

وعيك هو الأساس



الأدوات تحميك.. ووعيك هو الأساس



تمنحك أدوات الحماية خطوات دفاع متينة أمام
المخاطر السيبرانية المتجددة، وفاعليتها تبدأ
بالوعي واتباع الممارسات الآمنة.

الحماية.. بوعيك حاضرة

التهديدات السيبرانية لا تستهدف أجهزتك وحساباتك فقط، بل تمتد إلى قرارك في اللحظة الحاسمة:

- هل تفتح الرابط؟
- هل تتجاوب مع الرسالة؟
- هل تُفصح عن بيانات حساسة؟
- هل تؤجل تثبيت التحديث؟
- هل تشارك رمز الوصول المؤقت؟

في هذه اللحظة تحديداً، لا تنفع أدوات الحماية إن غاب الوعي.

**أدوات مفعّلة + وعي حاضر =
حماية حقيقية**

كلمة المرور القوية.. أساس لأمن الحسابات

تُعَدّ كلمة المرور أحد أدوات حماية الحسابات،
وضعفها يعني اختصاراً لطريق المهاجم.

لذلك، احرص على أن تكون:

- معقّدة، تجمع بين الألفبائية الكبيرة والصغيرة والأرقام والرموز
- طويلة، فكلما زاد طولها صُعُب تخمينها
- فريدة، لا تُكرّر من حساب لآخر
- بعيدة عن بياناتك الشخصية، كالاسم وتاريخ الميلاد ورقم الجوال
- متغيّرة فوراً عند أي اشتباه بتسريبها

كلمة المرور..
غير قابلة للمشاركة أو التكرار.





أداة حماية ثانية.. تُبقي حسابك بعيداً عن الاختراق

عند تفعيل خاصية التحقق الثنائي، لا يكفي أن يعرف المهاجم كلمة مرورك، بل يحتاج إلى أداة تحقق ثانية لا تكون إلا بحوزتك أنت.

تعمل بعدة طرق، منها:

- التحقق الأول: كلمة المرور
- التحقق الثاني: رمز وصول مؤقت، أو تطبيق مصادقة، أو بصمة

احرص على تفعيل خاصية التحقق الثنائي لجميع حساباتك.

تفعيل التحقق الثنائي خطوة واحدة، تحمي الكثير.

الرمز لك وحدك

رمز الوصول المؤقت (OTP) مفتاح لحظي لحسابك. ولا توجد جهة رسمية تطلبه منك؛ لا عبر مكالمة، ولا رسالة، ولا رابط.

من آثار مشاركته:

- اختراق حساباتك
- انتحال هويتك
- انكشاف سرية بياناتك

كيف تتصرف عند طلبه؟

- لا تشاركه إطلاقاً، مهما بدت الجهة رسمية
- إنهاء المكالمة أو تجاهل الرسالة
- حظر المرسل والإبلاغ عنه

عند مشاركة الرمز.. تفقد أدوات الحماية فاعليتها.

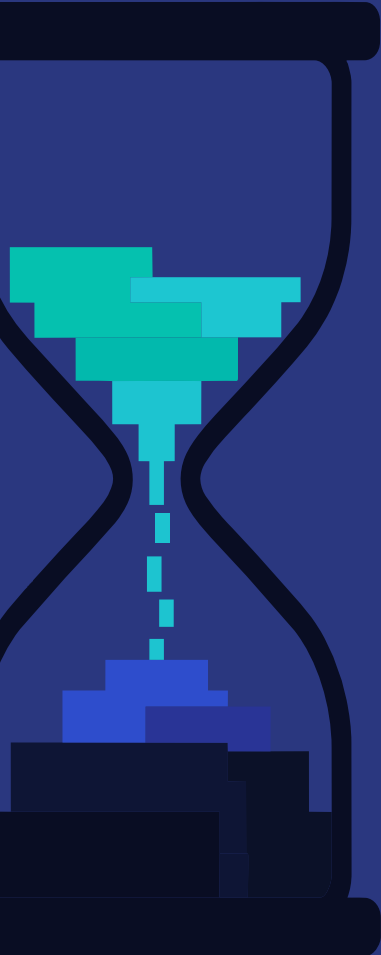
رمز الوصول المؤقت يحميك..
ما دمت لا تشاركه.



في الفضاء السيبراني

التأني يقيك بأمان

الوصول لأجهزتك وحساباتك ينجح باستعجالك،
التوقف لثوانٍ قبل التفاعل يمنحك مساحة كافية
لاكتشاف أساليب التصيد.



إغلاق الثغرة.. قبل أن تُستغل

التحديثات الأمنية ليست تحسينات شكلية، بل معالجة لثغرات أمنية جرى اكتشافها.

وتأجيل تثبيتها يعني ترك الباب مفتوحاً أمام من يبحث عنها.

لذلك، بادر بتفعيل خاصية التحديث
التلقائي لكلٍ من:

- نظام التشغيل
- التطبيقات والبرامج

لا تؤجل تحديث
اليوم إلى الغد.



