July Week 1: Data Backup & Recovery

Article Week 1

Data Backup & Recovery

النسخ الاحتياطي للبيانات واستعادتها

النسخ الاحتياطي للبيانات هو عملية حفظ نسخة من ملفاتك وأنظمتك في مكان آمن لاستخدامها لاحقاً عند حدوث خلل أو هجوم. هو بمثابة بوليصة تأمين رقمية، ضرورية وخط الدفاع الأول عند حدوث أي كارثة.

**ما هو؟**

النسخ الاحتياطي للبيانات هو عملية حفظ نسخة من ملفاتك وأنظمتك في مكان آمن لاستخدامها لاحقاً عند حدوث خلل أو هجوم. هو بمثابة بوليصة تأمين رقمية، ضرورية وخط الدفاع الأول عند حدوث أي كارثة.

**كيف يمكن أن يؤثر عليك؟**

* هجمات برمجيات الفدية: تستهدف الأنظمة الضعيفة وتسرق الملفات أو تطالب بمبالغ مالية كبيرة.
* فقدان البيانات: دون نسخ احتياطي قوي، قد تفقد بياناتك نهائياً.
* التعافي السريع: المؤسسات التي تملك نسخاً احتياطية تتعافى أسرع بنسبة 50%.
* توفير الخسائر: النسخ الاحتياطية يمكن أن توفر حتى 186,000 درهم من الخسائر.
* مثال: أحد الموظفين فقد ملفات مهمة بسبب هجوم برمجيات فدية، لكن المؤسسة التي اعتمدت نسخاً احتياطية تمكنت من استعادة البيانات بسرعة وتقليل الخسائر المالية.

**ما عليك فعله لتحمي نفسك:**

* كرر النسخ الاحتياطي باستمرار
* يومياً: لحماية بيانات العملاء والمعاملات
* أسبوعياً: للبيانات التشغيلية واستقرار بيئة العمل
* احرص على حماية أنظمة النسخ الاحتياطي
* تأكد من أنها غير متصلة مباشرة بالشبكة لتفادي الهجمات.
* احتفظ بنسخة خارجية
* استخدم مواقع تخزين سحابية أو وسائط خارجية مؤمنة.
* استعد لعملية التدقيق
* النسخ الاحتياطي يساعدك في الامتثال القانوني ويعزز جاهزيتك للتدقيق.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

Article Week 1

Data Backup & Recovery

Data backup means securely saving copies of your files and systems so you can restore them if something goes wrong.

**What is it?**Data backup means securely saving copies of your files and systems so you can restore them if something goes wrong.

How can it affect you?

* Ransomware attacks: Target vulnerable systems, stealing files or demanding large payments.
* Data loss: Without strong backups, you risk losing your data permanently.
* Faster recovery: Organizations with backups recover 50% faster.
* Cost savings: Backups can save up to AED 186,000 in losses.

Example: An employee lost important files due to a ransomware attack, but the organisation that used backups was able to quickly restore the data and reduce financial losses.

**How to protect yourself:**

* **Back up regularly:** • Daily: to protect customer data and transactions  
   • Weekly: for operational data and workplace stability
* **Secure your backup systems:** Make sure backups aren’t directly connected to your network to prevent cyberattacks
* **Keep an offsite copy:** Use secure cloud storage or encrypted external drives
* **Be audit-ready:** Backups help you stay legally compliant and prepared for audits

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.
3. Promote online safety for families, businesses, and the community by spreading this knowledge.





July Week 2: VPNs on Public Wi-Fi

**Week 2:**

**VPNs on Public Wi-Fi**

**الـVPN وشبكة الواي فاي العامة**

الـVPN (الشبكة الخاصة الافتراضية) هو أداة تقوم بتشفير اتصالك بالإنترنت، خاصة عند استخدام شبكات الواي فاي العامة مثل تلك الموجودة في المقاهي أو المطارات أو غيرها.

**ما هو؟**

الـVPN (الشبكة الخاصة الافتراضية) هو أداة تقوم بتشفير اتصالك بالإنترنت، خاصة عند استخدام شبكات الواي فاي العامة مثل تلك الموجودة في المقاهي أو المطارات أو غيرها.

**كيف يمكن أن يؤثر عليك؟**

الاتصال بالشبكات العامة دون VPN: الاتصال بشبكات عامة دون VPN قد يعرض معلوماتك الشخصية للخطر.

كشف المعلومات الشخصية: كلمات المرور، التفاصيل المصرفية، والمحادثات يمكن أن تكون مكشوفة.

اعتراض البيانات: القراصنة قد يعترضون اتصالك أو يوجّهونك لمواقع مزيفة.

سرقة البيانات الخاصة: يمكن للقراصنة قراءة بياناتك الخاصة بسهولة.

مثال: استخدم أحد المستخدمين شبكة واي فاي عامة في مقهى بدون VPN، وتمكن قراصنة من اعتراض اتصاله وسرقة بياناته المصرفية ورسائل البريد الشخصي.

**ما عليك فعله لتحمي نفسك:**

· حمّل تطبيق VPN موثوق.

· فعّله قبل التصفح على شبكة عامة.

