المركز الوطني
للأمن السيبراني
National Cyber
Security Center

ما هو الأمن السيبراني؟

المحـــاور

- الأمن السيبراني
  - تعريف الأمن السيبراني
  - الركائز الأساسية للأمن السيبراني
  - الأمن السيبراني والمملكة الأردنية الهاشمية
- المخاطر السيبرانية
  - تعريف الهجمات السيبرانية
  - أهداف الهجمات السيبرانية
- دور المستخدم في تعزيز الأمن السيبراني
  - المفاهيم الخاطئة للأمن السيبراني ومخاطرها
  - مسؤولية المستخدم في الحماية من المخاطر السيبرانية
  - بعض سياسات الأمن السيبراني
- التعامل مع مخاطر الأمن السيبراني
  - التعامل مع المخاطر والتهديدات السيبرانية
  - أدوات الإبلاغ عن الجرائم السيبرانية

- الأمن السيبراني

  - تعريف الأمن السيبراني
  - الركائز الأساسية للأمن السيبراني
  - الأمن السيبراني والمملكة الأردنية الهاشمية

تعريف الأمن السيبراني

"يشير الأمن السيبراني إلى الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية و البنى التحتية الحرجة من الاختراقات و القدرة على استعادة عملها و استمراريتها، سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إلى ذلك"*

* *وفقاً لقانون الأمن السيبراني الأردني*

الركائز الأساسية للأمن السيبراني

يهدف الأمن السيبراني إلى الحفاظ على ثلاث ركائز أساسية وهي:

- **سرية المعلومات**
ضمان عدم الوصول إلى البيانات إلا من قبل الأطراف المصرح لهم فقط

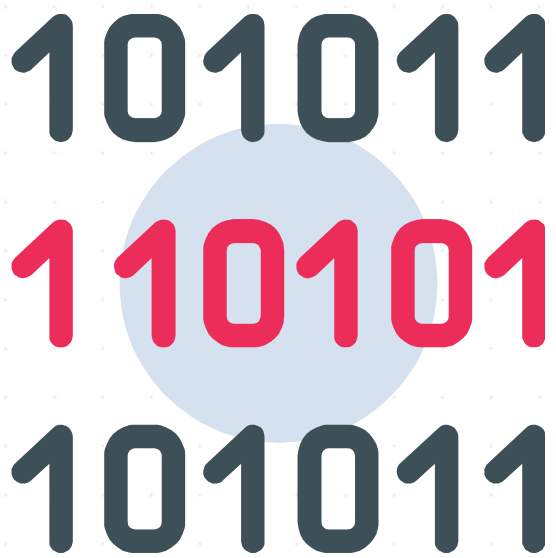
- **سلامة المعلومات**
ضمان عدم القدرة على تعديل البيانات إلا من قبل المستخدمين المصرح لهم فقط

- **الاستمرارية**
ضمان إتاحة البيانات عند الحاجة إليها في أي وقت من قبل المستخدمين المصرح لهم

الأمن السيبراني والمملكة الأردنية الهاشمية

قامت الإدارة الملكية السامية بالموافقة على إنشاء:

- قانون الأمن السيبراني الأردني
- المجلس الوطني للأمن السيبراني
- المركز الوطني للأمن السيبراني
- الاستراتيجية الوطنية للأمن السيبراني
- سياسة أمن المعلومات للبنك المركزي الأردني



- المخاطر السيبرانية

  - تعريف الهجمات السيبرانية
  - أهداف الهجمات السيبرانية

تعريف الهجمات السيبرانية

تُعرف الهجمات السيبرانية بأنها أي محاولة ضارة ومتعمدة لانتهاك أحد ركائز الأمن السيبراني (سرية - سلامة - استمرارية) المعلومات.

- **سرية المعلومات**

إفشاء المعلومات و وصول غير المصرح للمعلومات أو الأنظمة أو الشبكات.

- **سلامة المعلومات**

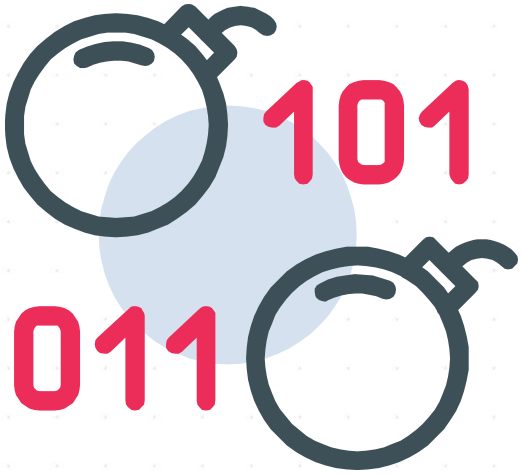
العبث بسلامة المعلومات أو مصدرها و تغييرها من قبل أشخاص غير مصرح لهم بذلك.

- **الاستمرارية**

تعطيل الأنظمة و منع الوصول إلى المعلومات عند الحاجة إليها.

أهداف الهجمات السيبرانية

هناك عدة أهداف للهجمات السيبرانية منها:



- **أهداف سياسية:** الحروب السيبرانية - التجسس السيبراني - تهديد الأمن القومي والعسكري
- **أهداف اقتصادية:** تحقيق أرباح ومكاسب مادية - الإضرار بالسمعة لحصول خسارة مالية - الاستيلاء على المعلومات والاتجار فيها
- **أهداف تخريبية:** تدمير الأنظمة والبنى التحتية
- **أهداف شخصية:** الانتقام - انتحال الشخصية - زعزعة ثقة المنافسين

- دور المستخدم في تعزيز الأمن السيبراني

  - المفاهيم الخاطئة للأمن السيبراني ومخاطرها
  - مسؤولية المستخدم في الحماية من المخاطر السيبرانية
  - بعض سياسات الأمن السيبراني

المفاهيم الخاطئة للأمن السيبراني ومخاطرها

المفاهيم الخاطئة:

- أمن المعلومات وحماية البيانات هو مسؤولية قسم تكنولوجيا المعلومات فقط.
- الهجمات الإلكترونية لا يسببها إلا جهات خارجية.
- برامج مكافحة الفيروسات والبرامج الضارة كافية للتأمين من المخاطر السيبرانية.
- إن لم تتعرض لهجوم سابق فأنت لست بحاجة إلى الأمن السيبراني.
- اعتقاد المستخدم بأنه من غير المحتمل أن يشهد اختراقاً إلكترونياً.

