### **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.