· وتجنّب تسجيل الدخول إلى حساباتك الشخصية على الشبكات المفتوحة.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

-البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

-تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة

**VPNs on Public Wi-Fi**

A VPN (Virtual Private Network) is a tool that encrypts your internet connection, especially when using public Wi-Fi networks like those in cafes, airports, or other public places.

**What is it?**A VPN (Virtual Private Network) is a tool that encrypts your internet connection, especially when using public Wi-Fi networks like those in cafes, airports, or other public places.

How can it affect you?

* Connecting to public networks without a VPN: Using public Wi-Fi without protection can expose your personal information.
* Personal data exposure: Passwords, banking details, and conversations may be at risk.
* Data interception: Hackers can intercept your connection or redirect you to fake websites.
* Private data theft: Cybercriminals can easily access and read your private information.

Example: A user connected to public Wi-Fi at a café without a VPN. Hackers intercepted the connection and stole their banking details and personal emails.

**How to protect yourself:**

* Download a trusted VPN app
* Activate it before browsing on public networks
* Avoid logging into personal accounts on open networks

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

July Week 3: Keeping Software & Devices Updated

**Week 3:**

**Keeping Software & Devices Updated**

**الحفاظ على تحديث البرامج والأجهزة**

تحديث البرامج والأجهزة يعني تحميل آخر الإصدارات الرسمية التي تصدرها الشركات المصنعة لإصلاح الثغرات وتحسين الأمان والأداء.

**ما هو؟**

تحديث البرامج والأجهزة يعني تحميل آخر الإصدارات الرسمية التي تصدرها الشركات المصنعة لإصلاح الثغرات وتحسين الأمان والأداء.

**كيف يمكن أن يؤثر عليك؟**

إهمال التحديثات: عدم تحديث الأنظمة يعرضك لمخاطر كبيرة.

زيادة التعرض للهجمات: الأنظمة غير المُحدثة أكثر عرضة بنسبة 70% للهجمات الإلكترونية.

ثغرات متزايدة: تم اكتشاف أكثر من 30,000 ثغرة في عام 2024 وحده.

خطر الاختراق: التأخير في التحديث قد يؤدي إلى اختراق بياناتك أو شبكتك.

مثال: أحد الموظفين لم يحدّث نظامه لعدة أشهر، ما سمح لقراصنة باستغلال ثغرة والوصول إلى بيانات الشركة الحساسة.

**ما عليك فعله لتحمي نفسك:**

فعّل التحديثات التلقائية على جميع أجهزتك.

راجع إعدادات التحديث في الهواتف، الحواسب، المتصفحات، أجهزة الراوتر، والتقنيات المنزلية الذكية.

لا تستخدم أجهزة أو برامج قديمة غير مدعومة.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

**Keeping Software & Devices Updated**

Keeping your software and devices up to date means downloading the latest official updates to patch vulnerabilities and boost security performance.

**What is it?**Keeping your software and devices up to date means downloading the latest official updates to patch vulnerabilities and boost security performance.

**How can it affect you?**

* Neglecting updates: Failing to update your systems exposes you to serious risks.
* Increased vulnerability: Outdated systems are 70% more likely to face cyberattacks.
* Growing threats: Over 30,000 vulnerabilities were discovered in 2024 alone.
* Risk of breach: Delaying updates can lead to your data or network being compromised.

Example: An employee failed to update their system for several months, allowing hackers to exploit a vulnerability and gain access to the company’s sensitive data.

**How to protect yourself:**

* Enable automatic updates for all your devices
* Review update settings on your phones, computers, browsers, routers, and smart home devices
* Avoid using outdated hardware and software

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

July Week 4: Email Encryption & Secure Comm

### **Week 4**

**Email Encryption & Secure Communication**

Email encryption is a security measure that protects your messages by ensuring only the intended recipient can read them.

**What is it?**Email encryption is a security measure that protects your messages by ensuring only the intended recipient can read them.

**How can it affect you?**

* Lack of encryption: Without encryption, your emails are vulnerable to interception.
* Unauthorised access: Cybercriminals may gain access to confidential information.
* Identity theft: Hackers can impersonate you and exploit your data for fraud.
* Security risks: This puts both your personal and professional security at risk.

Example: An employee received an email through an unencrypted account. Hackers intercepted it and used the sensitive information to carry out a fraud against the company.

**How to protect yourself:**

* Enable encryption features in Gmail and Outlook to secure your emails
* Use only trusted and verified websites for transactions and communications
* Avoid making purchases from unknown sources or via social media platforms
* Steer clear of instant transfers or payment methods that lack proper verification

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

**تشفير البريد الإلكتروني والاتصالات الآمنة**

تشفير البريد الإلكتروني هو إجراء أمني يهدف إلى حماية رسائلك، بحيث لا يمكن قراءتها إلا من قبل المستلم المقصود. وهذا يحافظ على معلوماتك الحساسة آمنة من المتسللين والمحتالين الذين يحاولون اعتراض بياناتك أو إساءة استخدامها.

**ما هو التشفير؟**

تشفير البريد الإلكتروني هو إجراء أمني يهدف إلى حماية رسائلك، بحيث لا يمكن قراءتها إلا من قبل المستلم المقصود. وهذا يحافظ على معلوماتك الحساسة آمنة من المتسللين والمحتالين الذين يحاولون اعتراض بياناتك أو إساءة استخدامها.