المخاطر السيبرانية:

- تُعتبر الأخطاء البشرية هي أكبر ثغرة يعاني منها أمن المعلومات.
- تُعتبر التهديدات الداخلية خطيرة بنفس قدر خطورة التهديدات الخارجية، وقد تبدأ من شخص تعرفه.
- برامج مكافحة الفيروسات والبرامج الضارة لن تحمي البنية التحتية لتكنولوجيا المعلومات بالكامل من جميع المخاطر السيبرانية.
- لا يُعد عدم تعرضك لهجوم سيبراني سابقاً مؤشراً لقوة موقفك الأمني الحالي.

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  1. البرمجيات الخبيثة

البرمجيات الخبيثة

- **الفيروسات**

عادةً ما تأتي كمرفق أو مستند في رسالة بريد إلكتروني يحتوي على فيروسات ، وعند فتح الملف ، يتم تنشيط الفيروس ثم يتكاثر بنفسه لنشر العدوى داخل جهاز كمبيوتر الضحية.

- **برامج الفدية**

برامج ضارة تقوم بالوصول إلى الملفات والبيانات الحساسة و تشفيرها وجعلها غير قابلة للوصول من قبل المستخدمين، ثم تطالب بدفع تعويض مالي مقابل البيانات حتى يتم إعادتها.

- **الديدان**

أخطر أنواع البرمجيات الخبيثة، تصيب الجهاز عبر ملف تم تنزيله أو الاتصال شبكة ما ولا يتطلب من الضحية تنشيطه ، ثم يتكرر بسرعة وينتشر إلى أي جهاز داخل الشبكة.

- **أحصنة طروادة**

برنامج يبدو مشروعاً و لكنه في الواقع برنامج خبيث يضر البيانات في الكمبيوتر و يسرق المعلومات الحساسة.

البرمجيات الخبيثة

- **برامج التخويف**

تستخدم الهندسة الاجتماعية للتلاعب بالمستخدمين و إقناعهم بشراء أو تنزيل برامج ضارة أو غير مرغوب فيها.

- **برنامج التجسس**

برنامج ضار يراقب سلوكيات المستخدمين ويسجلها و يرسلها إلى المهاجم.

- **برامج الإعلانات المتسللة**

تُستخدم لجمع البيانات حول مستخدم الكمبيوتر وتقوم بتقديم الإعلانات تلقائيًا لتوليد إيرادات لطرف ثالث.

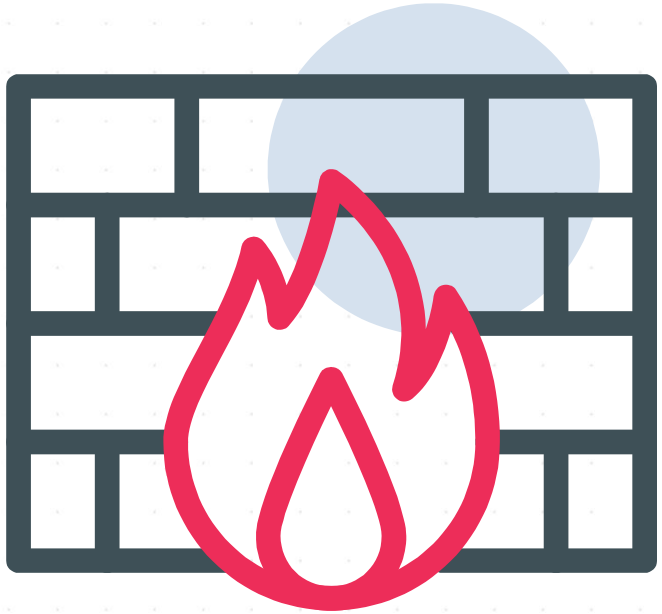
البرمجيات الخبيثة

طرق انتشار البرامج الخبيثة:

- الوسائط القابلة للإزالة
- مواقع الويب غير الموثوقة
- مرفقات البريد الإلكتروني
- مواقع التواصل الاجتماعي
- البرامج و التطبيقات غير الموثوقة

البرمجيات الخبيثة

طرق الحماية من البرمجيات الخبيثة:



- قم بتنشيط جدار الحماية
- حدد قوائم التحكم في الوصول لإنشاء منطقة عازلة بين الشبكة و الانترنت (قيّد الوصول باستخدام إعداد القائمة للمصرح لهم و ليس بإدراج عناوين أو خدمات معينة في القائمة السوداء)
- استخدم برامج مكافحة الفيروسات و الحماية من برامج التجسس
- قم بتفعيل خاصية "التحديث التلقائي" لجميع البرامج المثبتة على جهازك

