Alcester Academy

Online Safety Bulletin—December 2024

Welcome to this term's online safety bulletin. During safer internet day this year, pupils are going to learn about how to spot, respond to, and report different types of scams online. This term's online safety bulletin follows this theme and will outline how to avoid online scams, and will provide essential tips on how to safeguard your personal information.

Scams can take many forms, and may target anyone, including young people. In today's digital age, online scams have become increasingly sophisticated. It's crucial to stay informed and take proactive measures to protect yourself and your loved ones from cyber threats.

Common Online Scams

Some common online scams include the following;

- **Phishing:**

  Phishing is a cybercrime where attackers use fraudulent emails, text messages, phone calls, or websites to trick individuals into revealing sensitive information, downloading malware, or exposing themselves to other cyber threats.

  Phishing involves attackers creating fake messages or websites that appear to be from legitimate sources such as banks, social media sites, or government agencies. The messages often contain urgent requests, enticing offers, or warnings to create a sense of urgency or fear.

  Victims are lured into clicking malicious links, downloading attachments, or providing personal information like passwords, credit card numbers, or social security numbers. Once the victim falls for the trap, the attackers gain access to their sensitive information, which can be used for identity theft, financial fraud, or further cyberattacks.

- **Smishing:**

  Similar to phishing, but uses text messages to lure victims. This can include receiving text messages that claim to be from a delivery service, asking you to confirm your address by clicking a link.

- **Vishing:**

  Scammers use voice calls to deceive individuals into divulging personal information asking for personal information to avoid penalties.

- **Phishing Websites & Online Shopping Scams:**

  This can involve encountering fake websites that mimic legitimate ones, tricking you into entering your login credentials. Other examples include

fraudulent online stores that may sell counterfeit goods or take your money without delivering products.

- **Social Engineering:**

  Criminals know exactly what buttons to push to get what they want. It does not matter if this is in person on your doorstep, in your social media feeds, or in games being played online. These psychological tactics (which are given the term 'social engineering') are used to encourage you to act fast without having time to stop and think. Common examples include creating a false sense of urgency if something is scarce or in short supply, playing on your emotions, or trying to build relationships by asking lots of questions or making references to aspects of your life that may have been learnt from looking at your online profiles.

Warning signs to watch out for

If you receive one of these types of requests, it should be a warning sign. Take time to stop, think and check if it is real. Be wary if anyone:

- Asks you to share a one-time passcode
- Asks for your PIN or password in full
- Asks for payment before sending a prize or lost delivery
- Asks for a direct transfer of funds
- Asks you to move away from an official payment site to make a direct payment
- Asks you to click on any suspicious links

How to Protect Yourself

- **Be Vigilant:** Don't click on links or download attachments from unknown senders or suspicious emails. Be cautious of unsolicited calls or text messages, especially those asking for personal information. Avoid deals that seem too good to be true, they generally are! If you are unsure of who has sent you a link, hover over it to check the actual website address (the URL), and look for suspicious addresses, or phone numbers.
- **Strong Passwords:** Create strong, unique passwords for each online account, a reliable method is to combine three or four random words to create a password. Another method is to use a reliable password manager to securely store your passwords.
- **Secure Wi-Fi:** Avoid accessing sensitive information on public Wi-Fi networks, and use a strong password for your home Wi-Fi network.
- **Online Shopping Safety:** Only shop on reputable websites with secure payment gateways. This is shown by a padlock symbol before the website address (URL). Use credit cards for online purchases, as they offer better fraud protection.
- **Software Updates:** Keep your operating system and software up-to-date with the latest security patches and updates.
- **Two-Factor Authentication (2FA):** Enable 2FA for your online accounts to add an extra layer of security. 2FA can usually be found in the security settings of your accounts, and is available for most major online services, such as email, banking, and social media.

2FA doubles your defence against cyber criminals by asking for more information to prove your identity when you log in to your online accounts.

- **Beware of social engineering tactics:** Criminals use psychological tactics to get you to act fast without having time to stop and think.

