نشرة توعوية: الوقاية من المخاطر السيبرانية

ما هي المخاطر السيبرانية؟

المخاطر السيبرانية هي التهديدات التي تستهدف الأجهزة الإلكترونية أو الشبكات أو البيانات، وتهدف إلى سرقة المعلومات أو تدميرها أو تعطيل الأنظمة.

تشمل هذه التهديدات:

- **الفيروسات والبرمجيات الخبيثة(Malware)**
- **الاحتيال الإلكتروني(Phishing)**
- **الاختراق وسرقة البيانات**
- **ابتزاز المستخدمين(Ransomware)**
- **الهجمات على الشبكات والخوادم**

أمثلة على الهجمات الشائعة:

١. **رسائل بريد إلكتروني مزيفة** تطلب منك الضغط على رابط لتحديث بياناتك البنكية.
٢. **مواقع وهمية** تشبه المواقع الرسمية للحصول على كلمات المرور.
٣. **أجهزة USB مجهولة المصدر** تحتوي على برمجيات خبيثة.
٤. **رسائل عبر وسائل التواصل** تحمل روابط غير آمنة.

كيف تحمي نفسك ومؤسستك؟

١. **استخدم كلمات مرور قوية** تحتوي على رموز وأرقام وحروف متنوعة.
٢. **فعّل المصادقة الثنائية.(Two-Factor Authentication)**
٣. **تجنب فتح الروابط أو المرفقات المجهولة.**
٤. **حدّث برامجك وأنظمتك بشكل دوري.**
٥. **استخدم برامج مضادة للفيروسات وجدران حماية.**
٦. **لا تستخدم شبكات Wi-Fi عامة في العمليات الحساسة.**
٧. **احذر من مشاركة المعلومات الشخصية عبر الإنترنت.**

في حال التعرض لهجوم:

- لا تتخذ إجراءً عشوائيًا.
- قم **بفصل الجهاز عن الإنترنت فورًا.**
- أبلغ **قسم تقنية المعلومات أو الأمن السيبراني** في مؤسستك.
- لا تحذف أو تعدل أي ملفات قبل التحقيق الفني.

تذكّر:

الأمن السيبراني **مسؤولية الجميع**، وليس مسؤولية قسم التقنية فقط.
الوعي هو خط الدفاع الأول ضد الهجمات الإلكترونية.