البرمجيات الخبيثة

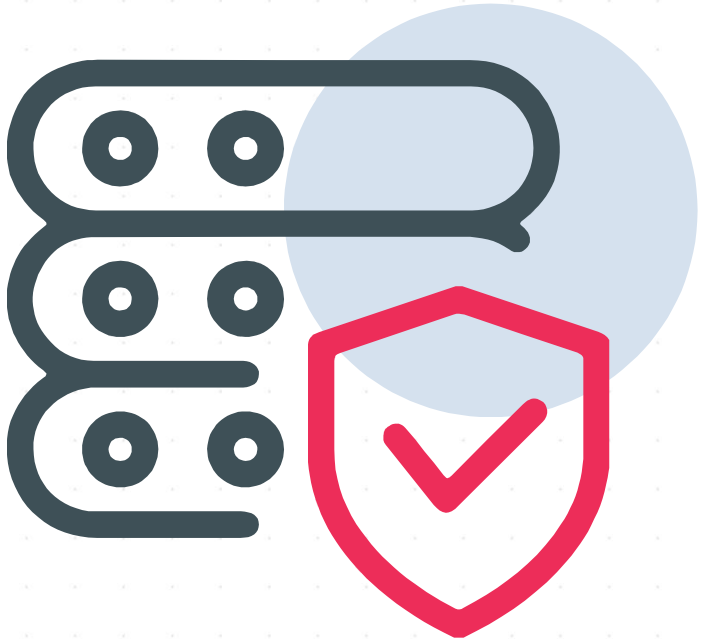
طرق الحماية من البرمجيات الخبيثة:

- احرص على تثبيت البرامج المسموح بها فقط في المركز الوطني للأمن السيبراني و تجنب نهائياً تنزيل أي برامج دون إذن مسبق من الإدارة المعنية بذلك
- احتفظ بسجلات الأنشطة التي يتم إنشاؤها بواسطة أجهزة و برامج الحماية
- احم سجلات الأنشطة بالتشفير و بكلمات المرور
- تجنب استخدام الوسائط القابلة للإزالة دون إذن مسبق من الإدارة المعنية بذلك
- قم بإعداد عوامل تصفية البريد العشوائي للبريد الإلكتروني الخاص بك

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  - 2. حماية البيانات

حماية البيانات



أهداف حماية البيانات:

- استخدام البيانات للأغراض المذكورة فقط
- عدم تخزين البيانات لفترة أطول من اللازم
- استخدام البيانات بشكل مناسب
- عدم مشاركة الشركات بيانات العملاء والعاملين والموردين مع أطراف غير مصرح لها

حماية البيانات

أفضل الممارسات العامة لحماية البيانات و المعلومات

- قم بإنشاء نسخ احتياطية منتظمة من بياناتك المهمة و احرص على تخزينها بشكل آمن
- تأكد من أن الجهاز الذي يحتوي على النسخ الاحتياطية غير متصل بالجهاز الذي يحتوي على النسخ الأصلية
- احرص على تثبيت واقيات أجهزة الحماية من التغير المفاجئ في شدة التيار الكهربائي و تأكد من توصيل جميع الأجهزة المهمة بمصادر طاقة غير منقطعة

حماية البيانات

أفضل الممارسات العامة لحماية البيانات و المعلومات

- قم بتشفير أو وضع كلمات مرور لحماية الملفات و الأجهزة التي تتضمن بيانات شخصية أو معلومات حساسة
- اختر طريقة آمنة للتخلص من البيانات فور أن تنتفي الحاجة إليها
- احرص على إعداد اتفاق مكتوب قبل مشاركة أي بيانات مع أي طرف آخر خارج المركز بعد مشاركة البيانات و التعهد بحمايتها والالتزام بالسياسات المطبقة في المركز.
- عند إرسال بيانات حساسة، لا تتصل بنقاط اتصال WiFi عامة

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

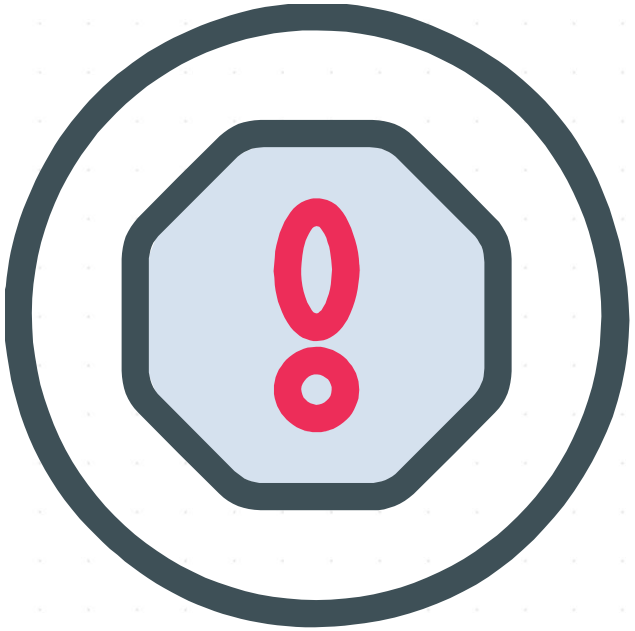
  - 3. الحفاظ على سلامة الأجهزة

الحفاظ على سلامة الأجهزة

أفضل الممارسات العامة للحفاظ على سلامة الأجهزة:

- قم بتشغيل حماية رقم التعريف الشخصي و كلمات المرور للأجهزة المحمولة
- قم بضبط إعدادات الأجهزة بحيث يمكن تتبعها أو محو محتواها عن بُعد عند فقدها أو سرقتها
- اعمل على إبقاء أجهزتك محدثة
- استبدل الأجهزة التي لم تعد جهات التصنيع تقوم بدعمها بأجهزة حديثة

الحفاظ على سلامة الأجهزة



أفضل الممارسات العامة للحفاظ على سلامة الأجهزة:

إجراءات الإبلاغ عن المعدات المفقودة أو المسروقة داخل المركز الوطني للأمن السيبراني:

يتم الإبلاغ عن أي هجوم إلكتروني أو محاولة اختراق أو احتيال عبر الرابط التالي:
https://ncsc.jo/?v=1&lang=ar#!/Report?ReportID=1

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  4. كلمات المرور

كلمات المرور

معايير كلمات المرور:

- يجب أن تتضمّن كلمة المرور (8) أحرف على الأقل
- يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