**كيف يمكن أن يؤثر عليك؟**

غياب التشفير: في حال عدم استخدام التشفير، تصبح رسائل بريدك الإلكتروني عرضة للاعتراض.

الوصول غير المصرح به: قد يتمكن مجرمو الإنترنت من الوصول إلى معلومات سرية.

انتحال الهوية: القراصنة يمكنهم انتحال هويتك واستغلال بياناتك في عمليات احتيال.

تعرض الأمن للخطر: هذا يعرض أمنك الشخصي والمهني للخطر.

مثال: تلقى أحد الموظفين رسالة عبر بريد غير مشفر، وتمكن قراصنة من اعتراضها واستخدام المعلومات الحساسة للقيام بعملية احتيال على الشركة.

**كيف تحمي نفسك؟**

• فعّل ميزات التشفير في خدمات البريد الإلكتروني مثل Gmail وOutlook

• استخدم مواقع موثوقة وموثّقة فقط في المعاملات والاتصالات

• تجنّب الشراء من مصادر غير معروفة أو عبر منصات التواصل الاجتماعي

• ابتعد عن التحويلات الفورية أو وسائل الدفع التي لا توفر تحققاً آمناً

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

-البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

-تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

July Week 5: Social Media Privacy

Social Media Privacy

Social media privacy is the practice of protecting the personal information and digital footprint you create through your posts, logins, and online activity.   
**What is it?**Social media privacy is the practice of protecting the personal information and digital footprint you create through your posts, logins, and online activity.

**How can it affect you?**  
Failing to safeguard your social media privacy can lead to:

* Tracking and monitoring of your online activity
* Privacy breaches that expose sensitive details
* Fraud and scams using your personal information

Example: One employee shared too much personal information online, which allowed scammers to impersonate them and gain access to their company’s confidential data.

**How to protect yourself**

* Turn off location tagging: Disable geotags on posts to protect your privacy.
* Review your followers: Regularly check your list and don’t accept requests from strangers.
* Download apps safely: Use trusted app stores and review permissions before downloading.
* Enable two-factor authentication (2FA): Add an extra layer of protection to your accounts.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

**خصوصية وسائل التواصل الاجتماعي**

**خصوصية وسائل التواصل الاجتماعي هي ممارسة حماية المعلومات الشخصية والآثار الرقمية التي تتركها من خلال منشوراتك وتسجيلات دخولك وأنشطتك عبر الإنترنت.**

**ما هو؟**

خصوصية وسائل التواصل الاجتماعي هي ممارسة حماية المعلومات الشخصية والآثار الرقمية التي تتركها من خلال منشوراتك وتسجيلات دخولك وأنشطتك عبر الإنترنت.

**كيف يمكن أن يؤثر عليك؟**

قد يؤدي عدم حماية خصوصية وسائل التواصل الاجتماعي الخاصة بك إلى:

-تتبع ومراقبة نشاطك على الإنترنت

-انتهاكات الخصوصية التي تكشف عن تفاصيل حساسة

-الاحتيال والخداع باستخدام معلوماتك الشخصية

**كيف تحمي نفسك؟**

إيقاف تحديد الموقع: عطّل ميزة تحديد الموقع الجغرافي في منشوراتك لحماية خصوصيتك.

مراجعة المتابعين: راجع قائمة متابعيك بانتظام ولا تقبل طلبات من أشخاص مجهولين.

تنزيل التطبيقات بأمان: نزّل التطبيقات فقط من المتاجر الموثوقة وراجع الصلاحيات المطلوبة قبل التثبيت.

المصادقة الثنائية: فعّل المصادقة الثنائية لإضافة طبقة أمان إضافية لحساباتك.

مثال: قامت إحدى المستخدمات بتفعيل المصادقة الثنائية وتعطيل الموقع الجغرافي، مما منع محاولة اختراق حسابها بعد أن حاول مجهول الوصول إليه عبر تطبيق غير موثوق.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

* البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.
* تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

August Week 1 AR+EN

**August week 1**

**Social Engineering: outsmart the scammers**

**الهندسة الاجتماعية: تفوق على المحتالين**

هو استغلال الثقة والعواطف لخداعك والحصول على معلوماتك، بدلاً من الاعتماد فقط على البرامج الخبيثة.

**ما هو؟**

هو استغلال الثقة والعواطف لخداعك والحصول على معلوماتك، بدلاً من الاعتماد فقط على البرامج الخبيثة.

**كيف يمكن أن يؤثر عليك؟**

* سرقة البيانات: قد يؤدي خداعك إلى تسريب معلوماتك الشخصية أو المصرفية واختراق حساباتك الرقمية.
* استغلال العواطف: يستخدم المحتالون الضغط، الخوف أو وعود المكافآت لدفعك إلى تصرفات مضرة بك أو بمؤسستك.
* العواقب: النتائج قد تشمل خسائر مالية، انتهاك الخصوصية أو تشويه السمعة.

مثال: رسائل احتيالية مزيّفة باسم المصرف تستغل خوفك لتسرق بياناتك وتؤدي إلى خسائر مالية وانتهاك الخصوصية.

