عرض تقديمي شامل

التوعية بمخاطر الإنترنت

حماية أنفسنا وأبنائنا في العالم الرقمي

استراتيجيات عملية لبناء جدار من الوعي والمعرفة لضمان بيئة آمنة في العصر الرقمي.

جهة الإصدار

مجلة البحوث والدراسات العربية للطفل والأسرة والمجتمع

التصنيف

أمن المعلومات / السلامة الرقمية

الواقع الرقمي اليوم

ضرورة حتمية

أصبح الإنترنت نافذة العالم للأطفال واليافعين.
التوعية ليست خياراً إضافياً، بل درعٌ أساسي.

الوضع السابق

~~مجرد التحذير~~

الهدف الحالي

التمكين المعرفي

أمن المعلومات والسلامة الرقمية

أهداف العرض التقديمي

نسعى للانتقال من مرحلة المراقبة السلبية إلى
بناء منظومة حماية ذاتية عبر محورين أساسيين:

أولاً: الوقاية الواعية

فهم عميق لطبيعة المخاطر الرقمية التي تتراوح بين الأذى النفسي، والاجتماعي، وصولاً للتهديدات الأمنية والمالية، وكيفية تجنبها بذكاء.

ثانياً: التمكين من التصرف

تسليح الأسرة بالأدوات والمعرفة للخطوات الصحيحة التي يجب اتخاذها فور التعرض لأي مشكلة، لضمان تجربة آمنة.

خريطة التهديدات

ما هي مخاطر الإنترنت؟

تتنوع مخاطر الإنترنت لتشمل جوانب نفسية، مالية، أمنية، وسلوكية. فهم هذا التصنيف هو الخطوة الأولى نحو حماية فعالة.

5 تصنيفات رئيسية

المخاطر النفسية والاجتماعية

وتشمل التنمر الإلكتروني، والتعرض لمحتوى غير لائق، وتأثير المقارنات الاجتماعية السلبية.

المخاطر المالية والأمنية

مثل عمليات الاحتيال، والتصيد الإلكتروني، والابتزاز مقابل المال، وسرقة الهوية.

مخاطر الخصوصية

كشف البيانات الشخصية، تتبع الموقع، واختراق الحسابات الشخصية واستغلالها.

المخاطر السلوكية والصحية

الإدمان الرقمي وتأثيره على النوم والدراسة، والانعزال الاجتماعي.

مخاطر الألعاب الإلكترونية

التواصل مع الغرباء، عمليات الشراء غير المراقبة، والتعرض لمحتوى عنيف داخل بيئات اللعب.

التنمر الإلكتروني

استخدام التكنولوجيا الرقمية لإيذاء أو مضايقة أو إحراج شخص آخر بشكل متعمد ومتكرر.

النطاق

يتجاوز حدود المدرسة ويلاحق الضحية في كل مكان، مما يتطلب تدوخلاً سريعاً.

أشكال شائعة للتنمر

المضايقة
رسائل تهديدية أو مهينة.

التشهير
نشر شائعات أو صور محرجة.

الانتحال
حسابات مزيفة باسم الضحية.

الاستبعاد
الطرد المتعمد من المجموعات.

علامات الخطر (تحذيرات)

- تغير مفاجئ في المزاج (قلق، حزن، غضب) خاصة بعد استخدام الأجهزة.
- الانسحاب الاجتماعي وتجنب الأصدقاء أو المدرسة.
- سرية مفرطة وإغلاق الشاشات عند اقتراب الوالدين.
- انخفاض ملحوظ في مستوى التحصيل الدراسي.

الآثار النفسية العميقة

- **الشعور بالخزي والعار**
- **فقدان الثقة بالنفس**
- **الاكتئاب الحاد**
- **خطر إيذاء الذات (في الحالات الشديدة)**

المخاطر الرقمية

الاحتيال والابتزاز الإلكتروني

أساليب الاحتيال والتصيد

تصلك رسائل تبدو رسمية (بنوك، شحن) تطلب تحديث البيانات عبر روابط مزيفة تهدف لسرقة كلمات المرور. وتشمل أيضاً وعوداً بجوائز وهمية مقابل بياناتك الشخصية.

