :عندما تتواصل مع السلطات المختصة، تأكد من تقديم كل الأدلة التي جمعتها بشكل منظم. يمكن أن تكون هذه الأدلة ضرورية لمساعدتهم في التحقيق واتخاذ الإجراءات اللازمة.

التواصل مع المحامي :إذا كان لديك محامٍ، قم بتقديم الأدلة له أيضًا للحصول على المشورة القانونية حول كيفية المضي قدمًا.

8- الحفاظ على النسخ الاحتياطية

النسخ الاحتياطية الإلكترونية :تأكد من حفظ نسخ احتياطية من جميع الأدلة على وسائط تخزين منفصلة أو على الخدمات السحابية لضمان عدم فقدانها.

النسخ الورقية :قد يكون من الجيد طباعة بعض الأدلة الهامة والاحتفاظ بها في مكان آمن.

باتباع هذه الخطوات، ستكون مستعدًا بشكل أفضل للتعامل مع حالة الابتزاز الإلكتروني وستتمكن من تقديم الأدلة المطلوبة لدعم قضيتك أمام السلطات المختصة.

التواصل مع السلطات المختصة والمنصات الإلكترونية

التواصل مع السلطات المختصة والمنصات الإلكترونية عند التعرض للابتزاز الإلكتروني هو خطوة حاسمة لحماية نفسك والحصول على الدعم اللازم. إليك كيفية القيام بذلك:

1- التواصل مع السلطات المختصة

الإبلاغ عن الحادث :قم بزيارة أقرب مركز شرطة لتقديم بلاغ رسمي عن الابتزاز الإلكتروني. قدم جميع الأدلة التي جمعتها، مثل لقطات الشاشة والرسائل.

الاتصال بالخطوط الساخنة :توجد خطوط ساخنة مخصصة للإبلاغ عن الجرائم الإلكترونية. ابحث عن الرقم المناسب في منطقتك واتصل بهم للحصول على المساعدة. ويوجد في العراق الرقم 119 اتصل ليتم تحويل طلبك للجهة المختصة.

التواصل مع وحدة الجرائم الإلكترونية :إذا كانت هناك وحدة متخصصة في الجرائم الإلكترونية في منطقتك، تواصل معهم مباشرة للحصول على إرشادات حول كيفية التعامل مع الموقف.

2.التواصل مع المنصات الإلكترونية

الإبلاغ عن الحسابات المشبوهة :إذا تلقيت رسائل ابتزاز عبر منصات التواصل الاجتماعي، استخدم أدوات الإبلاغ المتاحة على المنصة للإبلاغ عن الحسابات المشبوهة.

Facebook:انتقل إلى الملف الشخصي للحساب المبتز، انقر على النقاط الثلاث في الزاوية العلوية اليمنى، واختر "الإبلاغ."

Instagram:انتقل إلى الملف الشخصي للحساب المبتز، انقر على النقاط الثلاث في الزاوية العلوية اليمنى، واختر "الإبلاغ."

Twitter:انتقل إلى الملف الشخصي للحساب المبتز، انقر على النقاط الثلاث في الزاوية العلوية اليمنى، واختر "الإبلاغ."

التواصل مع دعم العملاء :اتصل بفريق دعم العملاء للمنصة المعنية وقدم لهم تفاصيل الحادث. قد يكون لديهم إجراءات إضافية يمكنهم اتخاذها لحمايتك.

البريد الإلكتروني :إذا تلقيت رسائل ابتزاز عبر البريد الإلكتروني، اتصل بمزود خدمة البريد الإلكتروني للإبلاغ عن الحادث وطلب المساعدة.

2- حماية حساباتك الشخصية

تغيير كلمات المرور :قم بتغيير كلمات المرور لحساباتك الشخصية التي قد تكون تعرضت للاختراق. استخدم كلمات مرور قوية وفريدة لكل حساب.

تمكين التحقق بخطوتين :قم بتمكين خاصية التحقق بخطوتين لحساباتك لتوفير طبقة إضافية من الأمان.

مراجعة إعدادات الخصوصية :تأكد من أن إعدادات الخصوصية على حساباتك تمنع الغرباء من الوصول إلى معلوماتك الشخصية.

