

## مَسرد المصطلحات

**التصيّد الإلكتروني:** هجمة أمنية سيبرانية تُنفَّذ عبر الرسائل الإلكترونية وتُتيح سرقة المعلومات الشخصية، بإدراج روابط زائفة في الرسائل الإلكترونية يمكنها عند النقر عليها سرقة كلمات السر الخاصة بكل منكم أو تركيب ملفات تحوي برمجيات خبيثة. البرمجية الخبيثة: برنامج إلكتروني يُلحق أضراراً بالأجهزة الإلكترونية (كالحواسيب والهواتف الذكية). الرقابة الوالديّة: ممارسة تُشير إلى الأدوات التي تُتيح حماية الأطفال من التهديدات التي قد يتعرّضون لها على الإنترنت، وذلك بمنع الأفعال التي قد تكون خطرة.

# السلامة على الإنترنت مع سنانغو



## الأخطار

- سرقة البيانات
- انتحال الهوية
- التصيّد الإلكتروني
- رؤية صور وتسجيلات فيديو غير مناسبة لأعماركم
- معرفة التطبيقات دائماً لأماكن وجودكم عندما يكون خيار "الموقع" في أجهزتكم الإلكترونية مُفَعَّلًا
- إمكانية نشر المحتوى الشخصي الخاص بكل منكم دون إذنه



## شبكات التواصل الاجتماعي

- إن شبكات التواصل الاجتماعي أدوات تستخدمونها للبقاء على اتصال بأصدقائكم، لكنها تخفي أيضاً العديد من الأخطار. والحقيقة أن من السهل جداً إنشاء ملف شخصي زائف: فاحترسوا، لأنكم لا تعلمون أبداً من قد يكون ذلك الشخص المُتخفي باسم المستخدم
- وإضافة إلى احتمال أن تلتقوا أشخاصاً سيئِي النوايا، يُحتمل أيضاً أن تلتقوا محتوى غير مناسب لأعماركم كصور أو تسجيلات فيديو قد تُزعجكم.

## البيانات الشخصية

- عندما نستخدم الإنترنت، فإننا لا ندرك كم البيانات الشخصية التي نُشاركها وكيف يمكن للآخرين استخدامها دون إذنتنا.
- فلا تشاركوا أبداً كلمات السر الخاصة بكل منكم وعناوين منازلكم وأرقام هواتفكم وأيام أعياد ميلادكم. بل حتى هوياتكم معلومات خاصة أيضاً! فتأثروا فيما تنشرونه من صور وتسجيلات فيديو.
- وتذكروا دوماً: لا شيء على الإنترنت خاص تماماً!

## التطبيقات

- تُسجل التطبيقات مجموعة من المعلومات الشخصية كبيانات الاتصال بكم وأماكن وجودكم، وهو ما يُتيح للأشخاص سيئِي النوايا معرفة أماكن وجودكم عند استخدامكم هذه التطبيقات.
- فتحدّثوا دوماً مع شخص بالغ قبل شراء التطبيقات أو تفعيل المستويات الجديدة في الألعاب، تجنّباً للمواقف المكروهة.
- ولا تلعبوا سوى مع الأصدقاء الذين تعرفونهم شخصياً عند استخدام التطبيقات والمواقع الإلكترونية المناسبة لأعماركم.

## ما الأعمال التي يمكنكم القيام بها لحماية أنفسكم على الإنترنت؟

- أغلقوا أجهزتكم دوماً بشفرة السر الخاصة بكل منكم عند عدم استخدامها، واستخدموا كلمات سر طويلة ومعقدة وسرية لحماية جميع حساباتكم.
- اضبطوا إعدادات ملفاتكم الشخصية لتكون خاصة، ولا تشاركوا أحداً بمعلوماتكم الشخصية، واستخدموا أسماء مستعارة إن لزم الأمر..
- تأكدوا من أنكم تعرفون الأصدقاء الذين تتواصلون معهم عبر تطبيقات المحادثات وشبكات التواصل الاجتماعي: لا تشاركوا الآخريين سوى المحتوى الذي تتراحون إليه.
- أخبروا شخصاً بالغاً إن تلقيتم طلباً أو محتوى يُزعجكم أو رأيتم شيئاً غير مناسب لأعماركم، مناسباً للأعماركم.
- اطلبوا من شخص بالغ تثقون به تفعيل أدوات الرقابة الوالديّة في الأجهزة التي تستخدمونها.

تايكونا وابقوا على علم عبر الموقعين الإلكترونيين التاليين:  
[www.itu.int\cop](http://www.itu.int\cop) و [www.itu-cop-guidelines.com](http://www.itu-cop-guidelines.com)



هل تعلمون ...

أن حتى هواتفكم الذكية تحوي معلوماتكم الشخصية؟ فأغلقوها دوماً بشفرة السر وانتبهوا إليها!



Deloitte.

