Live My Digital Parental Guide

Privacy & Security

What is private information?

Private information is information that can be discovered online, which reveals your identity. For your child, this could be anything from the school they attend to their date of birth to the names of family members.

Today, so much gets shared online about who we are, what we're doing and where we're going that it's important that your child is aware that oversharing can have repercussions, especially if private information gets into the wrong hands.

41%

of teenagers have been targeted by fraudsters

Why it's important to be secure online?

When personal information does get into the wrong hands, it can be used for a number of security breaches, from identity theft to viruses to online grooming.

Often we aren't aware when private information is visible to others. For example, it could be that an app that you're using has been disclosing where you are without you knowing that you had enabled it to access your location.

How online scams occur

There are a number of ways online scams can take place. Some of the most common ways people fall victim of cybercrimes are via:

Phishing scams which happen when someone tries to access private information such as passwords or credit card details online by pretending to be a trustworthy entity such as a bank

Insecure websites that may compromise your security by not having basic security measurements in place or by failing to store passwords properly

Having weak passwords which are easy for criminals to hack into (such as "password1"). This enables them to easily access your online accounts

Spyware traps which gather information about you without your knowledge, for example when you create a profile on an insecure website. This information could be shared without your permission or used to control your computer

Viruses which are programmes or pieces of code that damage your device. It could become infected with a virus by simply clicking on a link that says "You've won an iPad!"

Sharing private information as mentioned above

Live My Digital has been created by the Girls' Day School Trust in partnership with Digital Awareness UK to empower families to use social media safely and responsibly together.

The 12-part video series, which can be accessed at www.livemy.digital, is designed to inspire young people to want to use technology responsibly and empower parents to be part of the learning process.

Girls' Day School Trust

DIGITAL AWARENESS UK

Jargon Buster

Malware:
Malicious software, such as a virus or spyware which could cause damage to your device

Trojan:
A type of malware that usually pretends to be legitimate software

Firewall:
A security system designed to prevent unauthorised access to or from a private network

Antivirus:
A programme that protects your device from malicious code, which could damage it

Hacker:
Someone who exploits weaknesses in a security system

Hacktivism:
The act of hacking into computer systems for politically or socially motivated reasons like free speech or human rights

Cookie:
Information that a website stores on your device in order to recall that information at a later dat

What to do to prevent your child from security scams

Talk to them about the dangers of using the internet unsafely, giving examples such as those outlined above how easy it can be to become a victim of a security scam

Strong passwords should always be encouraged to prevent people from hacking into your child's online accounts

Anti virus software should be activated on the devices your child uses to protect them from harmful software

Privacy settings on your child's online accounts should be set to a standard you're both happy with, to ensure cyber criminals or strangers can't see the things they post online

Private information such as your child's home address, the school they go to, or their location should not be disclosed to people they don't trust. Remind them of the importance of not sharing this information

Suspicious links should be avoided at all times. Your child must be aware that they may infect their devices with a virus just by clicking on a link that says "free downloads"

Secure websites usually have a padlock symbol in the address bar and a web address starting with https://. If your child is aware of that it may help them to think twice before sharing private information such as card details on a website when paying for something

Looking after their tech is important, remind your child that leaving their devices unattended or forgetting to log out of their online profiles could leave them open to security breaches

Where to go for further information

There are some fantastic resources available to parents online that offer tips and advice on how to manage privacy and security-related issues. We're recommend the following:

www.childline.org.uk
www.nspcc.org.uk
www.thinkuknow.co.uk
www.internetmatters.org
www.vodafone.com/content/parents
www.saferinternet.org.uk
www.childnet.com