FACT SHEET
FOR PRACTITIONERS

AGES 11-14

This factsheet is designed to help you to better understand some of the risks and issues associated with cyber threats and harms. It gives an overview of some of the risks and will support you in delivering the content to young people.

Definitions

- **Adware** - Causes pop-ups or windows that will not close.
- **Blagging** - When someone makes up a story to gain a person's interest and engage them in communication.
- **Cyber security** - The means by which individuals and organisations reduce the risk of being affected by cyber crime. Cyber security's core function is to protect devices (smartphones, laptops, tablets and computers), and services from theft or damage. It's also about preventing unauthorised access to the personal information stored on devices and online.
- **Cyber crime** – Cyber crime can take different forms; it can include things like phishing scams or malware.
- **Cyber threat** - Malicious attempts to damage or disrupt devices, services and networks, and the information on them.
- **Hacking** – Gaining unauthorised access to data in a system or computer. Hacking is not always malicious, but it is mainly associated with criminal activity.
- **Malware** - Derived from 'malicious software', malware includes viruses, trojans, worms or any code or content that can damage computer systems, networks or devices.
- **Password manager** - A password manager is an app on someone's phone, tablet or computer that stores passwords, so the user doesn't need to remember them. Once someone is logged into the password manager using a 'master' password, it will generate and remember passwords for all their online accounts. Many password managers can also enter passwords into websites and apps automatically, so there is no need to type them in with each log in.
- **Patching** - Applying updates to devices or software to improve security and/or enhance functionality.
- **Personal data** - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- **Pharming** – When a user is redirected from a genuine website to a fake one.
- **Phishing** - Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
- **Ransomware** – A type of malware that makes data or systems unusable until the target makes a payment.
- **Shouldering/shoulder surfing** – Looking at someone's information over their shoulder, for example whilst they are entering a pin.
- **Smishing – Phishing via SMS** – text messages are sent to users, asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.
- **Social engineering** – The tactic of manipulating, influencing, or deceiving someone in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- **Spear-phishing** – A targeted form of phishing, where the email is designed to look like it is from a person the recipient knows and/or trusts.
- **Spyware** – Collects the activity on a computer system without the user knowing.
- **Trojans** – Malware that appears legitimate but isn't.
- **2-Step Verification (2SV)** – Also known as two-factor authentication (2FA) or multi-factor authentication (MFA), 2SV helps to keep cyber criminals out of accounts, even if they know the passwords. When someone sets up 2-Step Verification, they'll be asked to input a second piece of unique information, such as a PIN or code, often sent by SMS or email.
- **Viruses** – Malware that infects a computer
- **Vishing –** Phishing via voice message – phone calls or voice messages purporting to be from reputable companies in order to persuade individuals to reveal sensitive personal information (e.g. bank details).
- **Whaling** – Highly targeted phishing attacks (which look like legitimate emails) that are aimed at senior executives.

FACT SHEET
FOR PRACTITIONERS

AGES 11-14

What are some of the risks and harms for young people?

Young people (aged 20-29) are more at risk of becoming targets of cyber-dependent crime, particularly through social media and email hacking. This is because internet and social media use is higher among this age group. It is likely that teenagers are also frequent targets of social media and email hackings, but this is not reflected in reporting because they are less likely to report to law enforcement.

Technical ability appears to have little effect on becoming a target of cyber-dependent crime. Targets of cyber-dependent crime often know how to use their devices, but not know how to better protect their accounts (for example with strong passwords and 2SV). Young people, in particular, can be reluctant to act upon advice when given to them by law enforcement. Without a change in the attitudes towards cyber security, it is expected that young people and teenagers will continue to be the most common targets of cyber-dependent crime.

The greatest harm caused by cyber-dependent crime is psychological, rather than financial. The psychological effect of cyber-dependent crime depends on a number of factors. For example, those who present with anxiety or other mental health conditions are more vulnerable to the psychological impact of cyber-dependent crime.

In social media hacking, hackers will adjust their language based upon the age and gender of the person being targeted and their contacts. Social media account hackings that threaten to publish intimate images or attempt to elicit them from targets cause the greatest psychological harm. Young females are at the greatest risk of such cyber incidents.

Individuals involved in an abusive relationship are vulnerable to cyber-dependent crime perpetrated by their abuser. Tactics such as monitoring or impersonating the target online are common features of domestic abusers' controlling behaviour. Acts of financial and emotional abuse often have a cyber element, such as monitoring email or social media, or accessing bank accounts. Targets in abusive relationships are particularly prone to repeated experiences of cyber-dependent crime. Indeed, when they try to physically distance themselves from their abuser, the abuser may use cyber techniques to prolong their abuse.