آلية الابتزاز الإلكتروني

يبدأ بإقناع الضحية بإرسال صور خاصة، ثم استخدامها للتهديد المالي أو الإجبار على أفعال أخرى. يستهدف غالباً المراهقين عبر استغلال الثقة.

⚠ الركيزة الأساسية: المحتال يعتمد على الخداع النفسي واستغلال "الثقة".

قواعد التحقق الأساسية

4 خطوات ذهبية لقطع الطريق على المحتالين

لا تثق بالروابط

لا تضغط على الروابط في الرسائل غير المتوقعة. اكتب عنوان الموقع الرسمي للجهة مباشرة في المتصفح.

دقق في العنوان

افحص عنوان البريد الإلكتروني جيداً. رسائل التصيد غالباً تحتوي على أخطاء إملائية أو تأتي من نطاقات غريبة.

احذر الاستعجال

عبارات مثل "حسابك سيغلق" أو "عرض سري" هي فخاخ نفسية لدفعك للتصرف بسرعة دون تفكير نقدي.

لا تشارك أبدًا

كلمات المرور، رموز التحقق (OTP)، ومعلومات البطاقة البنكية لا تطلبها الجهات الرسمية عبر البريد أو الرسائل.

الأمن الرقمي

سرقة البيانات والخصوصية

خصوصيتنا هي أثمن ما نملك في العالم الرقمي. كل معلومة نشاركها تشكل جزءًا من بصمتنا الرقمية التي قد تُستغل ضدنا إذا لم نتعامل معها بحذر.

البيانات الحساسة

هي أي معلومة يمكن استخدامها لتعريف هويتك أو الوصول إلى حساباتك.

أمثلة حيوية

- الاسم الكامل وتاريخ الميلاد
- عنوان المنزل
- رقم الهاتف
- كلمات المرور
- المعلومات المالية

مخاطر المشاركة

مشاركة الموقع

يكشف روتينك اليومي وأماكن تواجدك، مما يجعلك هدفًا للسرقة أو التتبع.

الصور والمعلومات الشخصية

قد تُستخدم في عمليات انتحال الهوية أو الابتزاز الإلكتروني.

كلمات مرور ضعيفة

استخدام "123456" أو تواريخ الميلاد يسهل اختراق جميع حساباتك فوراً.

إجراءات الحماية

إعدادات الخصوصية

اضبط حساباتك لتكون "خاصة" أو "للأصدقاء فقط".

كلمات مرور قوية

استخدم مزيجاً طويلاً من الحروف والأرقام والرموز.

فكر قبل النشر

"هل أرغب في أن يرى العالم كله هذه المعلومة عني؟"

الإدمان الرقمي

يتحول استخدام الإنترنت من عادة إلى إدمان عندما يبدأ في السيطرة على وقتنا ويؤثر سلباً على صحتنا وعلاقاتنا.

التأثير على الحياة

يؤثر سلبًا على التركيز، يقلل من جودة النوم (خاصة قبل النوم)، ويؤدي إلى تدهور العلاقات الاجتماعية الحقيقية.

التشخيص والعلاج

ميزان التوازن الرقمي

مؤشرات الخطر

الاستخدام المفرط
فقدان الإحساس بالوقت لساعات طويلة.

أعراض الانسحاب
القلق والغضب عند انقطاع الاتصال.

الانعزال الاجتماعي
تفضيل العالم الافتراضي على الواقعي.

المشاكل الصحية
اضطرابات النوم وآلام الظهر والرقبة.

قواعد التنظيم

1 **تحديد أوقات صارمة**
تخصيص فترات زمنية محددة للاستخدام والالتزام بها.

2 **مناطق خالية من الأجهزة**
منع الأجهزة في غرف النوم وأماكن الطعام.

3 **فلترة الإشعارات**
تفعيل التنبيهات الضرورية فقط لتقليل التشتت.

4 **البدائل الصحية**
استبدال الشاشات بالرياضة والهوايات الواقعية.