✓ أحرف كبيرة (Upper Case Letters)
✓ أحرف صغيرة (Lower Case Letters)
✓ أرقام (1235)
✓ رموز خاصّة (@*%#)

المدة التي يستغرقها المتسللون لاختراق كلمة المرور الخاصة بك

عدد الأحرف	أرقام فقط	حروف صغيرة فقط	حروف كبيرة و صغيرة	أرقام، أحرف كبيرة و صغيرة	أرقام، أحرف كبيرة و صغيرة، و رموز
4	لحظياً	لحظياً	لحظياً	لحظياً	لحظياً
5	لحظياً	لحظياً	لحظياً	لحظياً	لحظياً
6	لحظياً	لحظياً	لحظياً	ثانية واحدة	5ثوان
7	لحظياً	لحظياً	25ثانية	دقيقة واحدة	6دقائق
8	لحظياً	5ثوان	22دقيقة	ساعة واحدة	8ساعات
9	لحظياً	دقيقتان	19ساعة	3أيام	3أسابيع
10	لحظياً	58دقيقة	5أعوام	7أشهر	شهر واحد
11	ثانيتان	يوم واحد	400عام	41عام	5أعوام
12	25ثانية	3أسابيع	34عام	الفين عام	300عام
13	4دقائق	عام	2مليون عام	100ألف عام	16ألف عام
14	41دقيقة	51عام	200مليون عام	9مليون عام	800ألف عام
15	6ساعات	ألف عام	12بليون عام	600مليون عام	43مليون عام
16	يومان	34ألف عام	1تريليون عام	37بليون عام	2بليون عام
17	4أسابيع	800ألف عام	93تريليون عام	2تريليون عام	100بليون عام
18	9أشهر	23مليون عام	7كوادرليون عام	100تريليون عام	6تريليون عام

كلمات المرور

أفضل الممارسات العامة عند استخدام كلمات المرور:

- تأكد من أن جميع أجهزتك تتطلب كلمة المرور لبدء التشغيل
- استخدم كلمات مرور قوية و تجنب الكلمات الشائعة و المتوقعة و المعرفات الشخصية
- استخدم المصادقة الثنائية حيثما أمكن
- غير كلمات المرور الافتراضية الصادرة من الشركات المصنعة
- احرص على تغيير كلمة المرور بشكل دوريّ

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  - 5. تأمين شبكات الإنترنت

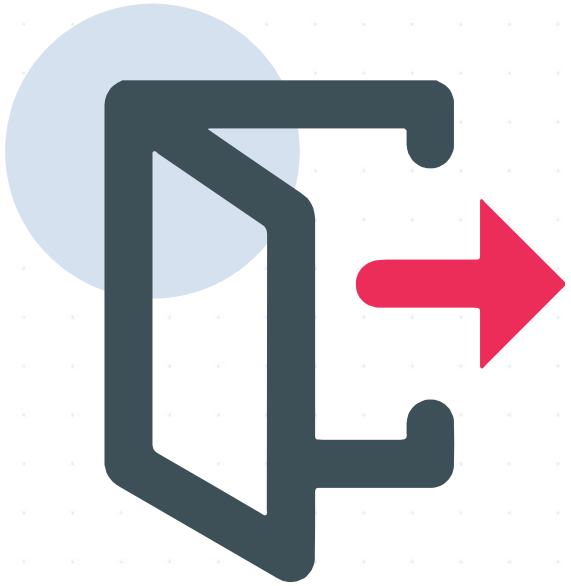
تأمين شبكات الإنترنت

أفضل الممارسات العامة لتأمين شبكات الإنترنت:

- تأكد من أن شبكة ال WiFi آمنة ومشفرة باستخدام WPA2
- قم بوضع كلمة مرور آمنة و قوية على أجهزة التوجيه
- احرص على تحديث كلمات مرور أجهزة التوجيه باستمرار
- قم بتغيير كلمات المرور الافتراضية لأجهزة التوجيه
- عطِّل أي خاصية إدارة عن بُعد لأجهزة التوجيه

تأمين شبكات الإنترنت

أفضل الممارسات العامة لتأمين شبكات الإنترنت:

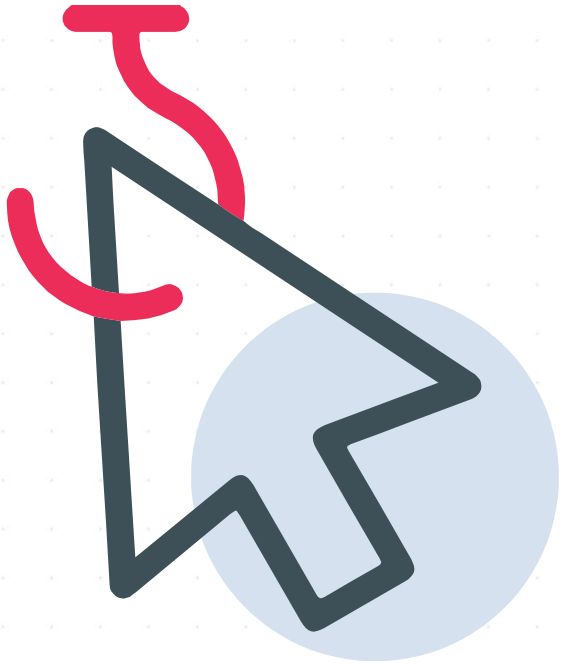


- حدد الوصول إلى شبكة الـ WiFi فقط عن طريق السماح للأجهزة ذات العناوين المعنية بالتحكم في الوصول إلى الوسائط
- قم بتمكين بروتوكول التكوين الديناميكي للمضيف DHCP على أجهزة الشبكة للسماح بتتبع جميع الأجهزة التي قامت بالاتصال بالشبكة
- قم بتسجيل الخروج كمسؤول بعد الإنتهاء من ضبط إعدادات جهاز التوجيه
- احرص على تحديث برنامج جهاز التوجيه باستمرار

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  - 6. تجنب هجمات التصيد الاحتيالي

تجنب هجمات التصيد الاحتيالي



مفهوم مواقع التصيد:

هي مواقع وهمية غير حقيقية تشبه في شكلها مواقع شرعية، تم تصميمها للحصول على بيانات الضحية مثل اسم المستخدم وكلمة المرور الخاصة به.

