THEME OF THE MONTH
FEBRUARY 2024

ONLINE SAFETY

Staying safe online

With the increasing use of the internet and technology it has become important that individuals have the appropriate knowledge and skills to be able to keep themselves safe online.

Every minute we are creating more data about ourselves on line.

- Twitter (X) users send 456,000 tweets
- Google conducts 3,607,080 searches
- Wikipedia users publish 600 new page edits
- Instagram users post 46,740 photos
- Snapchat users share 527,760 photos

We have created this booklet to help individuals of any age to understand the hidden dangers and risks of the internet and consider how consent works in an on line context. This essential knowledge will ensure that you are aware how to ensure your data is secure and allow you to protect yourself online.

Main rules for staying safe online

- Don't give out any personal information including your password. address or telephone number.

- Don't send pictures of yourself to someone that you wouldn't want to be shared online.

- Don't open emails or attachments from someone you don't know.

- Never arrange to meet someone who you have met online.

- If you have a problem with something you have seen on read online, tell someone.

- Don't make friends with people on line if you don't know them.

- If you would not give your consent in person then don't give it online either.

Online consent

When we are on line we must ensure how our actions can impact ourselves and others. We should always make sure that we have consent from others before posting or sharing something online etc ..

Consent is specific permission for something to happen or an agreement to do something.

Online consent can be seen differently to offline consent. We may be more likely to give consent on line as it could give us a better experience by clicking agree. Sharing our photos and experiences online is also fun to gain likes and comments. however this might be something you wouldn't usually share with people offline. Without realising we all may have different expectations and online behaviours compared to being offline.

If you would not give consent in person then don't give it online either. Photos and comments can spread much quicker in the online world.

Discuss with your relatives and friends about what they are happy with you to share about them on line.

Only use websites on line that give you choices about your consent and make sure to read any conditions before clicking agree.

Consider everyone's feelings before doing anything online. Consent is also needed from strangers. not just people you know offline.

Email safety

Email is a great communication tool for both individuals and businesses. However, it is sometimes used to send unwanted content and possibly harm computers and the user. This can include Spam (junk email), Phishing and Viruses.

SPAM

Unwanted bulk messages, especially advertising.

Spot Spam Emails:

- You don't know the sender
- Contains spelling errors
- Contains a virus warning
- Offer is too good to be true
- Contains attachments (exe. file)

PHISHING

The act of attempting to acquire sensitive information.

Spot Phishing Emails:

- Not a trusted email address
- Does not use your proper name
- A sense of urgency to act
- Personal information request
- The email wasn't expected

VIRUSES

Programs that may be harmful to your computer.

Spot Virus Emails:

- Links to a third party website
- Contains attachments
- Unknown senders
- Must be a legitimate email address
- Spelling and grammar errors

Top 10 internet safety rules

Keep personal information professional

Potential employers or customers don’t need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn’t hand purely personal information out to strangers individually - don’t hand it out to millions of people online.

Keep your privacy settings on

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. Both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

Practice safe browsing

You wouldn’t choose to walk through a dangerous neighbourhood—don’t visit dangerous neighbourhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware.
By resisting the urge, you don’t even give the hackers a chance.

Be careful what you download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Don’t download apps that look suspicious or come from a site you don’t trust.

Be careful who you meet online

People you meet online are not always who they claim to be. They may not even be real. Fake social media profiles are a popular way for hackers to gain trust with unwary web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

Make sure your internet connection is secure

When you go online in a public place, for example by using a public WiFi connection, you have no direct control over its security. Corporate cybersecurity experts worry about “endpoints”—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you’re able to connect to a secure WiFi network) before providing information such as your bank account number. To further improve your Internet browsing safety, use secure VPN connection (virtual private network). VPN enables you to have a secure connection between your device and an Internet server that no one can monitor or access the data that you’re exchanging.

Use strong passwords

Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don’t forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

Make online purchases from secure sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. You can identify secure sites by looking for an address that starts with https: (the S stands for secure) rather than simply http: They may also be marked by a padlock icon next to the address bar.

Be careful what you post

Any comment or image you post online may stay online forever because removing the original (say, from Facebook) does not remove any copies that other people made. There is no way for you to “take back” a remark you wish you hadn’t made, or get rid of that embarrassing selfie you took at a party. Don’t put anything online that you wouldn’t want your family or a prospective employer to see.

Keep your antivirus program up to date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it’s to date. Be sure to stay current with your operating system’s updates and updates to applications you use. They provide a vital layer of security.

Protecting your identity

- **Use secure passwords:** A strong password should be more than eight characters in length. and contain both capital letters and at least one numeric or other non alphabetical character.

- **Be cautious when sharing personal information:** Don’t give out any information on the phone or over the internet unless you’ve initiated the contact.

- **Check your privacy settings:** Be sure to check your personal settings regularly and make adjustments as needed. Not all content uploaded is hidden from other users.

- **Know who your friends are:** Do not accept any random friend requests. Keep your personal profile private. only giving your real friends access to view your content.

Don’t forget to sign out of your personal accounts.

Don’t believe everything you read online.

Don’t open emails from people you don’t know.

Be mindful of your reputation online.

Additional information

Ensuring online safety is crucial in today's digital age. Here are some resources specifically focused on online safety:

National Cyber Security Centre (NCSC):
Website: NCSC
The NCSC is a key authority on cybersecurity in the UK, providing comprehensive guidance and resources for individuals, businesses, and organizations to enhance their online security.

Get Safe Online:
Website: Get Safe Online
Get Safe Online is a government-backed initiative offering practical advice to help individuals and businesses protect themselves from various online threats, including fraud, identity theft, and cybercrime.

Internet Matters:
Website: Internet Matters
Internet Matters focuses on providing information and resources for parents and caregivers to ensure the online safety of children. It covers topics such as setting up parental controls and managing online risks.

UK Safer Internet Centre:
Website: UK Safer Internet Centre
This center offers a range of resources for schools, parents, and professionals, promoting safer internet use. They also coordinate Safer Internet Day and provide valuable insights into online safety issues.

Thinkuknow:
Website: Thinkuknow
Thinkuknow, run by the National Crime Agency's CEOP Command, focuses on educating children, parents, and teachers about online safety. It provides age-appropriate resources and guidance to help individuals stay safe in the digital world.

LSP's Safeguarding & Mental Health First Aider Teams

If you have any concerns at all, please don't hesitate to contact a member of our Safeguarding or Mental Health teams. You can find the contact details here.

MORE INFORMATION

www.learningskillspartnership.com
info@learningskillspartnership.com