**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* Increased vulnerability: Outdated systems are 70% more likely to face cyberattacks.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* Avoid using outdated hardware and software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.