مخاطر الألعاب الإلكترونية

الألعاب الإلكترونية بيئة ممتعة ولكنها تحمل مخاطر فريدة تتطلب يقظة الأهل، بدءاً من التفاعل مع الغرباء، وصولاً إلى الاستنزاف المالي والتعرض لمحتوى غير لائق.

التواصل مع الغرباء

تتيح الدردشة الصوتية والنصية للأطفال التفاعل مع غرباء قد يحملون نوايا سيئة كالتنمر أو الاستدراج.

الاستنزاف المالي

تصميم الألعاب (مثل Loot Boxes) يشجع على الإنفاق المستمر، مما قد يؤدي لخسائر مالية دون إذن.

المحتوى غير المناسب

احتواء بعض الألعاب على مشاهد عنف أو لغة بذيئة لا تتناسب إطلاقاً مع الفئة العمرية للطفل.

مشاركة البيانات

طلب أذونات وصول حساسة أو تشجيع اللاعبين لبعضهم البعض على كشف معلومات شخصية خاصة.

التأثير السلوكي والنفسي

قضاء ساعات طويلة في اللعب يؤدي للعزلة الاجتماعية، كما أن التعرض المستمر للألعاب العنيفة قد يعزز الميول العدوانية ويغير سلوك الطفل في الواقع.

كيف نحمي أنفسنا؟

حمايتنا الرقمية لا تتطلب خبرة تقنية معقدة، بل هي مجموعة من العادات والممارسات اليومية البسيطة التي تشكل درعًا واقيًا.

خط الدفاع الأول:

الوعي المسبق

كلمات مرور قوية

يجب أن تكون طويلة (12 حرفًا على الأقل) وتجمع بين الحروف الكبيرة والصغيرة والأرقام. استخدم كلمة مرور مختلفة لكل حساب.

المصادقة الثنائية (2FA)

تضيف طبقة أمان إضافية حيوية، حيث تطلب رمزًا يتم إرساله إلى هاتفك عند محاولة تسجيل الدخول من جهاز جديد.

ضبط الخصوصية

اجعل حساباتك على وسائل التواصل الاجتماعي "خاصة" (Private) وراجع بدقة من يمكنه رؤية منشوراتك ومعلوماتك.

التفكير قبل النشر

ما تنشره يبقى للأبد. تجنب مشاركة المعلومات الشخصية الحساسة مثل عنوان المنزل أو رقم الهاتف بشكل تام.

الحذر من الروابط

لا تضغط على أي رابط غير متوقع أو مشبوه، حتى لو كان من صديق، فقد يكون حسابه مخترقًا.

تحديث البرامج

حافظ على تحديث نظام التشغيل والمتصفح ومكافحة الفيروسات باستمرار لسد الثغرات الأمنية المكتشفة حديثاً.

خطة العمل الطارئة

ماذا نفعل عند التعرض لمشكلة؟

عند مواجهة مشكلة على الإنترنت، فإن التصرف السريع والهادئ والمنظم هو مفتاح تقليل الضرر. الخطوة الأهم هي كسر حاجز الصمت.

القاعدة الذهبية

لا ترد ▪ وثّق ▪ بلّغ

01

توقف فورًا!

لا ترد على المتنمر، ولا تستجب لطلبات المبتز، ولا تدفع أي أموال. أي رد فعل منك سيشجعه على الاستمرار.

02

احتفظ بالأدلة

قم بأخذ لقطات شاشة (Screenshots) للرسائل أو الصور المسيئة. هذه الأدلة مهمة جدًا عند الإبلاغ لاحقاً.

03

احظر وبلّغ

استخدم خاصية الإبلاغ في المنصة وأحظر المسيء فورًا لمنعه من التواصل. أوقف دائرة الأذى التقني.

04

أمّن حساباتك

إذا شككت باختراق، غيّر كلمة المرور فورًا وفعل المصادقة الثنائية (2FA) لقطع الطريق على المخترق.

05

اطلب المساعدة

تحدث فورًا مع شخص تثق به (أحد الوالدين أو معلم). لا تحاول حل المشكلة بمفردك؛ المشاركة نصف الحل.

06

الجهات المختصة

في حالات التهديد أو الابتزاز المالي، لا تتردد في التواصل مع وحدات الجرائم الإلكترونية فوراً.