

أمان الإنترنت

يبدأ من هنا

دليل التوعية السيبرانية لأولياء الأمور

أبناءؤنا اليوم في فضاء سيبراني مفتوح

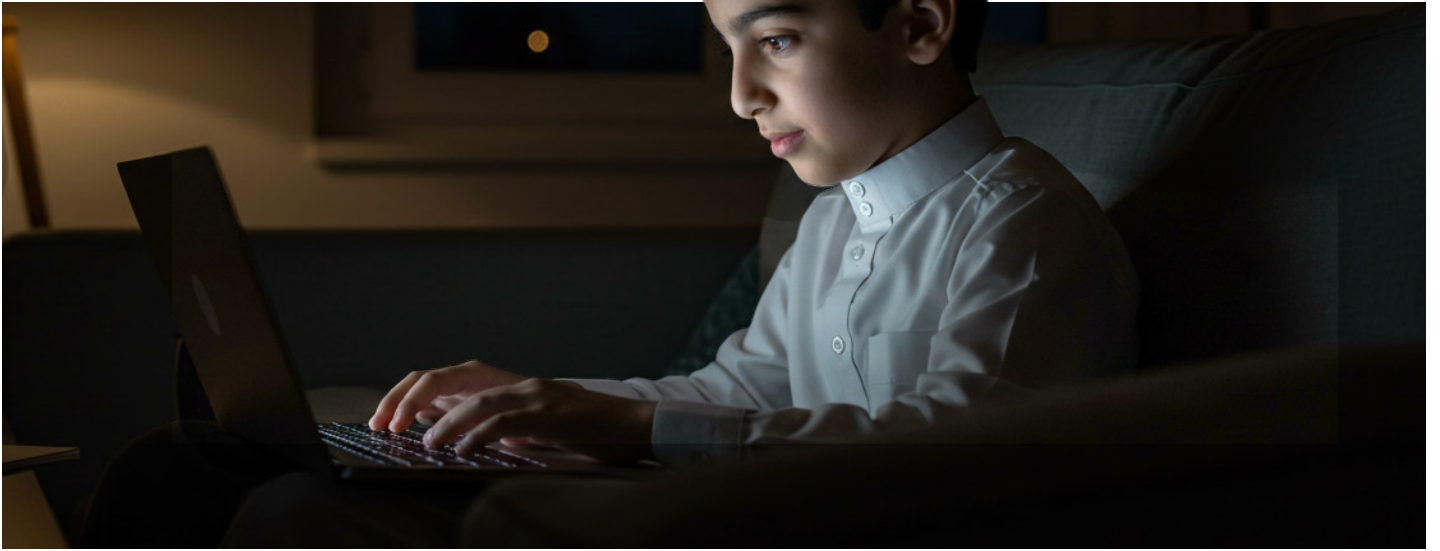
تعرف على دليل التوعية السيبرانية لحماية
الأبناء من مخاطر الفضاء السيبراني

يساعدنا الوعي بأهمية الأمن السيبراني

على حماية أجهزتنا وبياناتنا وحساباتنا من الاختراقات والوصول غير المشروع. وبما أن الأبناء أصبحوا جزءاً من هذا الفضاء السيبراني، من المهم أن يتم توعيتهم حيال المخاطر السيبرانية وإجراءات الحماية منها.



مخاطر الفضاء السيبراني



أبرز التهديدات السيبرانية التي قد يتعرض لها الأبناء:



الاختراق وسرقة البيانات

مهاجمون قد يستغلون حسابات الأبناء للوصول إلى بيانات العائلة (بريد إلكتروني، صور، معلومات مصرفية).



البرمجيات الخبيثة

برامج ضارة تنتقل من روابط أو تطبيقات مزيفة، قد تسرق البيانات أو تعطل الأجهزة.



التصيد الإلكتروني

روابط مزيفة تُقنع الأبناء بإدخال معلومات حساسة مثل الحسابات ورموز الوصول المؤقتة (OTP).