**ما عليك فعله لتحمي نفسك:**

* لا تثق بالطلبات الرقمية غير المتوقعة.
* راقب دائمًا لغة الرسائل وطريقتها.
* لا تشارك معلوماتك أو أسرارك عبر الإنترنت أو الهاتف.
* تأكد من هوية من تتواصل معه قبل الرد أو التفاعل.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

Social Engineering: Outsmart the Scammers

It is the exploitation of trust and emotions to deceive you and obtain your information, instead of relying only on malicious software.

What is it?  
It is the exploitation of trust and emotions to deceive you and obtain your information, instead of relying only on malicious software.

How can it affect you?

* Data theft: You may be tricked into revealing personal or banking details, leading to hacked accounts.
* Emotional manipulation: Scammers use fear, pressure, or promises of rewards to push you into harmful actions.
* Consequences: This can result in financial loss, privacy violations, or reputational damage.

Example: Fake emails in your bank’s name exploit fear to steal your data, causing financial loss and privacy breaches.

How to protect yourself?

* Don’t trust unexpected digital requests.
* Watch the language and tone of messages.
* Never share your information or secrets online or over the phone.
* Verify who you’re dealing with before replying or engaging.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

August week 2 EN+ AR

Mobile Device Security

**Mobile Device Security: Protect Your Pocket**

Smartphones and tablets carry sensitive and financial data, making them a top target for cybercriminals.

What is it?  
Smartphones and tablets carry sensitive and financial data, making them a top target for cybercriminals.

How can it affect you?  
Failing to secure your mobile device can lead to:

* Sensitive and financial data being exposed
* Tracking and theft through weak PIN codes
* Malware infections from unsafe downloads
* Higher risks as 60% of users ignore updates and malware attacks on smartphones have increased by 50% in recent years

Example  
One user relied on a simple PIN and downloaded a free app. Hackers used it to steal their banking login, leading to unauthorized transactions.

How to protect yourself?   
• Regularly update your operating system and apps  
• Create a strong PIN  
• Enable face ID, fingerprint, or other biometric locks  
• Download apps only from secure and trusted source

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

**أمن الأجهزة المحمولة: احمِ جيبك**

تحتوي الهواتف الذكية والأجهزة اللوحية على بيانات حساسة ومالية، مما يجعلها هدفاً رئيسياً للمجرمين الإلكترونيين.

**ما هو؟**

تحتوي الهواتف الذكية والأجهزة اللوحية على بيانات حساسة ومالية، مما يجعلها هدفاً رئيسياً للمجرمين الإلكترونيين.

**كيف يمكن أن يؤثر ذلك عليك؟**

قد يؤدي عدم تأمين جهازك المحمول إلى:

• كشف البيانات الحساسة والمالية

• التتبع والسرقة من خلال رموز PIN الضعيفة

• الإصابة بالبرامج الضارة من التنزيلات غير الآمنة

• مخاطر أعلى حيث يتجاهل 60٪ من المستخدمين التحديثات وزادت هجمات البرامج الضارة على الهواتف الذكية بنسبة 50٪ في السنوات الأخيرة

مثال: اعتمد أحد المستخدمين على رقم تعريف شخصي بسيط وقام بتنزيل تطبيق مجاني. استخدمه المتسللون لسرقة معلومات تسجيل الدخول إلى حسابه المصرفي، مما أدى إلى إجراء معاملات غير مصرح بها.

**كيف تحمي نفسك؟**

• قم بتحديث نظام التشغيل والتطبيقات بانتظام.

• أنشئ رقم تعريف شخصي قوي.

• قم بتمكين ميزة التعرف على الوجه أو بصمة الإصبع أو أي أقفال بيومترية أخرى.

• قم بتنزيل التطبيقات من مصادر آمنة وموثوقة فقط

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

August week 3 EN+ AR

### **Digital Banking: Greater Security**

Digital banking security is the practice of protecting your accounts and transactions through tools like Face ID, multi-factor authentication (MFA), and trusted apps.

**What is it?**Digital banking security is the practice of protecting your accounts and transactions through tools like Face ID, multi-factor authentication (MFA), and trusted apps.

**How can it affect you?**Neglecting your digital banking security can lead to:

* Stolen credentials: Hackers can use your login details to access accounts and make fraudulent transactions.
* Financial losses: Unauthorized transfers or stolen funds can cause severe personal or business damage.
* Legal consequences: You may face disputes or investigations over compromised accounts.

**Example:**

A customer fell for a phishing email and unknowingly gave away their online banking password. Because Face ID was enabled on their app, the criminals could not log in from another device, preventing unauthorized access.

**How to protect yourself:**

* Use apps that support multi-factor authentication (MFA)
* Enable transaction notifications and alerts
* Avoid accessing accounts on public devices
* Never share personal data through calls or messages
* Don’t respond to suspicious calls
* Keep your banking apps updated regularly
* Use only trusted, official channels

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

**الخدمات المصرفية الرقمية: أمان أكبر**

أمن الخدمات المصرفية الرقمية هو ممارسة حماية حساباتك ومعاملاتك عبر أدوات مثل التعرف على الوجه (Face ID)، والمصادقة متعددة العوامل (MFA)، والتطبيقات الموثوقة.

