



الأمن السيبراني

الأمن السيبراني:

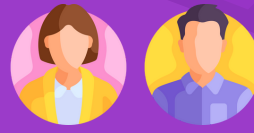
هو فرع من فروع علوم الحاسب الآلي الذي يهتم بابتكار أساليب مطورة ومعقدة من أجل حماية الأجهزة والشبكات والبيانات المتصلة بشبكة الأنترنت من سوء الاستخدام التقني والوصول الغير مصرح به لهذه الأجهزة.

أهمية الأمن السيبراني:



المجتمع:

تحقيقًا لرؤية 2030 وتخريج كادر متمكن ومتخصص من علوم الأمن السيبراني والتحري الرقمي.



الأفراد:

تكمّن أهمية التوعية بالأمن السيبراني في تمكين الفرد من حماية أجهزته وبياناته المرتبطة بشبكة الأنترنت ومعرفة الإجراءات المتبعة عند اكتشاف أي ثغرة أو حدوث انتحال للهوية الشخصية أو سرقة البيانات.

تهديدات الأمن السيبراني:



برامج الفدية الضارة:

هي نوع من البرامج الضارة يستخدمها المخترقين بهدف إبتزاز المال عن طريق عدم السماح للوصول إلى الملفات أو نظام الكمبيوتر حتى يتم دفع الفدية. دفع الفدية لا يضمن للشخص استعادة نظامه وملفاته.



تصيد المعلومات:

هو عملية إرسال رسائل احتيالية والإدعاء بأنها من جهة رسمية موثوقة والهدف منها سرقة معلومات حساسة مثل أرقام بطاقات الائتمان أو بيانات تسجيل الدخول كإسم المستخدم وكلمة المرور وهو أكثر أنواع الهجمات الإلكترونية شيوعًا.



الهندسة الاجتماعية:

هي أسلوب يستخدمه المقرصنين لاستدراجك للكشف عن معلوماتك وبياناتك الحساسة، مثل: طلب الحصول على دفع نقدي أو الوصول إلى بياناتك السرية عن طريق إدخالها أو النقر على الروابط أو تنزيل البرامج الضارة أو الوثوق بمصدر ضار.



البرامج الضارة:

هي نوع من البرامج تسمح للمقرصنين بالوصول الغير مصرح به إلى جهاز الحاسوب أو إلحاق الضرر به وتخريبه.

كيفية الحماية من المخاطر على الأنترنت:

يجب توخي الحذر عند اختيار اسم المستخدم وذلك بأن لا يتضمن معلومات شخصية: مثل الاسم الشخصي ورقم الهوية وتاريخ الميلاد ومكان الإقامة... إلخ.

تجنب استخدام كلمة مرور موحدة لجميع حساباتك الشخصية على شبكة الإنترنت مما يعطي للمخترقين فرصة الوصول إلى حساباتك بسهولة.

استخدام القياسات الحيوية في إجراءات تسجيل الدخول إلى الحسابات الشخصية أو الهاتف المحمول مثل بصمة الاصبع وشبكية العين وخاصية التعرف على الوجوه أو الأصوات.

تفعيل تنبيهات تسجيل الدخول عند محاولة شخص تسجيل الدخول على حسابي الشخصي.

تثبيت برامج مكافحة الفيروسات وجدار الحماية ووضع PIN كإجراء عند فتح الهاتف المحمول.

