Keep out!

Criminals are finding increasingly sophisticated ways to get you and your family to part with personal details or cash online. **Ann-Marie Corvin** describes their methods, and how you can stop them

Phishing

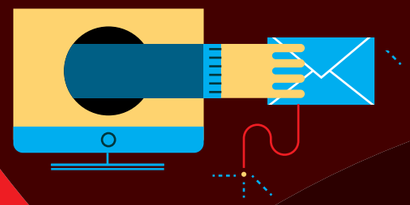
This involves fake emails asking for your security information and personal details. They are usually highly tempting (often appearing to be from official sources, offering tax rebates or 'special' student grants), or highly convincing, from a large company you may have an account with (because so many people do).

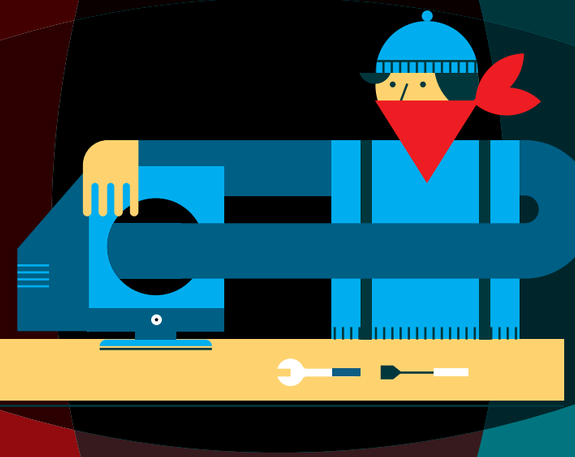
This will often be in the form of a bill you weren't expecting and ask for your bank details and/or account passwords. In 2016, for example, a convincing email was sent to teenagers who were about to start university – so even young people can be targeted.

Remember, no bank or institution will contact you by email and ask you to enter all your personal and financial details online.

What you can do

If you receive a message like this, delete it. If you are worried about an outstanding invoice email, contact the relevant company through their websites, but never through the contact links sent in the email.





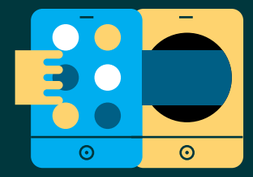
Clickjacking

This is a malicious technique frequently found on social media. The links are designed to be highly clickable, luring you in with an amazing offer or fake sensationalist celebrity gossip.

Once you click on the link, they will generally take you through to other sites, asking you for personal information. Once activated, these links may download malware or ransomware, allowing criminals to take over your device.

What you can do

Warn your child to be careful what they click on. With clickjacking links, there is often something suspicious if you look closely – like a spelling mistake or a logo that isn't quite right. An offer that is too good to be true often is. If it doesn't seem right, don't click on it.



Ratting

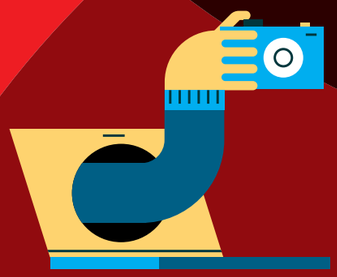
'Peeping Tom' hackers fool users into downloading a piece of software on to their computer called a Remote Access Trojan (RAT), which then takes over their webcam. Phishing emails or clickjack links – often aimed at teens – are common techniques for spreading them. Some have been spread by downloading online games.

Once criminals have access to the webcam, they can start spying on and filming the device's user. Victims can then be blackmailed, or images can be auctioned on the Dark Web.

What you can do

Ensure your family computer's firewall is switched on and install security software that offers malware and spyware protection on all your family's devices.

Advise your child to download games from reputable sites only. Think carefully about leaving webcam-enabled devices in bedrooms and private areas, or follow the Pope's example: he was pictured with a sticker covering the camera on his iPad.



Cyber attacks

Large corporations and institutions, including the NHS, have fallen prey to hackers unleashing malicious ransomware programmes that lock companies or individuals out of their computers until a ransom has been paid. (Although, even then, you may never recover your files.) Two years ago, a well-known educational toymaker was also hacked by criminals, resulting in parents' and children's data being stolen.

What you can do

Ransomware attacks prey on the vulnerability of machines running unsupported older operating systems.

Protect your family at home by running operating system and security updates as soon as you are notified about them, using firewalls and anti-virus software, and by being cautious when opening emails.

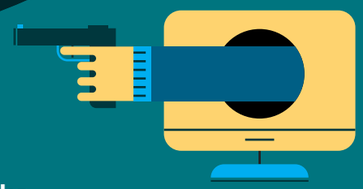


Illustration: Romualdo Faura

Passwords

Be unique

Teach your child to create strong, unique passwords for each device and service they use – games, social media, forums. The same goes for internet-enabled toys. Many use Bluetooth and have pre-set passwords that are easily hackable, such as 0000 or 1234. Change these as a matter of course.

Selfish is good

Tell them not to share their passwords with anyone.

Use 'passphrases', not passwords

Longer passwords are difficult to remember. So, create a 'passphrase' using three random words together.

Complicate things

Symbols, numbers, and combinations of upper and lower case can also be used for added security.

Further information
Get Safe Online:
www.getsafeonline.org