**ما هو؟**

أمن الخدمات المصرفية الرقمية هو ممارسة حماية حساباتك ومعاملاتك عبر أدوات مثل التعرف على الوجه (Face ID)، والمصادقة متعددة العوامل (MFA)، والتطبيقات الموثوقة.

**كيف يمكن أن يؤثر عليك؟**

إهمال الأمان المصرفي الرقمي قد يؤدي إلى:

* سرقة بيانات الدخول: يمكن للمتسللين استخدام بياناتك للوصول إلى الحسابات وإجراء معاملات احتيالية.
* خسائر مالية: التحويلات غير المصرح بها أو سرقة الأموال قد تسبب أضراراً جسيمة على المستوى الشخصي أو للأعمال.
* عواقب قانونية: قد تواجه نزاعات أو تحقيقات نتيجة اختراق الحسابات.

مثال:

أحد العملاء وقع ضحية لرسالة تصيد إلكتروني (Phishing) وشارك كلمة مرور حسابه المصرفي عبر الإنترنت دون قصد. ولكن بفضل تفعيل ميزة التعرف على الوجه في التطبيق، لم يتمكن المجرمون من تسجيل الدخول من جهاز آخر، مما حال دون الوصول غير المصرح به.

**كيف تحمي نفسك؟**

استخدم تطبيقات تدعم المصادقة متعددة العوامل (MFA).

فعّل إشعارات وتنبيهات المعاملات.

تجنّب الدخول إلى الحسابات من الأجهزة العامة.

لا تشارك بياناتك الشخصية عبر المكالمات أو الرسائل.

لا تستجب للمكالمات المشبوهة.

حافظ على تحديث تطبيقاتك المصرفية بشكل منتظم.

استخدم القنوات الرسمية والموثوقة فقط.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

August week 4 EN+ AR

"اشترِ الآن وادفع لاحقاً" (BNPL

خدمات "اشترِ الآن وادفع لاحقاً" (BNPL) تسمح لك بالشراء الفوري وتأجيل الدفع على أقساط، لكنها أصبحت هدفاً رئيسياً لعمليات الاحتيال.

**ما هو؟**

خدمات "اشترِ الآن وادفع لاحقاً" (BNPL) تسمح لك بالشراء الفوري وتأجيل الدفع على أقساط، لكنها أصبحت هدفاً رئيسياً لعمليات الاحتيال.

**كيف يمكن أن يؤثر عليك؟**

* عمليات شراء مزيفة: قد تُستخدم بياناتك المسروقة لإجراء عمليات شراء باسمك.
* خسائر مالية: يمكن أن تتحمل خسائر مالية بسبب ضعف التحقق أو بطء الاستجابة.
* سرقة الحسابات: قد تتعرض لسرقة حساباتك أو استغلال بياناتك الشخصية.

**مثال**: قد يؤدي تسريب بياناتك المصرفية إلى إجراء عمليات شراء مزيفة باسمك، وخسارة أموالك، بل وحتى سرقة حساباتك واستغلال بياناتك الشخصية.

**ما عليك فعله لتحمي نفسك:**

استخدم كلمات مرور قوية وفريدة.

فعّل التحقق المتعدد العوامل (MFA).

راقب تنبيهات المعاملات باستمرار.

بلّغ فوراً عن أي نشاط مشبوه.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

BNPL (Buy Now, Pay Later) allows you to buy immediately and pay later in installments, but these services are increasingly vulnerable to fraud.

**What is it?**BNPL (Buy Now, Pay Later) allows you to buy immediately and pay later in installments, but these services are increasingly vulnerable to fraud.

**How can it affect you?**

* Fake purchases: Stolen credentials may be used to make transactions in your name.
* Financial losses: You could bear the costs due to weak authentication or delayed provider response.
* Account takeover: Criminals may steal your accounts or misuse your personal details.

Example: A leak of your banking details could lead to fraudulent purchases in your name, financial loss, and even account takeover with misuse of your personal data.

**How to protect yourself:**

* Use strong, unique passwords.
* Enable Multi-Factor Authentication (MFA).
* Monitor transaction alerts regularly.
* Report any suspicious activity immediately.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

September week 1 AR+EN

**المنازل الذكية**

**Smart Homes**

المنازل الذكية تعتمد على أجهزة إنترنت الأشياء (IoT) مثل المساعدات الصوتية، الكاميرات، وأجهزة المراقبة، لزيادة الراحة والتحكم عن بُعد.

**ما هو؟** المنازل الذكية تعتمد على أجهزة إنترنت الأشياء (IoT) مثل المساعدات الصوتية، الكاميرات، وأجهزة المراقبة، لزيادة الراحة والتحكم عن بُعد. لكن **70% من هذه الأجهزة معرضة للهجمات الإلكترونية**.

**كيف يمكن أن يؤثر عليك؟**

* اختراق محتمل: الاتصال التلقائي بالإنترنت قد يفتح الباب للاختراق.
* تجسس مباشر: إبقاء المساعد الصوتي في حالة التشغيل الدائم يسمح بالتجسس.
* خطر الشبكة: مشاركة كلمة مرور الواي فاي الرئيسية مع الضيوف قد تعرّض شبكتك للخطر.
* انتهاك الخصوصية: أجهزة مراقبة الأطفال قد يتم اختراقها للتحدث معهم أو تسجيل المحادثات والتحركات داخل المنزل.

