CYBER SECURITY BUZZWORDS

CHEAT SHEET

Do you know your phishing from your smishing? Or the difference between malvertising and malspam? Cyber security terms can be confusing so keep this cheat sheet handy to help build your cyber resilience.

Online Safety Shareable by SAFER SCHOOLS NI saferschoolsni.co.uk

Common Cyber Security Terms

Authentication
The process of identifying a user's identity, making sure that they can have permission to access a particular system and/or files.

Firewall
Any technology used to keep intruders out. This could be software or hardware that aims to block unwanted internet traffic.

Spoofing
This is when a hacker changes the IP address of an email so that it appears to come from a trusted source.

Spyware
A form of malware used by hackers with the aim of spying on you and capturing your computer activities.

Cyber resilience
Understanding when you are at risk online and having policies and procedures in place to mitigate against these threats.

Hacker
Any person who attempts to gain unauthorized access to a system with the intent to cause mischief, damage, or theft.

Trojan Horse
A malware that disguises itself as something innocent (e.g. an online game) but allows a hacker access to your computer.

Virus (Malware)
Changes, corrupts, or destroys information and passes it to other systems. In some cases, a virus can cause physical damage to a device.

Phishing Terms

Phishing attacks are the most common form of cyber attack in the UK

Phishing
The use of 'real' or authentic looking messages and emails pretending to be someone or something else to gain access to your personal information and/or account details.

Spear phishing
A highly targeted phishing attack. While both scams use email to reach their victim, spear phishing involves sending customised emails to a specific individual.

Vishing
The use of phone calls or voice messages in phishing schemes. Criminals can use voice over technology to change or alter their voice, appearing more convincing to the victim.

Whaling
Attacks targeted at a senior executive, and usually don't contain a link but are looking for a 'favour' from a more junior employee e.g. buying gift cards for staff members.

Smishing
Similar to Phishing this scam looks authentic and attempts to gain access to personal information but instead of an email it uses SMS text messages.

Ransomware terms

Reports of ransomware attacks have more than doubled since 2020

Ransomware
Also known as ransom malware, is a type of malware that prevents users from accessing their system, account or personal files and demands a 'ransom' payment in order for them to regain access to their systems.

Malvertising
Also known as malicious advertising is the use of online advertising to distribute malware. This can take the form of pop up adverts. When clicked, a web page may be 'infected' and send the user's data to criminal servers.

Malspam
Also known as Malicious spam, may use the same tactics as phishing schemes, with one MAJOR difference – the link may lead to a malicious site with attachments which if clicked, will trigger malware to begin downloading.

Top Tips for Being Cyber Resilient

- Do not click any suspicious links – this includes any from accounts you may know or recognise.
- Report scams to the appropriate authorities.
- Create a strong password and review it regularly.
- Remember to back up and update your device often.
- Regularly scan your devices for viruses or malware.
- If you aren't sure or don't know the sender, don't reply.
- Don't enter or give your personal information, account details or card details on login sites you are sent to via links.
- Pay attention to misspellings or grammatical errors in official messages/ emails – this is usually an indicator.
- Always ignore accounts representing companies, organisations or public figures who are not verified.
- Never send money to anyone in order to 'receive a gift, prize or winnings'.

Version: 1.0.0 - Published 21/10/22