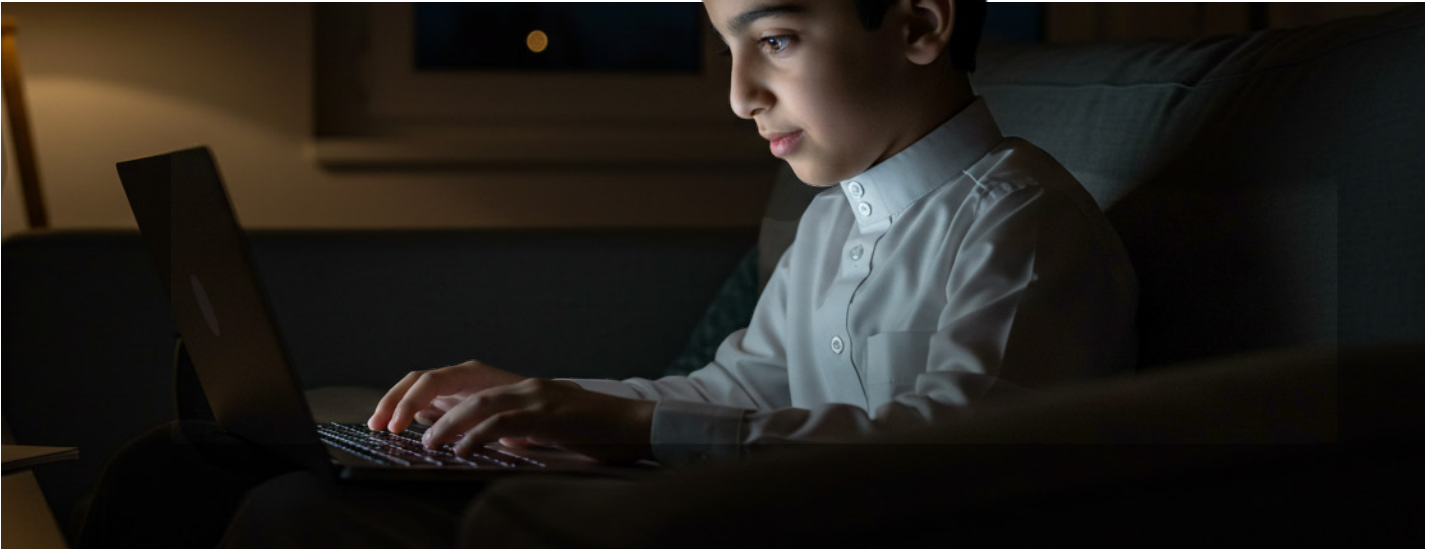


الخداع السيبراني

أشخاص مزادعون يتظاهرون بأنهم أطفال أو جهات رسمية للحصول على معلومات حساسة أو كلمات مرور.



مخاطر الفضاء السيبراني



أبرز التهديدات السيبرانية التي قد يتعرض لها الأبناء:



تنزيل تطبيقات من مصادر غير موثوقة

قد تحتوي التطبيقات من خارج المتاجر الرسمية على برمجيات ضارة أو تفعيل كاميرا/ميكروفون بدون إذن.



الاتصال بشبكات Wi-Fi عامة

الاتصال بشبكات غير آمنة قد يعرض الجهاز للتجسس وسرقة البيانات.

ملاحظة

ليس كل تهديد يظهر بشكل مباشر، إذ أن بعض التهديدات السيبرانية تعمل في الخفاء وتجمع البيانات دون أن يشعر الأبناء.

الدراسة بأمّان



طوال العام الدراسي، يزداد تفاعل الأبناء وأولياء الأمور مع الفضاء السيبراني

عبر منصات التعليم، ومواقع التسجيل، وتطبيقات المتابعة، والتواصل بين الأسرة والمدرسة؛ لكن هذا النشاط المكثف يجعل الجميع عرضة لمحاولات التصيد الإلكتروني.

انتبه

ولي الأمر أيضاً مُعرّض للمخاطر السيبرانية

اتتبعه



ولي الأمر أيضاً مُعرّض للمخاطر السيبرانية

مواقع وهمية مشابهة للمواقع الرسمية

يتم إرسال روابط عبر الرسائل النصية أو البريد الإلكتروني تحتوي على صفحات مزيفة تطلب:



معلومات الحساب البنكي



بيانات الأبناء



رقم الهوية



رسائل بريد إلكتروني مزيفة:

بعض المهاجمين ينتحلون صفة المدارس لإرسال روابط تصيدية تطلب فتح ملف أو تحديث معلومات.



تطبيقات غير موثوقة تدّعي متابعة الطالب:

قد تُظهر بعض التطبيقات نفسها كأدوات لمتابعة أداء الطالب، لكنها في الحقيقة تجمع البيانات أو تُخفي برمجيات خبيثة.