**مثال**: قد يؤدي إبقاء المساعد الصوتي في وضع التشغيل الدائم أو مشاركة كلمة مرور الواي فاي مع الآخرين إلى اختراق أجهزتك، مما يعرّض خصوصيتك وعائلتك للتجسس والمخاطر.

**ما عليك فعله لتحمي نفسك:**

* استخدم كلمات مرور قوية ومختلفة.
* حدّث أنظمة وأجهزة المنزل الذكي باستمرار.
* اختر الأجهزة حسب احتياجاتك فقط.
* تحكّم بها من جهاز واحد موثوق.
* فعّل إعدادات الأمان والخصوصية.
* أطفئ المساعد الذكي عند عدم الاستخدام.
* خصص شبكة واي فاي خاصة للضيوف.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

### **Smart Homes**

Smart homes rely on Internet of Things (IoT) devices such as voice assistants, cameras, and monitoring systems to provide comfort and remote control.

**What is it?**Smart homes rely on Internet of Things (IoT) devices such as voice assistants, cameras, and monitoring systems to provide comfort and remote control. However, 70% of these devices are vulnerable to cyberattacks.

* Hacking risks: Always-on internet connections can make your devices easier to breach.
* Spying concerns: A voice assistant left running may allow outsiders to eavesdrop.
* Network exposure: Sharing your primary Wi-Fi password with guests can put your whole network at risk.
* Privacy breaches: Baby monitors or smart cameras could be hacked to speak to children or record conversations and activity inside your home.

Example: Keeping your voice assistant always on or sharing your Wi-Fi password with others could expose your devices to hacking, putting your privacy and family at risk of spying and other threats.

**How to protect yourself:**

* Use strong and different passwords.
* Keep smart home devices and systems updated.
* Choose devices that fit your needs.
* Control all devices from one spot.
* Enable security and privacy settings.
* Turn off the smart assistant when not in use.
* Set up a separate Wi-Fi network for guests.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

September week 2 AR+ EN

**Secure Video Conferencing**

**كاميرا ويب آمنة في الاجتماعات**

كاميرا ويب آمنة في الاجتماعات تعني استخدام الكاميرا والبرامج المرافقة ضمن بيئة محمية، بحيث يتم تشفير الاتصال ومنع الوصول غير المصرح به، مما يضمن سرية الصوت والصورة وحماية بيانات المشاركين من التجسس أو الاختراق.

**ما هو؟**

كاميرا ويب آمنة في الاجتماعات تعني استخدام الكاميرا والبرامج المرافقة ضمن بيئة محمية، بحيث يتم تشفير الاتصال ومنع الوصول غير المصرح به، مما يضمن سرية الصوت والصورة وحماية بيانات المشاركين من التجسس أو الاختراق.

**كيف يمكن أن يؤثر عليك؟**

* انتهاك الخصوصية: تصويرك أو تسجيل محادثاتك دون علمك.
* مخاطر الابتزاز: استخدام الصور والفيديوهات لتهديدك مقابل المال.
* تسريب معلومات حساسة: كشف تفاصيل شخصية أو مهنية من الاجتماعات الافتراضية.
* استغلال اجتماعاتك: الدخول غير المصرح به قد يؤدي إلى سرقة بيانات أو عرقلة أعمالك.

**مثال**: قد يتم تسجيل اجتماعك الافتراضي دون علمك، ثم استغلال الصور أو المحادثات لابتزازك مالياً أو تسريب معلوماتك الحساسة.

**ما عليك فعله لتحمي نفسك:**

* لا تُشغّل الكاميرا إلا عند الحاجة، واستخدم خاصية التمويه.
* ضع غطاءً للكاميرا عند عدم الاستخدام.
* أنشئ رابطاً جديداً لكل اجتماع مع كلمة مرور واقفل غرفة الانتظار.
* حدّث جهازك بانتظام، ولا تضغط على روابط غير موثوقة.
* استخدم شبكات VPN موثوقة لزيادة الأمان.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

### Secure Video Conferencing

Secure video conferencing is the use of webcams and conferencing tools in a protected setup, ensuring encrypted communication, preventing unauthorized access, and safeguarding participants’ voice, video, and data.

What is it?  
Secure video conferencing is the use of webcams and conferencing tools in a protected setup, ensuring encrypted communication, preventing unauthorized access, and safeguarding participants’ voice, video, and data.

How can it affect you?

* Privacy violation: Your image or conversations may be recorded without your knowledge.
* Blackmail risks: Photos or videos can be used to extort money.
* Data leaks: Sensitive personal or professional details from virtual meetings can be exposed.
* Meeting exploitation: Unauthorized access can lead to stolen data or disruptions to your work.

Example: Your virtual meeting may be recorded without your knowledge, with images or conversations later used for blackmail or to leak sensitive information.

How to protect yourself:

* Switch on your camera only when needed and use blur or background filters.
* Cover your webcam when not in use.
* Create a new meeting link for every session, add a password, and enable waiting rooms.
* Keep your device updated and avoid clicking suspicious links.
* Use a trusted VPN for added security.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

Promote online safety for families, businesses, and the community by spreading this knowledge.

