



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER



ما هو الأمن السيبراني؟

هو عملية حماية الأنظمة والاتصالات والشبكات والبيانات الموجودة على شبكة الإنترنت ضد التهديدات والمخاطر السيبرانية الناتجة عن الهجمات السيبرانية والأفعال المتمثلة في ارتكاب الجريمة الإلكترونية التي تضر الهياكل والبنى التحتية الحيوية والمؤسسات والأفراد.

ما هو الفضاء السيبراني أو السايبر؟

هو عالم الحاسب الآلي الافتراضي، حيث تتلقي فيه جميع شبكات الحاسب الآلي والاتصالات الرقمية والبيانات الناشئة عن تلك الاتصالات عبر الشبكة العنكبوتية العالمية "الإنترنت".

خطورة الإفصاح المفرط



إلغاء

ما الفرق بين المعلومات الشخصية والخاصة؟

المعلومات الشخصية هي المعلومات التي لا يمكن استخدامها لتحديد هويتك مثل: سنة الميلاد فقط أو العمر والطعام المفضل والاسم الأول فقط.

أما **المعلومات الخاصة** فهي جميع التفاصيل التي ينبغي أن تظل سرية والتي يمكن استخدامها لسرقة الهوية والتصيد والاحتيال الإلكتروني.

أمثلة على المعلومات الخاصة:

- الاسم الكامل
- العنوان والموقع
- رقم الهاتف الخاص
- تاريخ الميلاد الكامل
- موقع المدرسة
- كلمات المرور أو رموز التحقق

إليك بعض التساؤلات التي تساعدك في تحديد المحتوى الذي يمكنك نشره ومشاركته مع الآخرين (النشر عبر وسائل التواصل الاجتماعي أو ألعاب الكمبيوتر أو المنتديات):

هل تقوم بمشاركة شيء قد يسمح لشخص لا تعرفه بالتعرف عليك والحصول على معلوماتك الشخصية؟

• هل تقوم بالتحقق من إعدادات الخصوصية في التطبيقات لمعرفة ما تسمح بمشاركته مع الأشخاص وما تتم المشاركة به تلقائيًا مع التطبيق؟

فكر في ترك بصمة رقمية إيجابية وتذكر أن الأشياء التي تشاركها عبر الإنترنت يمكن أن تظل موجودة إلى الأبد.

فكر جيدًا قبل الضغط على زر "النشر" أو "المشاركة"



لمزيد من المعلومات
امسح هنا

#الوعي_السيبراني
www.ncsc.gov.bh



إرشادات السلامة لاستخدام الإنترنت عند السفر

تأكد من تعطيل خاصية الاتصال التلقائي بشبكات الإنترنت .



احذر عند الاتصال بشبكة الإنترنت اللاسلكية "الواي فاي" العامة في الفنادق أو المطارات والمقاهي العامة، واجعل أولوية استخدام الـ Wi-Fi المجاني للتحقق من المعلومات الخاصة برحلتك والعثور على الاتجاهات لوجهتك لحماية خصوصيتك.



إذا كنت متصلاً بشبكة عامة، فتأكد من استخدام مواقع "https" فقط وتجنب التسوق عبر الإنترنت أو الوصول إلى أي بيانات حساسة لتجنب حدوث أي اختراق أمني.



تأكد من القيام بالنسخ الاحتياطي لأجهزتك قبل أن ترافقك في سفرك، وحدّث أجهزتك بشكل دوري أو فعّل التحديث التلقائي.



يفضل أن تخصص بطاقة واحدة للتسوق عبر الإنترنت أو استخدام بطاقة مسبقة الدفع.



لا تشارك معلومات بطاقتك الائتمانية عبر القنوات غير الآمنة، مثل: وسائل التواصل الاجتماعي.



راجع كشوفات حسابك بصفة دورية وقدم شكوى لمؤسستك المالية فوراً حال ارتياك من أي عملية شراء.



احذر عند مشاركة معلوماتك البنكية عند التسوق أونلاين وتأكد من تفعيل خاصية المصادقة الثنائية.



تأكد من أن الموقع الإلكتروني الذي تزوره موثوق. يحتاج المحتالون إلى تغيير حرف واحد للحصول على URL مختلف رغم أنه قد يكون مشابهاً للعنوان الأصلي، وهذا ما يسمى بالتصيد والاحتيال الإلكتروني.