3- البحث عن الدعم النفسي والقانوني

- **الدعم النفسي** :الابتزاز الإلكتروني يمكن أن يكون مرهقاً نفسياً. لا تتردد في البحث عن دعم نفسي من متخصصين في حال كنت بحاجة إلى ذلك.
- **المشورة القانونية** :استشر محامياً للحصول على نصائح قانونية حول كيفية التعامل مع المبتز وحماية حقوقك.

الدعم النفسي والقانوني المتاح للضحايا

الدعم النفسي:

- **المراكز النفسية** :يمكنك البحث عن مراكز الدعم النفسي المحلية أو الوطنية التي تقدم الدعم لضحايا الابتزاز.
- **المنظمات غير الحكومية** :هناك منظمات تقدم الدعم النفسي والاجتماعي لضحايا الابتزاز، مثل "منظمة النساء العراقية للتنمية والتغيير" و"منظمة النساء العراقية للتنمية والتغيير."
- **المنتديات والدورات** :هناك منتديات عبر الإنترنت ودورات تدريبية تساعد الضحايا على التعامل مع تأثيرات الابتزاز.
- الدعم القانوني:
- **المحامين** :يمكنك البحث عن محامي متخصص في قضايا الابتزاز للحصول على استشارة قانونية.
- **الجهات الحكومية** :يمكنك التواصل مع الجهات الحكومية المختصة في حماية حقوق الضحايا والمساعدة في تقديم الدعم القانوني.
- **المنظمات القانونية** :هناك منظمات تقدم الدعم القانوني لضحايا الابتزاز، مثل "منظمة النساء العراقية للتنمية والتغيير."

التوعية الرقمية للأطفال والمراهقين

تعليم الأطفال والمراهقين السلوك الآمن على الإنترنت

تعليم الأطفال والمراهقين السلوك الآمن على الإنترنت أمر حيوي لضمان حمايتهم من التهديدات الرقمية والمشاكل المحتملة. إليك بعض الخطوات والإرشادات التي يمكن اتباعها:

1- توعية الأطفال بأهمية الأمان على الإنترنت

توضيح المخاطر :اشعرهم بأهمية الأمان على الإنترنت من خلال شرح المخاطر المحتملة مثل التنمر الإلكتروني، الاحتيال، والاختراق.

التحدث عن الخصوصية :علمهم كيفية الحفاظ على خصوصيتهم وعدم مشاركة معلومات شخصية مثل العنوان، رقم الهاتف، أو الصور الحساسة.

2- تحديد القواعد والإرشادات

تحديد وقت الاستخدام :حدد أوقاتًا محددة لاستخدام الإنترنت لضمان عدم قضائهم وقتًا طويلاً على الشبكة.

قائمة المواقع الآمنة :قم بإعداد قائمة بالمواقع الآمنة والمناسبة لأعمارهم وأرشدهم لتجنب المواقع المشبوهة أو غير الملائمة.

3- استخدام أدوات الأمان والمراقبة

برامج التحكم الأبوي :استخدم برامج التحكم الأبوي لمراقبة الأنشطة عبر الإنترنت وتحديد المواقع التي يمكن للأطفال الوصول إليها.

التحديثات الأمانية :تأكد من تحديث جميع البرامج ونظم الأمان بانتظام لحماية الأجهزة من التهديدات الأمنية.

4- تشجيع الحوار المفتوح

الاستماع والتوجيه :شجع الأطفال على التحدث معك عن أي شيء يرونه أو يتعرضون له على الإنترنت ويجعلهم يشعرون بأنهم يمكنهم اللجوء إليك في أي وقت.

طرح الأسئلة :اسألهم بانتظام عن أنشطتهم عبر الإنترنت وأصدقائهم الرقميين.

5- تعليمهم كيفية التفاعل الآمن

التفاعل مع الغرباء :وجههم لعدم التفاعل مع الغرباء على الإنترنت وعدم قبول طلبات الصداقة من أشخاص لا يعرفونهم.

السلوك اللائق :علمهم كيفية التصرف بشكل لائق على الإنترنت واحترام الآخرين.

