Dataspire
Creating ICT confidence for schools

Cybersecurity Cheatsheet

We know that the subject of Cybersecurity can be a bit of a minefield, so we've created this cheatsheet with a few hints and tips to help you along the way.

How to stay secure online

PASSWORDS

- Avoid obvious passwords that are easy to guess, e.g. **123456**
- Don't use passwords that can be guessed by your personal information e.g. **date of birth**
- Use a series of at least three unrelated words, as it's harder to crack, e.g. **AnimalNumberFruit**
- Add in some special characters, numbers, upper and lowercase and try to use a minimum of10 characters. e.g. **An!m@lNumb3rFru!t**
- Ideally, use a password manager to generate secure passwords and remember your logins
- Use two-factor authentication to make it more difficult for someone to access your account
- Never share your password with anyone, no matter who claims to be asking for it
- Don't write your passwords down, or at least not anywhere obviously accessible
- Change your passwords regularly to protect against data leaks
- Never use the same password twice, they should always be unique and unrelated

WEB BROWSING

- If you don't recognize or aren't expecting a link, don't click on it
- Check the address bar to ensure you're on the website that you think you are
- Is the website using a secure **HTTPS** connection? If not, there's a greater risk of data interception
- Avoid adverts disguised as fake download links. If you're uncertain, don't click.
- The dark web is full of scams and illegal activity, so avoid it
- Only download information from trusted providers and even then, scan the files with anti-virus software

SOCIAL MEDIA

- Everything you put online is permanent, so only share what you're comfortable with
- Regularly review your social media privacy settings. The apps often make changes within updates, which can include changes to your privacy settings.
- Never let anyone else use your social media account and never log in on a public computer
- Remain vigilant - If something sounds too good to be true, it usually is.
- Do not overshare. You don't know who's looking at your information or what they're doing with it.
- Only share the information of those who have consented. Are you sure you should share pictures of your children? "Sharenting"

EMAIL

- Check the sender's email address, not just the name. The email sender can be spoofed so the email might not be from whom it claims to be.
- Don't recognize the sender? Not expecting that email? Don't open it - delete it.
- If an email asks you to click a link or open an attachment that seems suspicious, trust your instincts and delete it
- If you're being asked to share sensitive information, don't do it. E.g. your bank, Amazon etc. will never ask for this information via email.
- If someone is trying to impose a sense of urgency on you to do something, it's probably a scam.
- That long-lost relative who has died and wants to leave you a bundle of money? It's fake. Delete the email.
- Don't assume everything in your inbox is safe. Your spam filter offers great protection, but it isn't foolproof and cybercriminals are finding new ways to scam every day.

ANTIVIRUS

- Every system is susceptible to viruses, but some more than others
- Avoid dodgy downloads and opening unknown email attachments, as viruses are often spread this way
- The ultimate, nuclear way to clean a virus from your system is to completely wipe everything

SOFTWARE

- Keep all the software on your computer up-to-date to patch vulnerabilities and enjoy the latest features
- Install operating system updates as they come through, especially critical security ones
- If you no longer need the software, uninstall it completely
- Don't install random browser extensions, and only use those from trusted publishers

MOBILE

- When you install apps, check what permissions they ask for. Be mindful of camera, microphone and location access.
- Only install apps from authorised app stores, and even then, you should still be cautious
- Don't send and receive sensitive data over public Wi-Fi connections
- Protect your device with a PIN, pattern, fingerprint, or some type of security lock
- Follow the same precautions you do on your computer e.g. avoiding dodgy sites and downloads
- Keep your phone on you whenever possible as this also protects against SIM card swapping

DATA

- Encrypt private data and don't share the encryption key with anyone else
- External drives can easily be physically stolen, so be cautious about what you store on them
- If you're done with a computer or external drive, investigate how to securely wipe it as simply deleting the data isn't enough. (Dataspire can arrange wiping and recycling)
- If you buy a used computer, factory reset it and wipe it completely from top to bottom
- Backup your data: at least three copies, on two different types of media, with one off-site

If you would like to strengthen your school's cyber-defence, the team at Dataspire is here to help.

Simply contact us on 0345 603 1233 or email info@dataspire.co.uk for more details.