الدليل الإرشادي للمنظمات غير الربحية

لأبرز جوانب التوعية بالأمن السيبراني

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

NCA_KSA
NCA.GOV.SA

يهدف هذا الدليل الإرشـادي إلى تعزيز قيـم المحافظة على الأمن الوطني، ورفع مستـوى الوعـــي بالمخاطر والتهديدات السيبرانيـــة، وبنـــاء ثقافـــــة سيبرانية عالية للعامليـــن في المنظمات غير الربحية

محتوى الدليل

الأمن السيبراني

الأمـــن السيبرانـــي
هو حمايـــة:

الشبكات وأنظمة تقنية المعلومات

أنظمة التقنيات التشغيليـــة

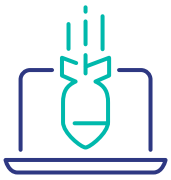
الأجهـــزة والبرمجيات

وما تقدمه مـن خدمات،
ومـا تحويـــه مـن بيانات،
مـن أي اختراق أو تعطيل
أو اسـتخدام غير مشروع

التهديدات السيبرانية كثيـرة مـــن أبــرزهـــا:

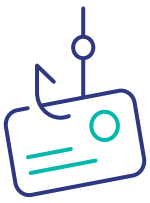
الثغــرات الأمنيـــة

هي مناطـق الضعــف فــي الأنظمة والتطبيقات والتي تفتـــح مجالاً للمهاجميــن



اختراق البيانـــات

يشمل كشف سريّة البيانــات، أو التلاعب بسلامتها، أو منع الوصول إليها



التصيّد الإلكتروني

شكل من أشكال الخداع الإلكترونـــي بهدف التلاعــب بالأفراد وابتزازهـــم وسرقة معلوماتهــم

ارفـــع مستـــوى
أمنك السيبراني

ممارسات تقلل نسبة المخاطر السيبرانية

تثبيـــت التحديثـــات الأمنيّـــة

يُساعد تثبيت التحديثـــات الأمنيـــة علـــى إغلاق الثغرات أمام المهاجميـــــن، مما يسهم في رفع مستوى الأمن السيبراني

كما أن تفعيل خاصيّة التحديث التلقائي يضمـــن تثبيت التحديثات حال صدورها

اختيار كلمات مرور قويّة

لضمان اختيار كلمة مرور قويّة، احرص على:

- ☐ أن تحتوي كلمة المرور على حروف كبيرة وصغيرة وأرقام ورموز
- ☐ استخدام كلمة مرور مختلفة لكل حساب
- ☐ عدم مشاركة كلمة المرور مع أيّ طرف آخر

ممارسات تقلل نسبة المخاطر السيبرانية

تفعيل التحقّق الثنائي

تفعيل خاصيّة التحقّق الثنائي يُساعد على رفع مستوى أمن الحساب، من خلال التحقّق من هويّة المستخدم باستخدام وسيلتين مختلفة

جدولة النسخ الاحتياطي

هو نسخ وأرشفة البيانات إلى مكان آخر لكي يُمكن استعادتها في حال فقدان البيانات الأساسيّة

الهندسة الاجتماعية

من أبرز أشكال الهجمات المستخدمة على نطاق واسع، والتي يقوم من خلالها المهاجم باستهداف الأشخاص مباشرة باستخدام عدد من أساليب التلاعب، إمّا لجعلهم يفصحون عن بيانات حسّاسة، أو يقومون بعمل يُعرّض أمنهم السيبراني للخطر

وتذكّر، أنّ هذا النوع من الهجمات لا يستهدف الثغـــرات الأمنيّـــة، بل العنصـر البشـــــري

التصيّـــد الإلكترونـــي

أحـد أنواع الهندسـة الاجتماعيّـة، والتي يهدف مـن خلالها المهاجم إلى خداع الأشخاص المستهدفين وسرقة بياناتهم، أو اختراق أجهزتهم، أو الاستيلاء على حساباتهم

بعض طرق التواصل مع الأشخاص المستهدفين:

الروابط والمواقع الإلكترونيـــة

منصّات التواصل الاجتماعـــي

البريـــد الإلكتروني

الرسائل النصيـة

الاتصالات الهاتفيـة

أبرز طرق الحماية من التصيّد الإلكتروني:

تحقّق
من الروابط التي تصـل إليك قبل التجاوب معها

تأكّد
من هويّة المُرسل أو المُتصـل

تجنّب
تحميـل المرفقـات، لا سيّما مجهولة المصدر

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

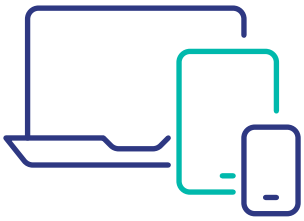
الأمن السيبـــــراني
مسؤوليّتنا المُشتركة