September week 3 AR+ EN

**Managing Your Digital Footprint**

**إدارة بصمتك الرقمية**

عملية متابعة وتنظيم كل ما تتركه من آثار في العالم الرقمي مثل حساباتك، منشوراتك، وملفاتك الشخصية. الهدف منها حماية هويتك، تقليل المخاطر مثل الاحتيال أو سرقة البيانات، وضمان أن تواجدك الإلكتروني يعكس ما تريد أنت فقط.

**ما هو؟**

عملية متابعة وتنظيم كل ما تتركه من آثار في العالم الرقمي مثل حساباتك، منشوراتك، وملفاتك الشخصية. الهدف منها حماية هويتك، تقليل المخاطر مثل الاحتيال أو سرقة البيانات، وضمان أن تواجدك الإلكتروني يعكس ما تريد أنت فقط.

**كيف يمكن أن يؤثر عليك؟**

* سرقة الهوية: بياناتك المنشورة قد تُستخدم لانتحال شخصيتك.
* الاحتيال عبر الإنترنت: ملفاتك الشخصية العلنية قد تُستغل في الاحتيال.
* ضعف الأمان: حساباتك القديمة غير المحمية تصبح هدفاً سهلاً للمخترقين.

**مثال:**

قد يعثر أحد المحتالين على حساب قديم لك على أحد مواقع التواصل لم تعد تستخدمه. باستخدام المعلومات المنشورة فيه، مثل بريدك الإلكتروني أو تاريخ ميلادك، يتمكن من اختراق حساباتك الأخرى وارتكاب عمليات احتيال باسمك.

**ما عليك فعله لتحمي نفسك:**

* ابحث عن اسمك وتحقق مما هو منشور عنك.
* احذف حساباتك غير المستخدمة.
* حدّث إعدادات الخصوصية باستمرار.
* اجعل ملفاتك الشخصية خاصة وحدد من يمكنه متابعتك.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

## **Managing Your Digital Footprint**

Managing your digital footprint means keeping track of and controlling everything you leave behind online, such as your accounts, posts, and profiles.

### **What is it?**

Managing your digital footprint means keeping track of and controlling everything you leave behind online, such as your accounts, posts, and profiles. The goal is to protect your identity, lower risks like fraud or data theft, and make sure your online presence reflects only what you choose.

**How can it affect you?**

* Identity theft: Your shared data could be used to impersonate you.
* Online fraud: Public profiles can be exploited for scams.
* Weak security**:** Old or unprotected accounts can become easy targets for hackers.

E**xample**

A scammer finds one of your old social media accounts that you no longer use. Using details posted there, such as your email address or date of birth, they manage to break into your other accounts and commit fraud in your name.

**How to protect yourself**

* Search your name and see what information is publicly visible.
* Delete accounts you no longer use.
* Regularly update your privacy settings.
* Keep your profiles private and control who can follow you.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

September week 4 EN+AR

## **Artificial Intelligence: A Tool to Invade Your Privacy and Steal Your Data**

Artificial Intelligence is the ability of systems to mimic human actions, such as imitating voices, tones, and even faces, to appear trustworthy and convincing.

### **What is it?**

Artificial Intelligence is the ability of systems to mimic human actions, such as imitating voices, tones, and even faces, to appear trustworthy and convincing.

**How can it affect you?**

Failing to recognize AI threats can lead to:

* Unsafe actions such as transferring money or sharing personal information
* Loss of trust through deception and manipulation
* Exploitation of your weaknesses through scams and phishing attacks
* Sensitive data being analysed and shared with third parties without your knowledge

**Example**

A user was contacted by what seemed to be their bank. The AI-generated voice imitated a customer service agent, convincing the user to share their ID details. These details were later used to access their accounts and commit fraud.

**How to protect yourself?**

* Never share family members’ names, card numbers, PINs, addresses, dates of birth, or ID details with AI tools
* Be cautious with AI chatbots; they are not bound by confidentiality laws
* Ignore suspicious messages that create urgency or fear
* Stay vigilant: even the smallest detail you share could be used against you

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

**الذكاء الاصطناعي: أداة لانتهاك خصوصيتك وسرقة بياناتك**

الذكاء الاصطناعي هو قدرة الأنظمة على تقليد أفعال البشر، مثل تقليد الأصوات والنبرات وحتى الوجوه، للظهور بشكل موثوق ومقنع.

**ما هو؟**

الذكاء الاصطناعي هو قدرة الأنظمة على تقليد أفعال البشر، مثل تقليد الأصوات والنبرات وحتى الوجوه، للظهور بشكل موثوق ومقنع.

**كيف يمكن أن يؤثر عليك؟**

* عدم إدراك تهديدات الذكاء الاصطناعي قد يؤدي إلى:
* القيام بأعمال غير آمنة مثل تحويل الأموال أو مشاركة معلومات شخصية.
* فقدان الثقة نتيجة الخداع والتلاعب.
* استغلال نقاط ضعفك من خلال الاحتيال وهجمات التصيّد.
* تحليل بياناتك الحساسة ومشاركتها مع أطراف ثالثة دون علمك.

**مثال**

تلقى أحد المستخدمين اتصالًا بدا وكأنه من البنك. استخدم الصوت المُولّد بالذكاء الاصطناعي لتقليد موظف خدمة العملاء، مما أقنع المستخدم بمشاركة تفاصيل بطاقته التعريفية. لاحقًا استُخدمت هذه البيانات للوصول إلى حساباته وارتكاب عمليات احتيال.

