At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

What you need to know about... PHISHING

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What is it?

'Phishing'

Phishing is a form of cyber-attack where victims are targeted in the form of spoof emails, phone calls or texts. These are commonly carried out by an attacker posing as someone else to influence individuals into giving out sensitive data such as payment details and passwords. Phishing usually takes place via email, where the attacker manipulates a message to make it appear to be from someone else, therefore deceiving the victim into doing as they say. Hackers try to deceive you into downloading malicious code and will aim to extract small pieces of information at a time.

Know the Risks

Loss of personal data

If a young person has been the victim of a successful phishing attempt, hackers may gain access to their personal data and destroy/corrupt it. Some hackers may ask for a ransom in order to get files back, whilst others may simply destroy it or even publish it on the dark web.

Targeted phishing

If a hacker can trick children with a phishing attack, the chances are that they'll be back for more. They may begin asking for 'harmless' information, then move on to sensitive information such as passwords and entry codes. Many phishing attacks start with the attacker offering to help the victim with a common problem to build enough trust to ask for information such as passwords.

Hidden entry

If an attacker manages to successfully execute a phishing attack on a victim, they have essentially found a 'way in', or backdoor into their online security. Even if they do not notice any changes, the hacker may be monitoring/controlling their computer without their knowledge.

Safety Tips

Backup your files

Always create a backup of your files to an external hard drive or USB before any potential damage or destruction. If you regularly perform backups, you may only have to backup any files recently added/updated since the last backup.

Disconnect the device

If you think a child has been a target of a phishing attempt, firstly disconnect the device from the network by switching off the Wi-Fi in settings or unplugging the ethernet cable. Alternatively find the router and unplug it. This will prevent any malware from accessing any internet services.

Scan your system

Always perform regular and full malware scans; this will check for any potentially harmful programs installed on your computer. Scans are most effective when the antivirus is up to date so it's crucial to keep on top of the latest security downloads.

Check official websites

If you're unsure about a message you receive, don't click any links or follow any instructions. Check the official websites online and don't give out any personal information that you don't need to. Even if the message seems like it's from someone you know, if anything seems suspicious, or matches any of the criteria above, simply do not open it...

Look out for...

Suspicious URLs

Sometimes links and attachments aren't always what they appear to be and could send you to a site completely different to what was expected. Hovering over a hyperlink will display the actual website. Some links are shortened, so the actual website address is hidden behind a generic link, such as goo.gl/7fh28. Never click shortened URLs.

Odd sense of urgency

Cyber criminals will put fear in their victim's mind in an attempt to push them into giving away personal information. They may act as if they're trying to help create a false sense of 'trust' or pressure users into giving information 'before it's too late'.

'Too good to be true'

If you receive an email saying you've 'Won a new phone' or a 'Holiday Abroad', it is likely to be a phishing email. Hackers engineer emails and trick targets into believing they've won something, as it puts a false sense of trust towards the hacker.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.