تجنب هجمات التصيد الاحتيالي

أفضل الممارسات السيبرانية لتجنب هجمات التصيد الاحتيالي:

- تأكد من عدم تصفح الويب أو التحقق من رسائل البريد الإلكتروني على الخوادم أو من حسابات ذات امتياز المسؤول
- قم بتفعيل عوامل تصفية الويب و البريد الإلكتروني
- فكر في حظر المواقع الإلكترونية المرتبطة عادة بتهديدات الأمن السيبراني
- ابحث عن علامات التصيد الواضحة مثل الأخطاء الإملائية و النحوية و الشعارات ذات الجودة المنخفضة.
- احرص على إجراء فحص دوري لأجهزتك بحثاً عن البرامج الضارة
- إذا كنت تشك في حدوث هجوم، غير كلمات المرور الخاصة بك فوراً و قم بالإبلاغ عن رسائل التصيد عبر الرابط التالي:
https://ncsc.jo/?v=1&lang=ar#!/Report?ReportID=1

تجنب هجمات التصيد الاحتيالي

أفضل الممارسات السيبرانية لتجنب هجمات التصيد الاحتيالي:

- لا تفتح مرفقات البريد الإلكتروني على الفور ولا تنقر على رابط في رسائل البريد الإلكتروني مشبوها فيه أو غير مرغوب به، توقف ، فكر، انقر.
- احذر عند اتصال شخص ما بك على نحو غير متوقع عبر الانترنت أو الهاتف و طلب معلومات شخصية
- قلل مشاركة المعلومات الشخصية عبر البريد الإلكتروني حتى عند الاتصال بالعناوين المعروفة
- تحقق من صحة رسائل البريد الإلكتروني قبل تقديم المعلومات الشخصية

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  - 7. التصفح الآمن للإنترنت

التصفح الآمن للإنترنت

أفضل الممارسات السيبرانية للتصفح الآمن للإنترنت:

- احرص على إعادة توجيه جميع حركات مرور Http إلى Https و تأكد من وجود علاقة القفل
- قم بتمكين تثبيت المفتاح العام على المواقع المتصفحة لمنع الهجوم الوسيط
- تجنب إدخال معلومات شخصية في المواقع غير الموثوقة
- قم بتعطيل البرامج النصية مثل جافا سكريبت في المتصفح بشكل افتراضي
- أغلق المتصفح بعد الانتهاء لضمان عدم تخزين المعلومات الحساسة في ذاكرة التخزين المؤقت
- استخدم النسخ الأحدث من المتصفح
- استخدم برامج مكافحة الفيروسات
- قم بمسح ملفات تعريف الارتباط للمواقع
- استخدم متصفح انترنت آمن

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  8. النسخ الاحتياطي للبيانات

النسخ الاحتياطي للبيانات

أفضل الممارسات السيبرانية عند النسخ الاحتياطي:

- استخدم أنظمة النسخ الاحتياطي الآمنة التي يتم تحديثها بشكل منتظم
- في حالة استخدام وسائط التخزين القابلة للإزالة، أفصل هذه الأجهزة فعلياً عن أجهزة الكمبيوتر المتصلة بالشبكة بعد استكمال إنشاء النسخ الاحتياطية
- أنشئ نسخ للقراءة فقط للرجوع إليها عند التعافي من الكوارث في أسوأ الحالات
- ضع سيناريوهات لتقييم المدة التي سيستغرقها استرداد البيانات المهمة

- مسؤولية المستخدم في الحماية من المخاطر السيبرانية

  - 9. تجنب هجمات الهندسة الاجتماعية

تجنب هجمات الهندسة الاجتماعية

مفهوم الهندسة الإجتماعية:

فن التلاعب و خداع الناس لجعلهم ينفذون إجراءات تؤدي إلى اختراق البيانات السرية و منح حق الوصول إلى معلومات شخصية حساسة

تجنب هجمات الهندسة الاجتماعية

خطوات سير المهندس الاجتماعي:

1) جمع المعلومات عن الضحية
2) تطوير العلاقات مع الضحية
3) استغلال الضحية و استدراجها للحصول على المعلومات
4) التنفيذ لتحقيق الهدف

تجنب هجمات الهندسة الاجتماعية

أشهر تقنيات الهندسة الاجتماعية:

- التصيد
- انتحال الشخصيات
- تنصت الكتف
- البحث في هاوية المهملات
- الهجوم من الخلف
- الاستدراج

تجنب هجمات الهندسة الاجتماعية

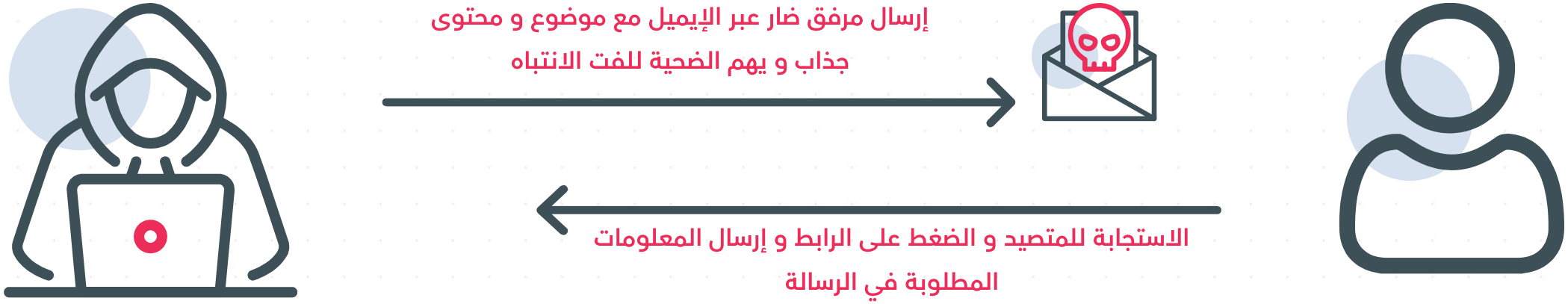
التصيد:

من صور التصيد الاحتيالي: التصيد عبر الهاتف

تجنب هجمات الهندسة الاجتماعية

التصيد:

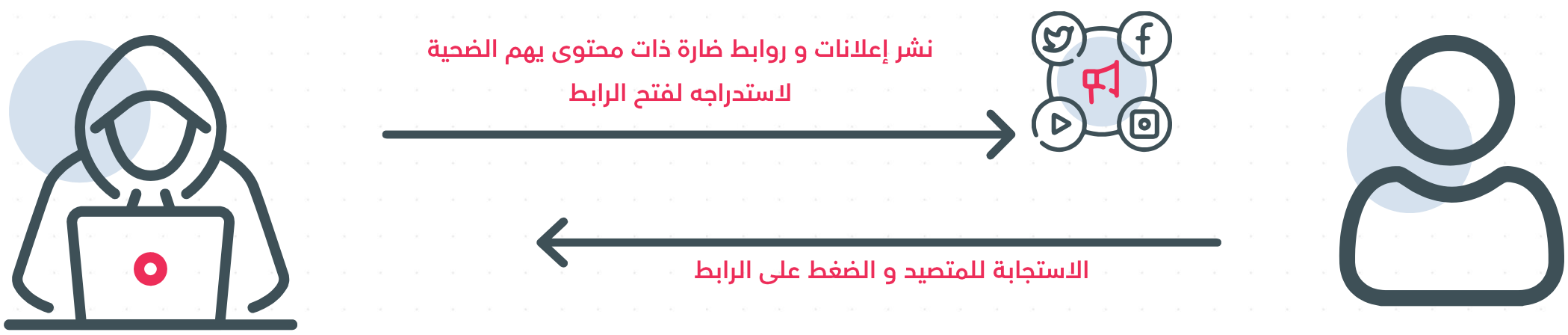
من صور التصيد الاحتيالي: الضغط على روابط البريد الإلكتروني المزيفة



تجنب هجمات الهندسة الاجتماعية

التصيد:

من صور التصيد الاحتيالي: مواقع التواصل الاجتماعي



تجنب هجمات الهندسة الاجتماعية

انتحال الشخصيات:

ينتحل المخترق هوية فرد تعرفه، أو جهة تتعامل معها لخداعك.
من الأمثلة التي قد يرسلها المهاجمون عبر البريد الإلكتروني أو الرسائل النصية:

1. "نحن نشك في وجود معاملة غير مصرح بها في حسابك، لضمان عدم اختراق حسابك يرجى النقر على الرابط أدناه و تأكيد هويتك".
2. أثناء التحقق المنتظم للحسابات، لم نتمكن من التحقق من معلوماتك، الرجاء النقر هنا لتحديث معلوماتك والتحقق منها".

تجنب هجمات الهندسة الاجتماعية

تنصت الكتف:

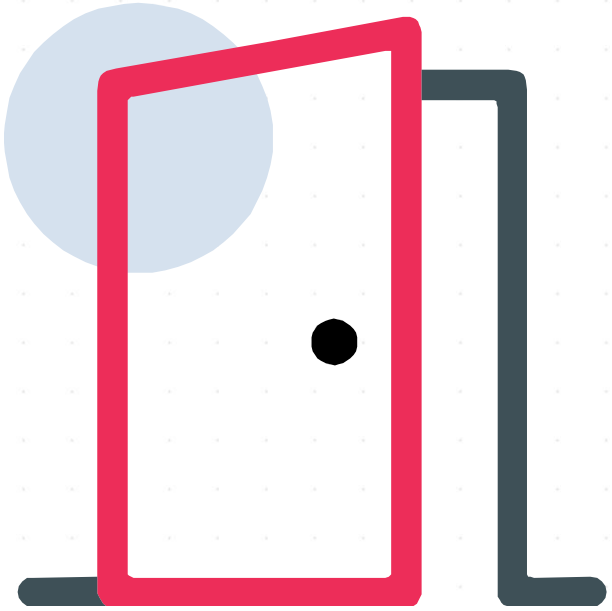
هو مراقبة وثائق تفويض الدخول أو الأرقام السرية لشخص ما من خلال النظر من فوق كتفه أثناء إدخاله تلك البيانات.

تجنب هجمات الهندسة الاجتماعية

البحث في هاوية المهملات:

البحث في الحاويات و سلات المهملات من أجل العثور على أي معلومات مهمة من كلمات مرور أو مذكرات أو عناوين IP أو أي معلومات تفيد المهاجم في تنفيذ هجومه على الضحية.

