الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

دليل التوعية السيبرانية

لتأمين الحسابات

لا تفتح مجال

NCA_KSA
NCA.GOV.SA

الحسابات بمثابة الهوية في الفضاء السيبراني

وتأمينها ضرورة ملحة للحد من المخاطر السيبرانية

لا تفتح مجال

خطر سيبراني محتمل حدوثه

وصول غير مشروع للحسابات

قد ينجح المهاجم بتحقيق وصول غير مشروع إلى الحسابات، ومن العوامل التي تساعده على ذلك:

استخدام
كلمات مرور ضعيفة أو مكررة.

مشاركة
رموز الوصول المؤقتة (OTP).

عدم تفعيل
خاصية التحقق الثنائي.

خطر سيبراني محتمل حدوثه

انتحـال الهـوية

انتحال هوية مالك الحسـاب واسـتغلال ذلك لتحقيق عدد من الغايات، منها:

- كشف سرية البيانات والمحادثات.
- تنفيذ عمليات تصيد تجاه أقارب أو زملاء مالك الحساب.

تأمينك لحساباتك

حمايـةٌ للك ولمن حولك مـن المخاطر

السيبرانية

لا تفتح مجال

NCA_KSA

NCA.GOV.SA

الابتعاد عن الممارسات الخاطئة عند التعامل مع كلمات المرور

يُعدّ استخدام كلمات مرور قوية عنصراً أساسياً لتأمين الحسابات. ومع ذلك، فإن تطبيق أي من الممارسات التالية يُقلل من جدوى كلمات المرور، ومن الأمثلة على ذلك:

- مشاركة كلمات المرور مع الآخرين.
- إعادة استخدام كلمات مرور سابقة.
- حفظ كلمات المرور في ملف ملاحظات أو جدول بيانات.

التعامل الآمن مع رموز الوصول المؤقتة

رمـوز الوصول المؤقتة خاصة بك فقط، ومشـاركتها تُعرّض الحسـاب للمخاطـر السـيبرانية، فقـد يحـاول المهاجـم استخدام الحيل التالية لإقناعك بمشاركتها:

- وجـود تحديث عاجـل للبيانات يترتب عليه إغلاق الحسـاب في حال عدم مشاركة رمز الوصول المؤقت.
- تطويـر صفحات تسـجيل دخول وهمية تسـاعد المهاجم على جمع البيانات الحساسة ومعرفة رموز الوصول المؤقتة

تفعيل خاصية التحقق الثنائي

خاصية أمنية تقوم على استخدام وسيلتين مختلفتين للتحقق من هوية المستخدم قبل السماح بالوصول للحساب، مثل:

(التحقق الأول) اسم المستخدم وكلمة المرور.

(التحقق الثاني) رمز الوصول المؤقت.

ويساعد تفعيلها على:

- تعزيز الأمن السيبراني للحسابات.
- منع محاولات الوصول غير المشروع.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

لا تفتح مجال