الأمن السيبراني ليس مقتصراً فقط على مختصي التقنية والأمن السيبراني، بل هو مسؤوليّتنا جميعاً، ولكلّ منّا دور يقوم به للمحافظة على أمننا السيبراني، من خِلال اتباعنا للممارسات الآمنة والابتعاد عن مصادر الخطر السيبراني

ساهم في الحفاظ على الأمن السيبراني من خِلال إبلاغ جهة عملك عن الأنشطة المشبوهة في الفضاء السيبراني

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تذكّـــر



أنّ الجميـــــع فـــي
الفضـــاء السيبرانـــي
مُعـــــرّض للمخاطـــر
والتهديدات السيبرانيّـة

الشبكات العامّة اللاسلكيّة

قد يشكّل استخدام الشبكات
اللاسلكية في الأماكن العامة
خطراً على أجهزتك وحساباتك

قد يتمكّن المهاجم من
اختراقها، ومن ثمّ اعتراض حركة
البيانات التي تمرّ من خلالها

مشاركة البيانات
في منصات التواصل الاجتماعي

زيادة مُشاركة البيانات الشخصيّة والحسّاسة في منصّات التواصل الاجتماعي يجعلك أكثر عُرضة لمحاولات الاحتيال. وتذكّر دائماً، أنّ هناك من قد يقوم بجمع بياناتك واستخدامها لاستهدافك

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

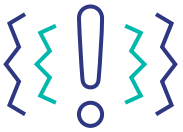
الأمن السيبرانـــي
في بيئة العمـــــل

تجنّب استخدام وسائل التواصل
الاجتماعي عند تبادل البيانـــات
أو الوثائق الخاصة بالعمـــــــل

احرص على استخدام كلمات
مرور قويّة لحسابات العمـل

تعامـل بحـــــذر مـع
الروابط والمُرفقـات

أسبـــاب تُعـــــرّض بيئـــة العمـــل للمخاطـر السيبرانيّـــة



قلّة الوعي بالمخاطر
والتهديدات السيبرانيّة

التساهـل بالالتزام
بالسياسات الأمنيّة

عـــدم اتبـــاع
أفضل الممارسات
السيبرانية

مشاركـــة البيانـــات
الحسّاسة مع الأطراف
غير المصرّح لهم

تثبيت البرامج دون
التأكد من موثوقية
مصدرها

تذكّر أنّ الأمـــن السيبراني عمليّة مُستمرّة، وليـس إجراء يتم لمـــرّة واحدة فقـــط

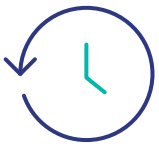
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الاستخـــــدام الآمــن لشبكـــة الإنترنـــــت

لكي تتمكّن من تصفّح الإنترنت بشكــل آمن، وتبتعد عن المخاطر والتهديدات السيبرانيّــة،

احرص على:

اختيــار كلمــات مرور قويّــة



تفعيل خاصيّة التحديث التلقائي للمتصفّح

استخدام التطبيقــات والمواقع الإلكترونيّة الموثوقة

الضبــط الملائــم لإعدادات الأمــن والخصوصيّــة

الاحتيال في الفضاء السيبراني
تعدّدت الطرق، والهدف واحـــد

في الفضاء السيبراني، يقوم المحتالون باستخدام طرق وأساليب مُتجدّدة لشنّ حملات الاحتيال، والتي يكون الهدف منها سرقة البيانات والأموال. وقد يتظاهرون بكونهم يمثّلون أحد الجهات المعروفة

تجنّب الوقوع لحملات التصيّد الإلكتروني، من خلال:

تجنّب التفاعل مـع أي روابط أو رسائل قبـــل التأكـــــد من مصدرها

التأكّد من موثوقيّـة المواقع والتطبيقـات التي تقـوم بزيارتهـا أو استخدامها

الحـرص على عـدم مشاركة رمز التحقق المرسل إليك مـع أي شخص آخر

توصيات

توصيـــات

احرص على اختيار كلمات
مرور قويّة لحساباتك

فعّل خاصيّة التحقق الثنائي
لإبقاء حساباتك آمنة

قم بإجراء النسخ الاحتياطي
لبياناتك بشكل دوري

شارك البيانات الحسّاسة
من خلال القنوات الآمنة

تجنّـــب التجـاوب مـــع
الرسائـل والاتصـــالات
مجهولة المصدر

تأكّد من تفعيل خاصيّة
التحديث التلقائي لنظام
التشغيل والتطبيقات

الهيئة الوطنية
للأمن السيبراني

National Cybersecurity Authority

NCA_KSA NCA.GOV.SA