Where to get help

If you know someone who has been the victim on a scam, online help is available. You can report fraud and cyber crime online to Action Fraud (https://www.actionfraud.police.uk/) or by telephoning 0300 123 2040. You may also be able to report via social media if the scam has occurred there, or to another relevant organisation such as your bank if you think your account may be at risk.

- **Educate Yourself:** Stay informed about the latest online scams and security threats.
- **Report Scams:** Report scams to the appropriate authorities to help prevent others from falling victim.
- **Trust Your Instincts:** If something feels suspicious, it probably is.

By following these guidelines, you can significantly reduce your risk of falling victim to online scams.

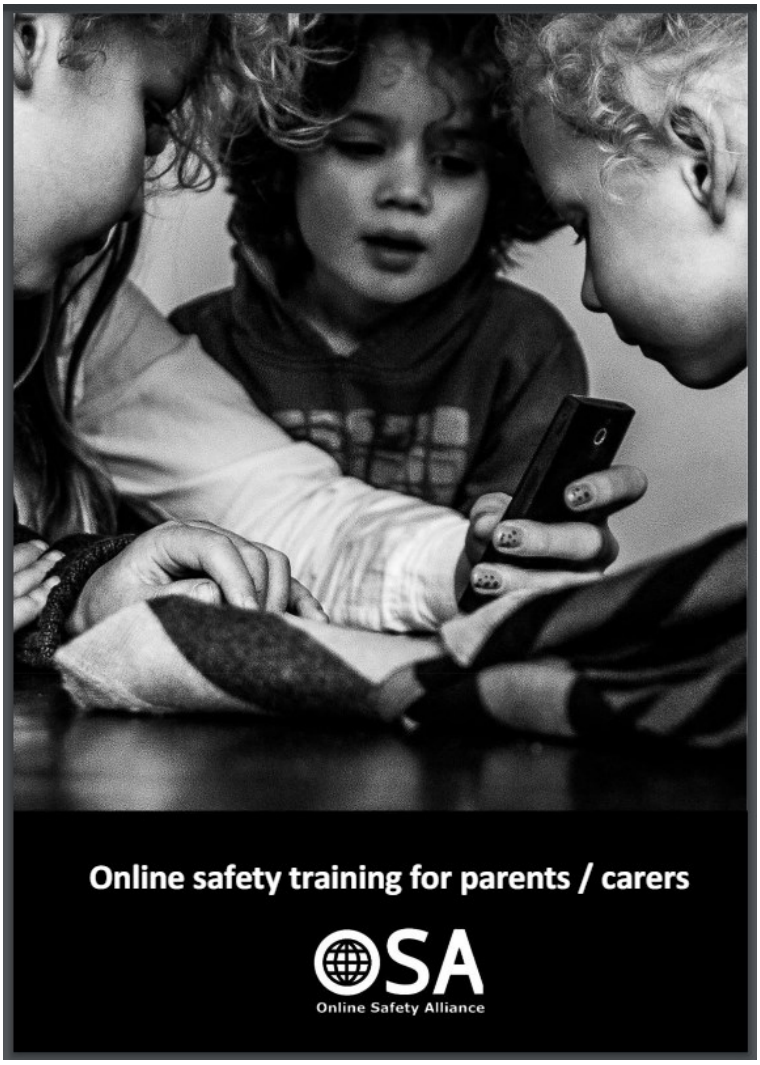
Other Useful Online Safety Links

- National Online Safety Centre (NOSC): https://nationalcollege.com/categories/online-safety
- UK Safer Internet Centre: https://saferinternet.org.uk/
- NSPCC Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- Internet Matters: www.internetmatters.org

Together, we can create a safe and positive online experience for our children.

If you have any immediate concerns, please do not hesitate to contact the school safeguarding team.

Thank you for your support.



Details from the Online Safety Alliance about its parental online courses can be found at:

https://www.onlinesafetyalliance.org/