

خطوات لحماية الأطفال عبر الإنترنت 6



دبي: «الخليج»

كشفت بالو ألتو نتوركس عن مجموعة من الخطوات التي تمكّن أفراد العائلة من الحفاظ على أمن الأطفال الإلكتروني في ظل انتشار التعليم عن بعد.

وقد يبدو استخدام التقنيات والتطبيقات الجديدة والتنقل بين الفصول الدراسية في بيئة افتراضية، أمراً مربكاً بعض الشيء، لكن ذلك يجب ألا ينطبق على قضية الأمن السيبراني ضمن هذه البيئات الافتراضية. فمن خلال اتباع بعض الممارسات الجيدة والبسيطة، يمكن للوالدين المساعدة في حماية أطفالهم من الجرائم الإلكترونية، فضلاً عن الحفاظ على خصوصيتهم على شبكة الإنترنت:

1 - اطلع على ما يفعله طفلك على شبكة الإنترنت

إذا كنت تستخدم جهازاً شخصياً، قم بضبط أدوات الرقابة الأبوية على جهاز طفلك ليتوجب عليه الحصول على إذن منك قبل تنزيل أي شيء، أو إجراء عمليات شراء. تحقق من الإعدادات المتوفرة على التطبيقات شائعة الاستخدام مثل لعبة فورتنايت، التي توفر لك خيار حظر المحادثات داخل اللعبة. تعرف إلى حسابات وسائل التواصل الاجتماعي التي

يستخدمها طفلك وافهمها جيداً. يجب عليك التعرف إلى جهات الاتصال الخاصة به، والمحادثات التي يجريها. تحدث إلى طفلك عن الانفتاح الذي تتسم به شبكة الإنترنت، وعن قدرة أي شخص على نشر أي شيء على هذه الشبكة، وكيفية التعرف إلى المعلومات المغلوطة.

2 - انتبه لأي سلوك مشبوه على تطبيقات مؤتمرات الفيديو

«الخطر المرتبط بالغرباء» ينطبق على العالم الافتراضي كما ينطبق على العالم المادي. وجّه طفلك ليقوم بمغادرة أي اجتماع يتضمن أي سلوك مشبوه لا يمكن قبوله في الحياة الواقعية، مثل انضمام مشاركين مجهولين، أو مشاركة من لم يتم الإعلان عنهم مسبقاً.

3 - وضّح لأطفالك أهمية كلمات المرور القوية

كلمة المرور هي بمثابة مفتاح المنزل، فهو يحمي كل شيء داخل منزلك، وأنت بحاجة إلى إبقائه آمناً طوال الوقت، احفظه من الغرباء، ومن الأصدقاء أيضاً. كما أن المفاتيح المختلفة تفتح أبواباً مختلفة، فمن تقع عليه مسؤولية حماية المعلومات في المنزل، يجب أن يستخدم كلمات مرور متنوعة للأجهزة الشخصية المختلفة والحسابات التي تتطلب من المستخدم استخدام كلمات المرور الخاصة به. تطبيقات إدارة كلمات المرور تشبه سلاسل المفاتيح على نحو كبير، فهي عبارة عن تطبيقات تجمع كلمات المرور معاً، وتحافظ عليها وتسهّل عملية استخدامها. يجب أن يتمتع الوالدان هنا بحق الوصول إلى كلمات مرور أطفالهم، وتطبيقات إدارتها أيضاً.

4 - راقب ما يقوم به طفلك

تأكد من أن وضعيّة شاشة طفلك تسمح لك بمراقبة نشاطاته باستمرار. استخدم خلفية افتراضية عند فتح الكاميرا للتعلم عن بعد إن أمكن، ويمكن لهذا أن يساعد في تعزيز حماية الخصوصية والتركيز على العملية التعليمية في المقام الأول.

تحدث إلى أطفالك حول مخاطر النقر فوق الروابط التي تحتوي على عروض خادعة، والتي تُصمم بشكل جيد جداً بحيث يمكن تصديقها. بدلاً من ذلك، يجب على الأطفال سؤال أحد الوالدين قبل قيامهم بالنقر على مثل هذه العروض. وبمجرد حصولهم على الإذن - وعندها فقط - يجب عليهم فتح صفحة جديدة في المتصفح والانتقال إلى الموقع مباشرة.

5 - لا تكشف أكثر مما يجب

ضع حدوداً لما يمكن لطفلك نشره عبر شبكة الإنترنت، مثل منعه من نشر صور للوجوه أو مواقع يسهل التعرف إليها، أو أية معلومات شخصية مثل الاسم الكامل ومعلومات الاتصال، واسم المدرسة وما إلى ذلك. قم بتغيير إعدادات جهازك لإيقاف تشغيل البيانات الوصفية في تطبيقات الكاميرا. يساعد ذلك على ضمان عدم تمكن الغرباء من معرفة مكانك من الصور التي تنشرها على شبكة الإنترنت.

6 - تحديث أنظمة التشغيل في أجهزتك باستمرار

احرص دائماً على تمتع أجهزتك بآخر التحديثات المتوفرة. يمكن لهذه التحديثات أن تتضمن أدوات الحماية اللازمة للحفاظ على أمان عائلتك.