6- استخدام محركات البحث الآمنة

محركات البحث الخاصة بالأطفال :استخدم محركات البحث المصممة للأطفال مثل Kiddleو KidRexالتي تقدم نتائج بحث آمنة وملائمة لأعمارهم.

تفعيل فلاتر البحث :تأكد من تفعيل فلاتر البحث الآمنة على محركات البحث التقليدية لمنع المحتوى غير المناسب.

7- التوعية بالتصيد والاحتيال

التعرف على رسائل التصيد :علمهم كيفية التعرف على رسائل البريد الإلكتروني المشبوهة والروابط غير الآمنة.

عدم مشاركة المعلومات الشخصية :أكد عليهم عدم مشاركة أي معلومات شخصية أو كلمات مرور مع أي جهة عبر الإنترنت.

8- تشجيع الاستخدام التعليمي والهادف للإنترنت

المواقع التعليمية :شجعهم على استخدام الإنترنت للبحث عن المعلومات التعليمية والمفيدة.

المشاركة في الأنشطة الإيجابية :اجعلهم يشاركون في الأنشطة الإيجابية عبر الإنترنت مثل البرمجة، التعلم عبر الإنترنت، والمشاريع الإبداعية.

موارد إضافية:

الدورات التوعوية :ابحث عن دورات أو ورش عمل محلية أو عبر الإنترنت تقدم توعية حول الأمان الرقمي.

الكتب والمقالات :اقرأ كتب ومقالات تتحدث عن الأمان على الإنترنت للأطفال وتقديمها لهم بطرق ممتعة ومبسطة.

التطبيقات والأدوات التي تساعد على متابعة نشاط الأطفال على الإنترنت

هناك العديد من التطبيقات والأدوات التي يمكن أن تساعد في متابعة نشاط الأطفال على الإنترنت. إليك بعض الخيارات الشهيرة:

Qustodio: يوفر تحليلًا شـــاملاً للنشـــاط على الإنترنت، بما في ذلك الوقت الذي يقضيه الأطفال على الإنترنت والمواقع التي يزورونها.

برنامج Qustodio هو أداة متقدمة لمتابعة ومراقبة الأطفال على الإنترنت. يمكنك اســـتخدامه لتحديد الســـياســـات والتحكم في الوصـــول إلى المواقع والمحتوى على الإنترنت. إليك بعض الخطوات الأساسية لاستخدامه:

تحميل وتثبيت :قم بتحميل برنامج Qustodio من موقعه الرســـمي وتثبيته على جهاز الطفل.

إنشاء حسابات :أنشئ حسابات لكل طفل وأعطهم إذناً للوصول إلى الإنترنت.

إعداد السياسات :قم بتحديد السياسات والتحكم في الوقت الذي يمكن للطفل الوصول إلى الإنترنت، والمواقع التي يمكنه الوصول إليها، والمحتوى المسموح به.

التقارير والتحليلات :يوفر Qustodio تقارير وتحليلات تفصـيلية عن الاسـتخدام الإنترنتي للطفل، مما يساعدك على مراقبة الأنشطة واتخاذ الإجراءات اللازمة.

التنبيهات والتحديثات :يمكنك تكوين تنبيهات للطفل عند وصـــوله إلى مواقع غير مسموح بها أو عند تجاوز الوقت المحدد.

Net Nanny: يتيح لـك تحـديـد الأنواع الفرعيـة من المواقع التي يمكن للأطفـال الوصول إليها وتحديد الوقت الذي يمكنهم البقاء عليه.

Kaspersky Safe Kids: يقدم تحليلًا للنشـــاط على الإنترنت ويمكنك من تحديد الأنواع الفرعية من المواقع التي يمكن للأطفال الوصول إليها.

Kaspersky Safe Kids هو تطبيق يســاعد الأهل على مراقبة وإدارة اســتخدام الأجهزة اللوحية للأطفال وضمان سلامتهم على الإنترنت. إليك كيفية استخدامه:

تثبيت التطبيق :قم بتثبيت التطبيق على جهازك اللوحي وعلى هاتفك المحمول.

إنشاء حساب :بعد التثبيت، قم بإنشاء حساب للطفل على التطبيق.