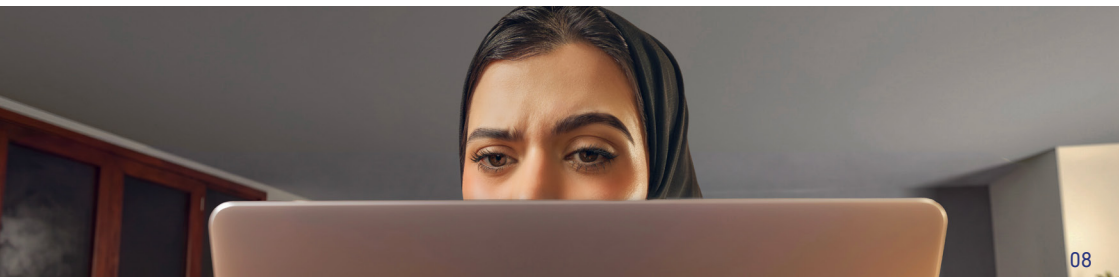
كل جهاز متصل.. يتطلب حماية إضافية

كاميرات المنزل والتلفزيونات وغيرها من الأجهزة الذكية في المنزل؛ جميعها تستدعي تفعيل أدوات الحماية.

لتعزيز أمنها السيرياني؛ احرص على:

- تغيير اسم المستخدم وكلمات المرور الافتراضيتين
- تثبيت التحديثات فور توفرها
- مراجعة الصلاحيات وإيقاف غير الضرورية منها
- تخصيص شبكة منفصلة للأجهزة الذكية في الراوتر المنزلي
- التحقق من وجود تحديثات أمنية قبل شراء الأجهزة

**مستوى أمانك يقاس بوعيك
وتفعيلك لأدوات الحماية.**



نسخة احتياطية.. ملاذ آمن



جدولة النسخ الاحتياطي بشكل دوري،
ممارسة آمنة لحماية البيانات من مخاطر
التلف أو الفقدان

تحقق من الرابط.. قبل أن تتفاعل معه

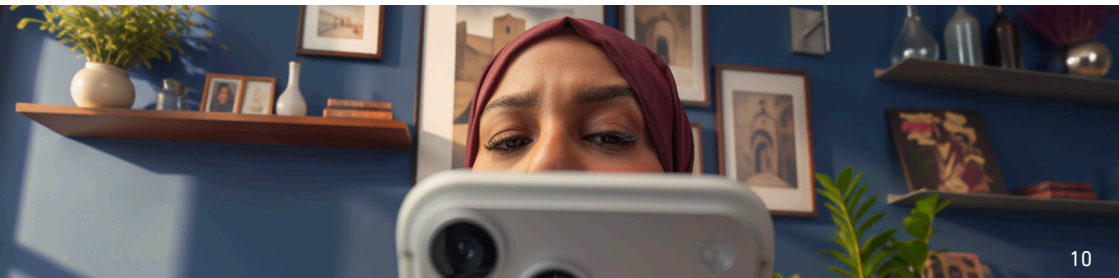
خدمة (تحقق) من الهيئة الوطنية للأمن السيبراني تتيح لك فحص الروابط، ورموز الاستجابة السريعة (QR code)، والملفات والتأكد من سلامتها قبل التعامل معها، بالإضافة إلى تزويدك بإرشادات سيبرانية تسهم في تعزيز أمنك السيبراني.

متى تستخدمها؟

تستخدم الخدمة قبل التعامل مع:

- الروابط
- رموز الاستجابة السريعة (QR code)
- الملفات

ثوانٍ للتحقق.. تحميك من مخاطر التصيد الإلكتروني.



خدمة تحقق TAHQAQ



للوصول إلى الخدمة

+966 11 813 6644

haseen.gov.sa/tahqaq

اضغط هنا



حماية تمتد إلى من تُحب

الأطفال عرضة للمخاطر السيبرانية، وأدوات الرقابة الأبوية تمنحك القدرة على تهيئة بيئة سيبرانية آمنة لهم.

ما الذي تتيحه لك؟

- تحديد المحتوى المناسب لأعمارهم وحجب غير المناسب
- ضبط مدة الاستخدام والتطبيقات المسموح بها
- التحكم في عمليات التحميل والشراء داخل التطبيقات
- تقييد التواصل مع مجهولين



تعرفّ على طريقة
تفعيل الرقابة الأبوية
للأبرز الأنظمة

نحو فضاء سيبراني آمن للأطفال



تقييد الصلاحيات..

يُجَنَّبُ أَجْهَزَتُكَ المخاطر السيبرانية

احرص على الاكتفاء بمنح التطبيقات الصلاحيات الضرورية فقط.



استفد منه.. بوعي مسؤول

التعامل الآمن مع أدوات الذكاء الاصطناعي جزء
من أمنك السيبراني.

احرص على:

- الاكتفاء بالمعلومات اللازمة لإنجاز المهمة،
وتجنّب إدخال البيانات الحساسة أو السرية
- مراجعة إعدادات الأمن والخصوصية وخيارات
استخدام البيانات
- تفعيل التحقق الثنائي لحسابات أدوات
الذكاء الاصطناعي

**اجعل الذكاء الاصطناعي أداة للإنجاز..
لا منفذاً إلى البيانات الحساسة.**

أدوات الحماية يبدأ أثرها بالتفعيل.. ويكتمل بالوعي

أدوات الحماية تبني الجدار، والوعي
هو الأساس.

تفعيل الأدوات خطوة أساسية، لكن
الحماية لا تتوقف عندها؛ فالوعي
يُختبر مع كل رسالة، ورابط.

أدوات مفعّلة، ووعي حاضر.. حماية
أكثر اكتمالاً.

وعيك السيبراني..
خط الدفاع الأول.

وعيك السيبراني وتفعليلك لأدوات الحماية يُعزز أمنك السيبراني

لا
تفتح
مجال