تجنب هجمات الهندسة الاجتماعية



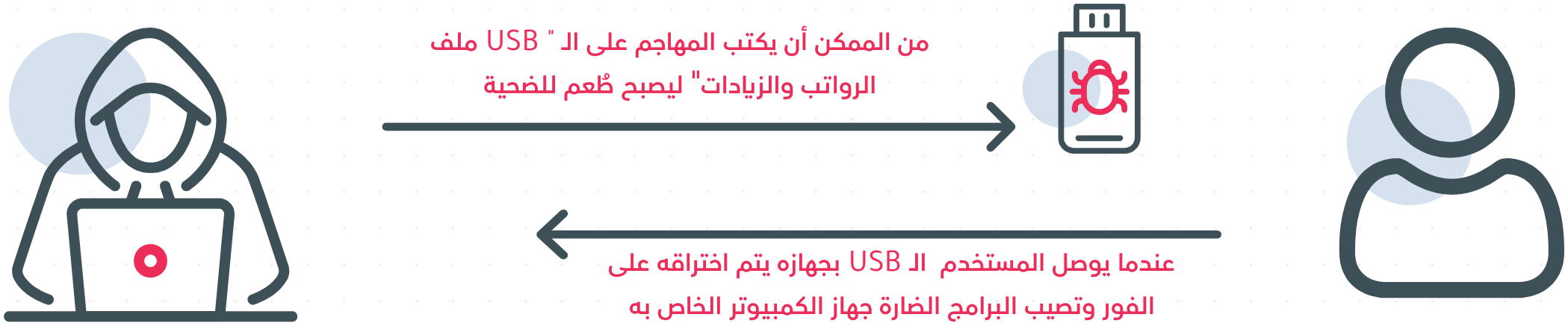
الهجوم من الخلف:

لحاق المهاجم بموظف ما إلى منطقة غير مصرح له الدخول إليها للدخول خلف الموظف قبل غلق الباب أو طلب المساعدة من الموظف لإمساك الباب بسبب إمساكه بكوب قهوة أو ما شابه.

تجنب هجمات الهندسة الاجتماعية

الاستدراج:

هذا النوع من الهجمات يتم عن طريق استخدام أداة تخزين مثل الـ USB كالتالي:



- بعض سياسات الأمن السيبراني
  - سياسة المكتب النظيف

سياسة المكتب النظيف

ما هي سياسة المكتب النظيف؟

سياسة المكتب النظيف هي توجيه يحدد كيف يجب على الموظفين ترك مساحة عملهم عند مغادرة المكتب، و تهدف السياسة إلى ضمان تنظيف مساحات العمل ، و إغلاق المستندات الحساسة أو حفظها بشكل مناسب في نظام الكمبيوتر.

سياسة المكتب النظيف

ما هو الغرض من سياسة المكتب النظيف؟

تُعد سياسة المكتب النظيف بمثابة تذكير يومي للموظفين بأن حماية المعلومات والبيانات السرية تمثل أولوية قصوى للحماية من الانتهاكات الأمنية.

سياسة المكتب النظيف

ما هي فوائد وجود سياسة المكتب النظيف؟

- توفير المال عن طريق تقليل تكلفة الطباعة بعد استخدام النسخ الرقمية من المستندات
- مساحة العمل النظيفة تجعل وزارتك أكثر فاعلية
- يتوافق نهج المكتب النظيف مع مبادئ الخصوصية الأساسية
- تثبيط عيون المتطفلين

سياسة المكتب النظيف

ما هي فوائد وجود سياسة المكتب النظيف؟

- التقليل من مخاطر الخروقات الأمنية وسرقة المعلومات
- يساعد في تطبيق قانون حماية البيانات والحفاظ على أمنها
- يساعد العاملين في المكتب على الاستفادة من مساحة المكتب الفارغة
- الشعور بالتنظيم يقلل من مستويات التوتر لدى العاملين في المكتب

سياسة المكتب النظيف

كيف تحافظ على سياسة المكتب النظيف؟

- لا تترك جهاز الكمبيوتر / أجهزة المحمولة في وضع تسجيل الدخول
- يجب أن يكون جهاز الكمبيوتر الخاص بك محميًا بكلمة مرور
- يجب تفعيل قفل أمان لجهازك بعد ثلاث دقائق من تركه كحد أقصى
- يجب أن يكون قفل أمان جهازك محميًا بكلمة مرور لإعادة فتحه

سياسة المكتب النظيف

كيف تحافظ على سياسة المكتب النظيف؟

- أغلق أجهزتك عندما تغادر نهاية اليوم
- لا ينبغي تعيين شاشة التوقف لأجهزة الكمبيوتر الفردية المكتبية / المحمولة
- يجب تخزين الورق ووسائط الكمبيوتر في خزائن مقفلة مناسبة عندما لا تكون قيد الاستخدام
- يجب مسح المعلومات الحساسة من الطابعات فور طباعتها
- يجب أن يظل مكتب الاستقبال خاليًا قدر الإمكان في جميع الأوقات