كيف تحمي نفسك وأسرتك؟

لولي الأمر



تجنّب الضغط على الروابط مجهولة المصدر



تعامل مع الروابط الموثوقة فقط



تحقق من عنوان الموقع بدقة



راجع الملاحظات عند تحميل التطبيقات



تجنب مشاركة البيانات الحساسة مع أي جهة غير موثوقة



راجع الروابط بدقة، فالفرق بين الموقع الموثوق والاحتيالي قد يكون حرفاً واحداً



ثبّت التطبيقات من خلال المتاجر الرسمية مثل (App Store/Google Play)



قُم بالبحث عن موقع المدرسة أو المنصة بنفسك، ولا تعتمد على الروابط المرسلة

إجراءات الحماية السيبرانية



للإسهام في الحماية من المخاطر السيبرانية، اتبع الإجراءات التالية:

التعامل الآمن مع كلمات المرور



- اختيار كلمات مرور قوية للحسابات
- عدم مشاركة كلمات المرور مع الآخرين
- الابتعاد عن إعادة استخدام كلمات مرور سابقة

تحميل التطبيقات من

المتاجر الرسمية فقط



تفعيل التحقق الثنائي

خاصية تُعزز حماية البيانات



تحديث التطبيقات والنظام باستمرار

التحديثات تُغلق ثغرات أمنية قد يستغلها المهاجمون



تعزيز الأمان

عطل صلاحية الوصول إلى الكاميرا والميكروفون من التطبيقات غير الضرورية.



راجع إعدادات الأمن والخصوصية في جميع التطبيقات التي يستخدمها ابنك (إخفاء المعلومات، إيقاف التتبع).



التصفح الآمن

علم ابنك عدم الضغط على "عروض" أو "جوائز" مجهولة.



راقب الإعلانات والنوافذ المنبثقة فالبعض منها يقود إلى برامج ضارة.



التواصل هو السر!



المعرفة بالمحتوى

تعرف على التطبيقات والألعاب التي يستخدمها، شاهدها أو جربها بنفسك، اسأل ابنك عن أكثر ما يعجبه فيها.



المحادثة المستمرة

تحدث مع ابنك عن تجربته السيبرانية كأنها جزء من يومه العادي، لا تُظهر صدمة أو خوفاً عند سماعك لأمر مزعجة، بل كن داعماً ومتفهماً.



تعزيز الثقة

يجب أن يدرك الابن أنه يمكنه اللجوء إليك دون أن يتعرض للعقاب، مهما كان الخطأ.



اشرح له الممارسات الآمنة بعبارات بسيطة

"اسمك، مدرستك، صورك... لا تشاركها مع أحد دون إذن."
"إذا ما عرفت الرابط... لا تضغط عليه".



عدم الاعتماد الكامل على التقنية

التطبيقات لا تحل مكان التوجيه، بل هي أدوات مساعدة فقط.

درع الأبطال

اختبار تفاعلي مشترك للابن وولي الأمر
لتكتشف مدى الوعي بمخاطر الفضاء السيبراني

شاركوا معاً في الإجابة على الأسئلة، وتعرّفوا على نتائجكم سوياً



01 | إذا طلب منك تطبيق جديد كتابة رقم جوالك، ما الخطوة الصحيحة التي يجب أن تقوم بها؟

استأذن والدي أولاً قبل إدخال أي رقم

أضع رقماً عشوائياً فقط لأتجاوز الخطوة

اكتبه فوراً لأنني أحتاج للتسجيل

02 | عند إنشاء حساب في لعبة أو تطبيق، ما هو التصرف الأكثر أماناً؟

اترك الخانات فارغة

لا أشارك معلومات حقيقية عني أبداً

استخدم اسمي الكامل وتاريخ ميلادي الحقيقي

03 | من الأشخاص الذين يُسمح لهم بمعرفة كلمات المرور أو بيانات الحساب؟

الأصدقاء المقربون

فقط أنا ووالدي ووالدي

أي شخص ألعب معه في نفس اللعبة

04 | ما أفضل وصف لكلمة مرور قوية؟

كلمة سهلة
حتى أتذكرها
بسرعة

كلمة طويلة تحتوي
على أرقام ورموز
ولا يعرفها أحد

123456
أو اسمي الأول

05 | ظهر لك تحديث لتطبيقك المفضل من خارج المتجر الرسمي... هل تثبته؟

أطلب من زميلي
إرساله لي

لا، أحمل التحديث
فقط من المتجر
الرسمي

نعم، حتى لو
من خارج المتجر

06 | رأيت إعلاناً يقول: "اربح جهازاً مجاناً الآن!"، ويطلب منك الضغط على رابط، ماذا تفعل؟