These resources contain key messages to help children and young people stay cyber secure. This includes making sure they have effective passwords, turning on 2SV where available, ensuring they keep devices up to date and supporting them to manage any suspicious online contact. The materials will help students to better protect themselves against cyber threats.

Below are some key questions with answers to help you to deliver the materials.

For more information visit https://www.ncsc.gov.uk

What are the best ways to stay cyber secure?

The NCSC has the following top tips for staying safe online:

- Protect email accounts by using a strong password, which is different from the password used on any other account. Cyber criminals can use email accounts to access other personal accounts and commit identity theft.
- Install the latest software and app updates. These contain vital security updates to help protect devices from cyber criminals.
- Turn on 2-Step Verification (2SV) to help protect online accounts. This means that a password, code, or sometimes finger-print is needed to access an account, in addition to a password.
- Use password managers. Some browsers incorporate a password manager, which help to create unique, strong passwords across different accounts. It can also store them securely.
- Back up your data. Important data, such as photos and key documents, can be kept safe by backing them up to an external hard drive or a cloud-based storage system.
- Create strong passwords that are hard to crack. The NCSC recommends creating passwords using three random words (more details below).

FACT SHEET
FOR PRACTITIONERS

AGES 11-14

Why are effective passwords so important?

Passwords to access online accounts should be really strong, and should not be used anywhere else. This is especially true for the password for email accounts. If the same password is used across different accounts, cyber criminals only need one password to access all of those accounts.

It is important to always use a strong and separate password for an email account; that is, a password that isn't used for any other accounts, either at home or at work.

Once a criminal can access an email account, they could:

- access private information, including banking details
- post emails and messages pretending to be from the account holder (and use this to trick other people)
- reset other account passwords and get access to other online accounts

Having a strong and separate password for an email account means that if cyber criminals steal the password for a less-important account, they can't use it to access an email account. The NCSC encourages people to use password managers, which can create strong passwords and remember them.

If an email password has been re-used across other accounts, the email password should be changed as soon as possible. It should be strong and different to all other accounts.

Ideally, unique passwords should be used for all important online accounts (such as banking accounts, shopping/payment accounts and social media accounts), not just for an email account. Additional protection can also be provided by setting up 2-Step Verification (2SV) for email accounts, which will prevent a criminal from accessing an email account, even if they know the password.

www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

How can a strong password be created?

Weak passwords can be cracked in seconds. The longer and more unusual a password is, the harder it is for a cyber criminal to crack.

A good way to make a password difficult to crack is by combining three random words to create a single password (for example applenemobiro). Alternatively, a password manager could be used, which can create strong passwords (and remember them).

It is important to avoid the most common passwords that criminals can easily guess (like 'password'). It is also best to avoid creating passwords from significant dates (like birthdays, or a loved one's birthday), or from favourite sports teams or pet names. Most of these details can be found within someone's social media profile.

Changing certain characters in a password (so swapping the letter 'o' with a zero, for example) is not effective - cyber criminals know these tricks as well. So this approach won't make a password significantly stronger, but it will be harder to remember.

Why does the NCSC recommend using 'three random words' as a way to create passwords?

A password that's made up of three random words will be 'strong enough' to keep criminals out of an account, but easy enough to remember.

Longstanding advice around making passwords very complex (full of random characters, symbols and numbers, for example) is not helpful. This is because memorising lots of complex passwords is almost impossible.

Passwords generated from three random words are 'long enough' and 'strong enough' for most purposes, but can also be remembered much more easily. Passwords could be written down if needed, provided they are kept somewhere safe.

www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words

FACT SHEET
FOR PRACTITIONERS

AGES 11-14

Why is it important to update devices?

Updates should be applied to apps and device software as soon as they are available. Updates include protection from viruses and other kinds of malware, and will often include improvements and new features.

Prompts to update devices or apps shouldn't be ignored. Applying these updates is one of the most important (and quickest) things someone can do to keep safe online.

It is also a good idea to turn on 'automatic updates' in a device's settings, if available, to avoid the need to remember to run updates.

Why should phishing scams be reported?

Reporting a scam is free and only takes a minute. By reporting phishing attempts, someone can:

- reduce the amount of scam communications they receive
- make themselves a harder target for scammers
- protect others from cyber crime online

How can phishing scams be reported?

- Phishing scams can be reported to the NCSC: https://www.ncsc.gov.uk/collection/phishing-scams
- Scam emails can be forwarded to report@phishing.gov.uk, where the NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately.
- Scam text messages can be forwarded on too. Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.
- Scam websites can be reported through an online form on the NCSC website: https://www.ncsc.gov.uk/section/about-this-website/report-scam-website
- Scam adverts can be reported via an online form to the Advertising Standards Authority and more information is available at: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-advert

National Cyber Security Centre
a part of GCHQ