تحديد الإعدادات :قم بتحديد الإعدادات الأســاسـية مثل العمر الذي يتناسـب مع الطفل والمنتجات التي تريد تجربتها.

تحديد القيود :يمكنك تحديد القيود المختلفة مثل الوقت الأقصـى للاستخدام، والمواقع التي يمكن الوصول إليها، والمنتجات التي يمكن شراؤها.

مراقبة النشـاط :يمكنك مراقبة النشـاط الإنترنتي للطفل والحصـول على تقارير عن الأنشطة التي يقوم بها.

التنبيـهات :يمكنك تكوين تنبيهات للتأكد من أن الطفل لا يســتخدم الأجهزة لفترات طويلة أو يقوم بأنشطة غير مسموحة.

Google Family Link: يتيح لك متابعة الأطفال على أجهزة Android و iOS وتحديد الوقت الذي يمكنهم البقاء عليه على الإنترنت.

Circle by Disney

مستقبل الأمن السيبراني

التطورات المستقبلية في مجال الأمن السيبراني

مع تزايد التكنولوجيا والاعتماد على الإنترنت في حياتنا اليومية، أصبح الأمن السيبراني أكثر أهمية من أي وقت مضى. يتطلب الأمن السيبراني الآن معالجة تهديدات متنوعة ومتطورة، ويتوقع أن تشهد هذه المجالات تطورات كبيرة في المستقبل.

التطورات المستقبلية:

- **التعلم الآلي والذكاء الاصطناعي** :سيستخدم الأمن السيبراني تقنيات الذكاء الاصطناعي والتعلم الآلي لتحليل البيانات الكبيرة وتحديد التهديدات بشكل أسرع وأكثر دقة.
- **التحليل الاستكشافي** :سيستمر التحليل الاستكشافي في تطوره للتعرف على التهديدات الجديدة والمتطورة قبل أن تصل إلى الأنظمة.
- **الأمن الذكي** :سيتم تطوير أنظمة أمن ذكية تستخدم الذكاء الاصطناعي لتعلم السلوكيات الطبيعية وتكشف الأنشطة غير الطبيعية.
- **التوافق مع القوانين واللوائح** :سيكون هناك تركيز أكبر على الامتثال للقوانين واللوائح المتعلقة بالأمن السيبراني، خاصة مع ظهور القوانين الجديدة مثل GDPR والقوانين الأخرى المتعلقة بحماية البيانات.
- **التعاون الدولي** :سيزداد التعاون بين الدول لمواجهة التهديدات السيبرانية المتعددة الجنسيات، مع تبادل المعلومات والتقنيات بين الدول.

التحديات القادمة وكيفية الاستعداد لها

❖ **تواجه مجال الأمن السيبراني تحديات كبيرة في السنوات القادمة، ومن أبرزها:**

- **الهجمات الأساسية :**تتزايد الهجمات الأساسية التي تستهدف الأنظمة الأساسية والخدمات الحيوية، مثل الطاقة والمياه والاتصالات.
- **التقنيات الجديدة :**تطور التقنيات الجديدة مثل الذكاء الاصطناعي والتعلم الآلي يعني أن الجهود الأمنية يجب أن تكون متقدمة للتعامل مع هذه التحديات.
- **التكنولوجيا الناشئة :**مثل الهواتف الذكية الذكية والأجهزة المتصلة، تزيد من المساحات الضعيفة التي يمكن استغلالها.
- **التشريعات والسياسات :**تتغير التشريعات والسياسات الأمنية بسرعة، مما يتطلب تحديث المعايير والممارسات الأمنية بشكل مستمر.

❖ **للتحضير لهذه التحديات، يمكن اتباع الخطوات التالية:**

- **التدريب المستمر :**تعليم الموظفين والمطورين عن أحدث التهديدات وكيفية الوقاية منها.
- **التحديث المستمر للأنظمة :**تحديث الأنظمة الأمنية والبرمجيات بشكل مستمر لتغطية الثغرات الجديدة.
- **التعاون الدولي :**العمل مع الجهات الأخرى على المستوى الدولي لمشاركة المعلومات والتقنيات.
- **التحليل الاستمراري** :القيام بتحليلات دورية للأنظمة للكشف عن أي تهديدات محتملة