**ما عليك فعله لتحمي نفسك؟**

* لا تشارك أسماء أفراد العائلة أو أرقام البطاقات أو الرموز السرية (PIN) أو العناوين أو تواريخ الميلاد أو بيانات الهوية مع أدوات الذكاء الاصطناعي.
* كن حذرًا عند استخدام روبوتات المحادثة بالذكاء الاصطناعي، فهي ليست ملزمة بقوانين السرية.
* تجاهل الرسائل المشبوهة التي تثير الخوف أو الاستعجال.
* ابقَ يقظًا: حتى أصغر تفصيل تشاركه قد يُستخدم ضدك.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.

September week 5 EN+AR

## **Scam Calls: Outsmart Fraudsters**

Scam calls are fraudulent phone calls designed to trick you into sharing personal information or sending money through threats, pressure, or fake offers.

### **What is it?**

Scam calls are fraudulent phone calls designed to trick you into sharing personal information or sending money through threats, pressure, or fake offers.

**How can it affect you?**

Neglecting to protect yourself from scam calls can lead to:

* **Stolen identity:** Criminals can use your voice or personal details to access sensitive accounts.
* **Financial losses:** Fraudsters may trick you into making payments or transferring money.
* **Emotional stress:** Constant threats and pressure can cause panic, confusion, and long-term anxiety.
* **Exploitation:** Scammers may request gift cards, cryptocurrency, or wire transfers that are hard to recover.

**Example**

A user received a call from someone posing as their bank. The caller pressured them into saying “yes” to confirm their account. That short recording was later misused to authorize fraudulent transactions.

**How to protect yourself**

* Don’t say “yes” to unknown callers, as your voice could be recorded and misused.
* Block suspicious numbers immediately to prevent repeated attempts.
* Avoid calling back numbers you do not recognize, even if they appear urgent.
* Don’t press buttons to “confirm” your number or respond to automated prompts.
* Watch for red flags such as “too good to be true” offers, urgent threats, or requests for gift cards and prepaid cards.

Stay Responsible: Follow and Share CSC Content

Your support can make a significant impact in building a secure digital future for everyone:

1. Staying informed is key to protecting yourself and your loved ones from online threats.
2. Follow our social media channels and website for regular updates on cybersecurity best practices.

**المكالمات الاحتيالية: كيف تتغلب على المحتالين**

المكالمات الاحتيالية هي اتصالات هاتفية مزيفة تهدف إلى خداعك لمشاركة معلوماتك الشخصية أو إرسال المال باستخدام التهديد أو الضغط أو العروض الوهمية.

**ما هو؟**

المكالمات الاحتيالية هي اتصالات هاتفية مزيفة تهدف إلى خداعك لمشاركة معلوماتك الشخصية أو إرسال المال باستخدام التهديد أو الضغط أو العروض الوهمية.

**كيف يمكن أن يؤثر عليك؟**

* إهمال حماية نفسك من المكالمات الاحتيالية قد يؤدي إلى:
* سرقة الهوية: قد يستخدم المجرمون صوتك أو بياناتك الشخصية للوصول إلى حسابات حساسة.
* خسائر مالية: قد يخدعك المحتالون لدفع مبالغ أو تحويل أموال.
* ضغط نفسي: التهديدات والضغط المستمر قد يسببان ذعرًا، ارتباكًا وقلقًا طويل الأمد.
* استغلال مباشر: قد يطلب منك المحتالون بطاقات هدايا، عملات مشفّرة، أو تحويلات مالية يصعب استردادها.

**مثال**

تلقى أحد المستخدمين مكالمة من شخص انتحل صفة البنك. ضغط عليه المتصل ليقول كلمة “نعم” لتأكيد حسابه. لاحقًا استُخدم هذا التسجيل القصير للموافقة على معاملات مالية احتيالية.

**ما عليك فعله لتحمي نفسك:**

* لا تقل “نعم” للمتصلين المجهولين، فقد يُسجَّل صوتك ويُستخدم بشكل سيئ.
* احظر الأرقام المشبوهة فورًا لتفادي المحاولات المتكررة.
* تجنّب معاودة الاتصال بأرقام لا تعرفها حتى لو بدت عاجلة.
* لا تضغط على الأزرار لتأكيد رقمك أو الاستجابة للردود الآلية.
* انتبه للإشارات التحذيرية مثل العروض “الخيالية”، التهديدات العاجلة، أو طلب بطاقات هدايا وبطاقات مسبقة الدفع.

كن مسؤولاً: تابع وشارك محتوى مجلس الأمن السيبراني

دعمك يصنع فارقاً كبيراً في بناء مستقبل رقمي آمن للجميع:

البقاء على اطلاع هو المفتاح لحماية نفسك وأحبّائك من التهديدات الإلكترونية.

تابع قنواتنا على وسائل التواصل وموقعنا الإلكتروني للحصول على تحديثات منتظمة حول أفضل ممارسات الأمن السيبراني.

ساهم في تعزيز السلامة الرقمية للأسر، والأعمال، والمجتمع من خلال نشر هذه المعرفة.