Jargon buster

Fraud and cyber terms you need to know

- **Anti-Virus** – a computer program used to prevent, detect and sometimes remove malicious software.
- **Bring Your Own Device (BYOD)** – a policy implemented by businesses that allows an employee to use their own personal electronic devices for work purposes.
- **Common Vulnerabilities and Exposures (CVE)** – a publicly available list of known security vulnerabilities, indexed with unique ID numbers, descriptions and references.
- **Cryptocurrency** – peer-to-peer decentralised, digital currencies that are traded like a commodity.
- **Cyber-attack** – malicious targeting of computer systems, networks, infrastructures or devices.
- **Cyber incident** – defined by the National Cyber Security Centre (NCSC) as a 'breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)'.
- **Dark web** – the portion of the internet that isn't indexed by a search engine and is only accessed with special permissions or software.
- **Digital footprint** – a trail of data left behind after internet use. This can include passive information such as stored cookies, or information that's been actively placed on the internet, such as social media posts.
- **Encryption** – the process of mathematically scrambling data. This data can be encrypted at rest, like data saved to a hard drive, or in transit, like data sent via HTTPS between your web browser and your bank's server. Encrypting data doesn't make it invisible to malicious cyber actors; it simply converts it into useless, unintelligible gibberish.
- **Firewall** – a network security system that monitors and controls incoming and outgoing network traffic based on a set of rules.
- **Hacker** – a person engaged in a wide range of computer network exploitation (CNE). 'Black hat' hackers generally conduct malicious CNE, whereas 'white hat' hackers conduct CNE for the benefit of cyber defences.
- **Malware** – an umbrella term for a wide variety of malicious code designed to accomplish nefarious goals such as providing remote access, loading or dropping additional malware, stealing bank information, encrypting and denying access to data, or hijacking a device's computing power.
- **Patching** – process of updating an existing software or hardware to fix known bugs and vulnerabilities.
- **Penetration testing (pen testing)** – a process used by organisations to probe their own security with tactics used by cyber threat actors, usually conducted by 'red teams' or teams of professional white hat hackers.

- **Phishing** – usually conducted via email, this is a message designed to trick the recipient in to disclosing sensitive information, click a malicious link and/or open a malicious attachment. Phishing is often used to establish initial access on a device or network.
- **Ransomware** – a type of malicious software that blocks or otherwise restricts access to data under the promise that the restriction will be removed once a ransom has been paid.
- **Smishing** – a phishing message via SMS/text message.
- **Social engineering** – the manipulation of people to perform an action, usually to disclose personal information.
- **Spear phishing** – a phishing message that has been directed to a specific person or select group of people.
- **Trojan** – malware disguised as a seemingly innocent file or program in an effort to convince a potential victim that it can be opened safely. Trojans are very common and are frequently delivered via phishing emails or loaded by other malware called 'loaders'.
- **Two-factor authentication (2FA)** – a process of authentication where a user is required to have two factors, such as a known password and a one-time passcode (OTP). Generally, these factors are categorised as something you know (a password), something you are (a fingerprint), or something you have (a key card).
- **Virtual Private Networks (VPN)** – allow for secure private connections over public infrastructure, originally developed for use by organisations to authenticate the employee to internal network resources like email servers or shared folders. Today, consumer VPNs are increasingly used by individuals to create encrypted connections to a VPN server of their choice and use that server to connect to other internet resources.
- **Vishing** – a phishing attempt via phone call with a heavy use of social engineering.
- **Zero-day vulnerability** – a vulnerability identified prior to a patch or update being issued. Malware that exploits such a vulnerability is commonly referred to as a zero-day exploit.