أرسله لأصدقائي
لتجربته

أتجاهل الإعلان وأخبر
والديّ لو تكرر

اضغط بسرعة
للفوز بالجائزة

07 | لماذا نستخدم التحقق الثنائي في الحسابات؟

حتى أتمكن من اللعب
في أكثر من جهاز

لزيادة الأمان ومنع
سرقة الحساب حتى لو
عُرفت كلمة المرور

لتسجيل الدخول
بشكل أسرع

08 | من أين يجب تحميل التطبيقات والألعاب؟

من المتجر الرسمي
فقط (App Store)
أو Google Play
أو (AppGallery)

من روابط
الأصدقاء

من أي رابط متاح على
منصات التواصل
الاجتماعي

09 | طلب منك موقع إلكتروني كتابة كلمة المرور الخاصة بحساب مدرستك، لكنه ليس الموقع الرسمي... ماذا تفعل؟

أغلق الصفحة فوراً ولا
أشارك أي بيانات

اسأل أصدقائي
إذا قاموا بتجربته

أكتبها إذا بدا
الموقع موثقاً

10 | لأولياء الأمور: أرسل لك رابط لتحديث بيانات الطالب من جهة "تبدو" رسمية... كيف تتصرف؟

ترسله إلى
مجموعة أولياء
الأمور للتأكيد

تتحقق من مصدر
الرابط بنفسك من
الموقع الرسمي للجهة

تفتحه فوراً
وتقوم بتعبئة
البيانات

11 | لأولياء الأمور: ما الموقف الصحيح إذا لاحظت تغييراً في سلوك طفلك السيبراني؟

تبدأ حواراً هادئاً لتفهم
ما حدث وتدعم
تصرفه الصحيح

تمنعه من
استخدام الجهاز

تتجاهل الموضوع
حتى يتحدث هو

تعرف على الأجوبة الصحيحة

01 | أستاذن والديّ أولاً قبل إدخال أي رقم.

02 | لا أشارك معلومات حقيقية عني أبداً.

03 | فقط أنا ووالدي ووالدي.

04 | كلمة طويلة تحتوي على أرقام ورموز ولا يعرفها أحد.

05 | أقوم بتحميل التحديث فقط من المتجر الرسمي.

06 | أتجاهل الإعلان وأخبر والديّ لو تكرر.

07 | لزيادة الأمان ومنع سرقة الحساب حتى لو عُرفت كلمة المرور.

08 | من المتجر الرسمي فقط (App Store أو Google Play أو AppGallery).

09 | أغلق الصفحة فوراً ولا أشارك أي بيانات.

10 | تتحقق من مصدر الرابط بنفسك من الموقع الرسمي للجهة.

11 | تبدأ حواراً هادئاً لتفهم ما حدث وتدعم تصرفه الصحيح.

تعرف على مستوى الأمان في الفضاء السيرياني!



الآن بعد الإجابة على الأسئلة.. احسب النتيجة:

من 5 إلى 7 إجابات صحيحة.. أمان متوسط

• معرفة متوسطة، وهناك فرصة كبيرة لتعزيز الأمان.

من 8 إلى 10 إجابات صحيحة.. أمان ممتاز!

• إدراك متميز للأساسيات وأساليب الحماية.

11 إجابة صحيحة.. أمان استثنائي!

• وعي سيرياني متقدم، ومن المهم مشاركة المعرفة مع الآخرين.

الرقابة الأبوية



درع الأمان للأبناء في
الفضاء السيبراني

الرقابة الأبوية

مجموعة من الأدوات والتقنيات التي تتيح لأولياء الأمور متابعة وتحديد استخدام الأبناء للإنترنت والأجهزة؛ بهدف حمايتهم من المحتوى غير المناسب والمخاطر المحتملة. تشمل هذه الأدوات تصفية المحتوى، وتحديد وقت الاستخدام، وتقييد الوصول إلى تطبيقات أو مواقع معينة.



نصائح لتطبيق الرقابة الأبوية

- **الحوار المفتوح:** التحدث مع الأبناء حول المخاطر السيبرانية وطرق الاستخدام الآمن للأجهزة.
- **إشراك الأبناء:** مشاركة الأبناء في إعداد أدوات الرقابة الأبوية لزيادة الوعي والمسؤولية.
- **المرونة:** تعديل إعدادات الرقابة الأبوية مع تقدم الأبناء في العمر وتغير احتياجاتهم.



مميزات الرقابة الأبوية

- **تصفية المحتوى:** حظر المواقع والتطبيقات والمحتوى غير المناسب.
- **تحديد وقت الاستخدام:** ضبط مدة استخدام الأجهزة أو التطبيقات.
- **إدارة التطبيقات:** الموافقة على طلبات تحميل التطبيقات.
- **تقييد عمليات الشراء:** منع عمليات الشراء داخل التطبيقات.

لا تفتح مجالات