CYBER THREATS AT HOME

How to keep kids safe while they're learning online

Paul Haskell-Dowland and Ismini Vasileiou

Before COVID-19, children would spend a lot of the day at school. There they would be taught about Internet safety and be protected when going online by systems that filter or restrict access to online content.

Schools provide protective environments to restrict access to content such as pornography and gambling. They also protect children from various threats such as viruses and unmoderated social media.

This is usually done using filters and blacklists (lists of websites or other resources that aren't allowed) applied to school devices or through the school Internet connection.

But with many children learning from home, parents may not be aware of the need for the same safeguards. Many parents are also working from home, which may limit the time to explore and set up a secure online environment for their children.

So, what threats are children exposed to and what can parents do to keep them safe?

WHAT THREATS MIGHT CHILDREN FACE?

With increased use of web-based tools, downloading new applications and dependence on email, children could be exposed to malware threats in the absence of school-based controls.

This can include viruses and ransomware — for example, CovidLock (an application offering coronavirus related information) that targets the Android operating system and changes the PIN code for the lock-screen. If infected, the user can lose complete access to her device.

Children working at home are not usually protected by filters provided by their schools. Seemingly innocent teaching activities like the use of YouTube can expose children to unexpected risks given the breadth of inappropriate adult content available.

Most videos end with links to a number of related resources, the selection of which is not controlled by th school. Even using YouTube Kids, a subset of curated YouTube content filtered for appropriateness, has some risks. There have been reports of content featuring violence, suicidal themes and sexual references.

Many schools are using video conferencing tools to maintain social interaction with students. There have been reports of cases of class-hijacking, including Zoom-bombing where uninvited guests enter the video conference session.

The FBI Boston field office has documented inappropriate comments and imagery introduced into an online class. A similar case in Connecticut resulted in a teenager being arrested after Zoom-bombing incidents. Because video conferencing is becoming normalised, malicious actors (including paedophiles) may seek to exploit this level of familiarity. They can persuade children to engage in actions that can escalat to inappropriate sexual behaviour. The eSafety Office reported a significant increase in a range of incidents online harm since early March.

In a particularly sickening example, eSafety Office investigators said: in one forum, paedophiles noted tha isolation measures have increased opportunities to con children remotely and engage in their "passion" for sexual abuse via platforms such as YouTube, Instagran and random webchat services.

Some families may be using older or borrowed devi if there aren't enough for their children to use. These devices may not offer the same level of protection aga common Internet threats (such as viruses) as they may longer be supported by the vendor (such as Microsoft Apple) and be missing vital updates.

They may also be unable to run the latest protectiv software (such as antivirus) due to incompatibilities or simply being under-powered.

WHAT CAN PARENTS DO TO PROTECT CHILDREN?

It's worth speaking with the school management to determine what safeguards may still function while away from the school campus.

Some solutions operate at device-level rather than based on their location, so it is possible standard protections will still be applicable at home.

Some devices support filters and controls natively. For example, many Apple devices offer ScreenTime controls to limit access to apps and websites and apply time limits to device use (recent Android devices might have the Digital Wellbeing feature with similar capabilities).

Traditional mechanisms like firewalls and anti-virus tools are still essential on laptops and desktop systems. It is important these are not just installed and forgotten. Just like the operating systems, they need to be regularly updated.

There is a wealth of advice available to support children using technology at home. The Australian eSafety Commissioner's website, for instance, provides access to:

- An online safety booklet for children under five
- Advice on parental controls such as setting up filters on the home Internet
- An online safety guide for young people
- Specific advice on the "big issues" such as cyberbullying and unwanted contact or grooming
- Global safety advice to help parents deal with online abuse.

But if you're feeling overwhelmed by these materials, some key messages include:

- Ensuring (where appropriate) the device is regularly updated. This can include updating the operating system such as Windows, Android or Mac
- Using appropriate antivirus software (and ensuring it is also kept up-to-date)
- Applying parental controls to limit screen time, specific app use (blocking or limiting use), or specific website blocks (such as blocking access to YouTube)
- On some devices, parental controls can limit use of the camera and microphone to prevent external communication
- Applying age restrictions to media content and websites (the Communications Alliance has a list of accredited family friendly filters)
- Monitoring your child's use of apps or web browsing activities
- When installing apps for children, checking online and talking to other parents about them
- Configuring web browsers to use "safe search"
- Ensuring children use devices in sight of parents
- Talking to your children about online behaviour.

While technology can play a part, ensuring children work in an environment where there is (at least periodic) oversight by parents is still an important factor.

(Paul Haskell-Dowland is associate dean (computing and security), Edith Cowan University and Ismini Vasileiou is associate professor in information systems, De Montfort University)