سياسة المكتب النظيف

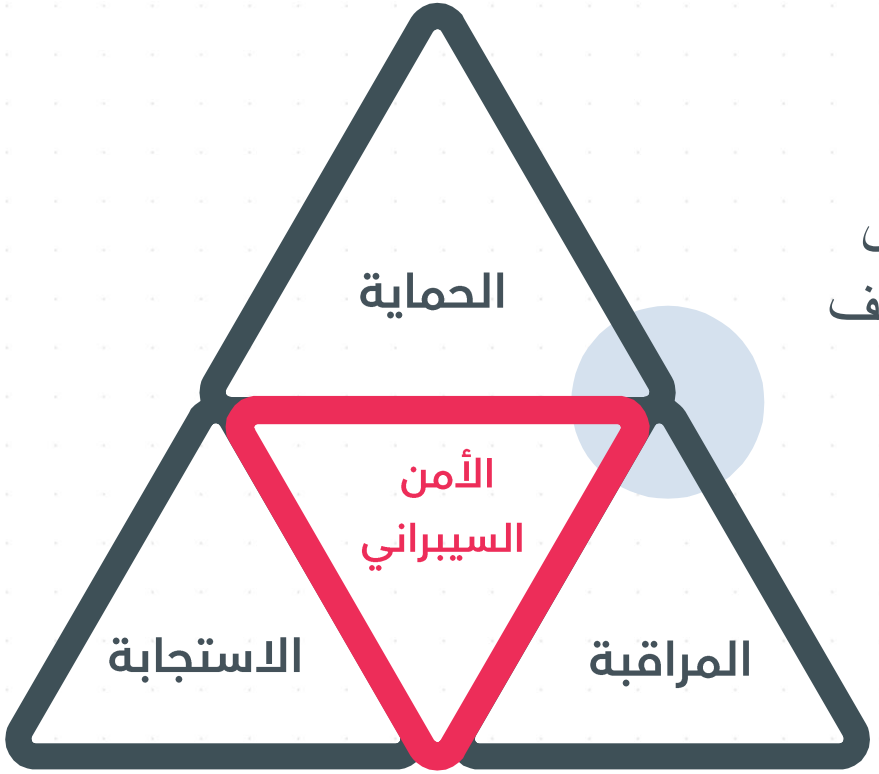
كيف تحافظ على سياسة المكتب النظيف؟

- يجب حفظ المتعلقات الشخصية الفردية في أدراج مقفلة
- تأكد من عدم ترك أي أوراق أو متعلقات على المكتب قبل المغادرة نهاية اليوم
- يجب أن تحتوي أجهزة سطح المكتب على اختصارات فقط وأن لا تحتوي على ملفات أو مجلدات كاملة
- يجب أن تكون شاشات الكمبيوتر بزاوية بعيدة عن أنظار الأشخاص غير المصرح لهم في الغرفة
- يجب أن تظل غرف الخادم / مناطق المكاتب مغلقة عندما لا تكون قيد الاستخدام
- يجب تأمين خزائن الملفات في حالة عدم استخدامها
- يجب عدم نشر كلمات المرور في أي مكان يمكن الوصول إليه
- يجب إزالة نسخ المستندات التي تحتوي على معلومات سرية على الفور

- التعامل مع مخاطر الأمن السيبراني

  - التعامل مع المخاطر والتهديدات السيبرانية
  - أدوات الإبلاغ عن الجرائم السيبرانية

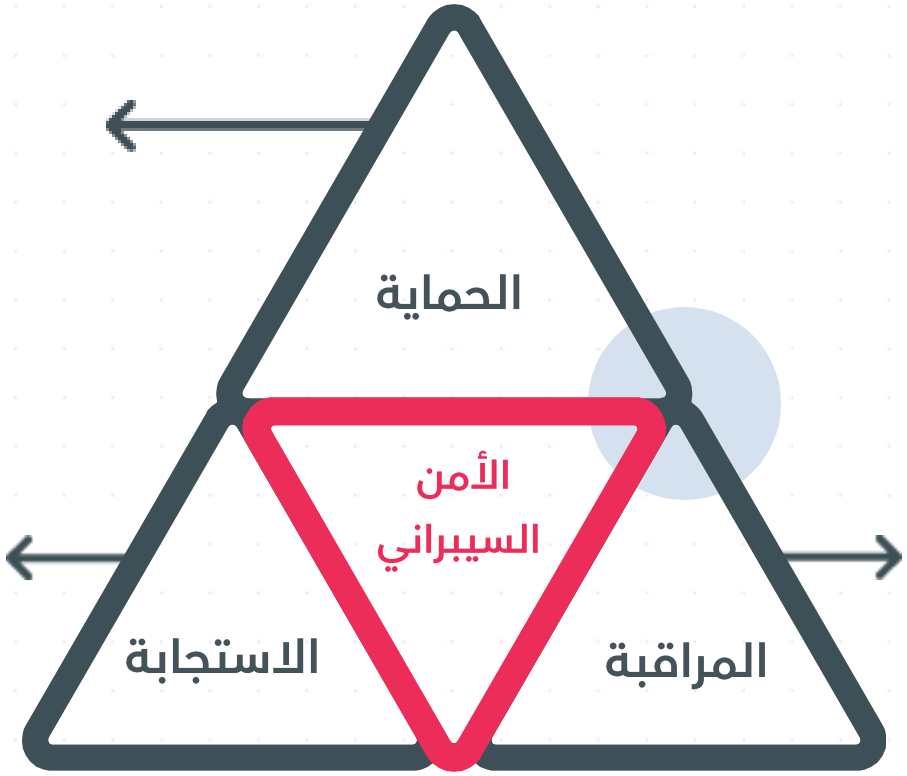
التعامل مع المخاطر والتهديدات السيبرانية



هي ضوابط يتم تنفيذها للتأكد من سرية واستمرارية وسلامة أصول تكنولوجيا المعلومات، الخاصة بالمركز، من التهديدات ونقاط الضعف مثل: القرصنة والبرامج الضارة والسرقة والتصيد الاحتيالي.

التعامل مع المخاطر والتهديدات السيبرانية

تهدف هذه المرحلة إلى الكشف عن التهديدات السيبرانية واختراق البيانات.
وتعد هذه المرحلة جزءاً مهماً من منهجية الأمن السيبراني، حيث تتمكّن المؤسسات من اكتشاف الهجمات السيبرانية في مهدها والتعامل معها قبل أن تتسبب في حدوث أي ضرر.



هي عملية تطبيق التقنيات والعمليات والضوابط لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من الهجمات الإلكترونية. مثال على ذلك، عملية الامتثال للضوابط التي وضعتها الهيئة الوطنية للأمن السيبراني.

هي عملية التحضير للاختراقات الأمنية واكتشافها ومن ثم التعافي منها. وعادة ما تنتج هذه العملية مستند يمنح متخصصي الأمن السيبراني تعليمات حول كيفية الاستجابة لحادث أمني خطير، مثل سرقة المعلومات الحساسة.

أدوات الإبلاغ عن الجرائم السيبرانية

للإبلاغ عن محاولات الانتحال أو الهجمات الإلكترونية أو للإبلاغ على أنك ضحية، قم بزيارة https://ncsc.jo/?v=1&lang=ar#!/Report?ReportID=1 لتقديم شكوى.

نتمنى لكم السلامة في

العالم

الرقمي.