أصبح الأمن السيبراني في العصر الرقمي أمراً بالغ الأهمية. ومع تزايد التهديدات السيبرانية، أصبح الحفاظ على سلامة المعلومات والأنظمة شيئاً ضرورياً للغاية. إلا أن الأمن السيبراني لا يعتبر مجرد قضية تقنية، بل يعتمد بشكل كبير على العامل البشري.

فالأمن السيبراني هو مجموعة من المبادئ والممارسات التي تهدف إلى حماية المعلومات والأنظمة من التلاعب أو التدخل أو السرقة أو التدمير من قبل جهات خارجية غير مشروعة. ويؤثر على جوانب كثيرة من حياتنا، سواءً كان ذلك في المجال الشخصي أو المهني أو الاجتماعي. ففقدان البيانات أو التعرض لهجمات سيبرانية يمكن أن يتسبب في خسائر مالية هائلة، ويؤثر على سمعة الشركات والمؤسسات (1) حكومية كانت أم خاصة ويضعف الثقة التي تمتلكها من قبل العملاء والشركاء التجاريين. كما يمكن أن يهدد خصوصية وأمن وحقوق الأفراد.

وللتهديدات السيبرانية أوجه عدة، تزداد مع ازدياد التطور التكنولوجي، وتجعل التحديات بالحفاظ على فضاء سيبراني آمن مهمة أكثر تعقيداً. وبالإضافة إلى التهديدات المتعارف عليها من فيروسات وبرامج فدية ورسائل احتيالية، هناك تقنيات الهندسة الاجتماعية التي تستخدم للوصول الى المعلومات المتوخاة من قبل مجرمي الإنترنت. وقد انتشرت تقنية التزييف العميق مؤخراً لتكون الأداة الجديدة لتحقيق أهدافهم وإلحاق الضرر بالجهات المعرضة للاستهداف.

فالتهديدات السيبرانية هي محاولات غير مشروعة للاستيلاء على المعلومات أو التأثير على سلوك المستخدمين أو إتلاف الأنظمة. وفقاً لتقديرات حديثة، من المتوقع أن يصل تأثير جرائم الإنترنت إلى 10 تريليون دولار هذا العام (2)، متجاوزاً إجمالي الناتج المحلي لجميع دول العالم باستثناء الولايات المتحدة والصين. ويرجع هذا إلى زيادة التهديدات السيبرانية وزيادة استخدام التكنولوجيا.

كيف يمكننا حماية أنفسنا من التهديدات السيبرانية؟

الحماية من التهديدات السيبرانية تبدأ بالتوعية بالأمان. فالعامل البشري هو الضعف الأكبر في سلسلة الأمان. وفقا لأحدث الإحصائيات، يتسبب الخطأ البشري في أكثر من 90% من هجمات الأمن السيبراني (3). هذا يعني أن معظم هذه الهجمات يمكن تجنبها من خلال تحسين التوعية بالأمان وتعزيز الممارسات الجيدة.

إليك بعض النصائح لتحسين التوعية بالأمان:

البقاء على اطلاع لأخر التطورات والتهديدات في مجال الأمن السيبراني، واتباع نصائح وإرشادات المصادر الموثوقة.

استخدام كلمات مرور طويلة ومعقدة وفريدة لكل حساب، وعدم استخدام نفس كلمة المرور لأكثر من حساب، وكذلك عدم مشاركة كلمات المرور، وتغييرها بشكل دوري.

استخدام التحقق ثنائي المصدر والتي تطلب إدخال رمز إضافي بجانب كلمة المرور عند تسجيل الدخول، عبر إرسال الرمز إلى البريد الإلكتروني أو رقم الهاتف.

الحفاظ على تحديث برامج مضادة للفيروسات، وفحص الجهاز بشكل دورى للتأكد من خلوه من أي برامج ضارة.

الحذر من رسائل البريد الإلكتروني غير المعروفة أو غير موثوقة المصدر، وعدم إدخال معلومات شخصية أو مالية في صفحات وهمية.

إذاً، في عصر التكنولوجيا، يبقى الأمان الإلكتروني ضرورياً. وبينما يقدِّم التطور التكنولوجى دوراً كبيراً في حماية المؤسسات، فإن التوعية بالأخطار الإلكترونية يُعتبر العنصر الأساسي للحفاظ على سلامة المعلومات والأنظمة. بالعمل معاً لتعزيز هذا الوعي، يمكننا تقليل مخاطر الإختراقات الإلكترونية والحفاظ على أمان عالمنا الرقمي.

المصادر

- Human Error Drives Most Cyber Incidents. Could AI Help? (hbr.org)
- Human Error Drives Most Cyber Incidents. Could AI Help? (hbr.org)
- More than 90% of cyberattacks are made possible by human error (techxplore.com)

الكاتب: رامي الأحمدية