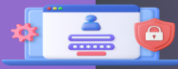


Digital Safety At Work

Digital Safety At Home

Digital Safety In Public

5 CYBERSECURITY TIPS FOR EMPLOYEES IN THE WORKPLACE



Password Strength

- Use complex passwords with a mix of letters, numbers, and symbols.
- Change passwords regularly, at least every 90 days.



Phishing Awareness

- Be cautious of unsolicited emails or messages.
- Verify the sender's identity before clicking on any links or downloading attachments.
- Report suspicious emails to the IT department.



Software Updates

- Keep your operating system and software up to date.
- Regularly install security patches and updates.
- Enable automatic updates whenever possible.



Two-Factor Authentication (2FA)

- Enable 2FA wherever available (email, apps, accounts).
- Adds an extra layer of security beyond just a password.



Safe Internet Usage

- Avoid using public Wi-Fi for work-related tasks.
- Use a VPN when accessing company resources remotely.
- Don't share sensitive information online unless it's secure.

Work from Home: Cyber Security Tips



LEARN ABOUT YOUR COMPANY'S WORK FROM HOME POLICIES

Before you start working from home, make sure that you're familiar with your company's guidelines for cybersecurity at home.



INVEST IN A DEDICATED DEVICE FOR WORK

Get a separate laptop, tablet, or even a smartphone. This will help to keep your personal data separate from your work data, which will make it easier to protect both.



SECURE YOUR WI-FI NETWORK

Use a strong password. Use WPA/WPA2 security. Enable MAC filtering. The last thing you want is for someone to be able to access your work data or devices.



BEWARE OF PHISHING ATTACKS

To protect yourself from phishing attacks, you should never click on links or open attachments from unknown sources.



LOCK AND ENABLE TRACKING ON YOUR WORK DEVICES

It's important to lock your work devices when you're not using them. This will help to prevent anyone from accessing your data if your device is lost or stolen.



REGULARLY BACK UP IMPORTANT DATA

In the event that your work device is lost or stolen, or if it becomes infected with malware, you'll want to have a backup of your important data.



USE AN AUTHENTICATOR APP

Authenticator apps generate one-time codes that you can use to log in, even if someone has your password.



KEEP YOUR SOFTWARE AND OPERATING SYSTEM UP TO DATE

Vulnerabilities in software and operating systems made public, might let hackers exploit them to gain access to devices and data.

DO YOU REALLY KNOW..

..HOW TO USE PUBLIC WI-FI SAFELY?



Whether it's in a cafe, hotel room, or one of the many other places they're available, public wi-fi hotspots are a quick and easy way to get online when you're out and about. However, unlike your wi-fi at home, not all public hotspots are password protected, which means anyone can connect to them. Even the hackers! Hackers use unsecured connections like this to infect your device with malware, steal your online usernames and passwords, access files on your computer, as well as steal your financial details.

76%

Of people with mobile subscriptions still use public wi-fi.

64%

Of people that use public wi-fi, do so at cafes and bars.

28 B

Every year, the public spends more than 28 billion minutes using public wi-fi.

BEHAVIOURS THAT PUT YOU AT RISK.



Installing any system or application updates on your mobile phone or computer whilst using public wi-fi.

Accessing your emails, social networks, online shopping or banking services whilst on public wi-fi.

Configuring your devices to connect to unknown wi-fi networks without prompting you first.

HOW TO USE PUBLIC WI-FI SAFELY..



Exercise caution and always verify with the provider that you are logging on to the correct wi-fi network.

When using public wi-fi, always use a trusted VPN service in order to secure your traffic.

Raise any concerns or suspicions with the manager of the organisation, or the police.

Whenever possible, use mobile data services, like 4G, in preference to public wi-fi.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Get Safe Online
Free expert advice

CITY OF LONDON POLICE
Metropolitan Police Service
Metropolitan Police Training Centre

Digital Skills

Digital skills encompass a wide range of abilities related to using technology effectively. These can include proficiency in software applications, programming languages, data analysis, digital communication, cybersecurity, and more. Digital skills are increasingly important in today's technology-driven world for both personal and professional success.

DIGITAL SKILLS

Information / data literacy



- Browsing, searching and filtering data, information and digital content
- Evaluating data, information and digital content
- Managing data, information and digital content

Communication and collaboration



- Interacting via ICT
- Sharing via ICT
- Engaging in citizenship via ICT
- Collaborating via ICT
- Netiquette
- Managing digital identity

Digital content creation



- Developing digital content
- Integrating and re-elaborating digital content
- Copyright and licences
- Programming

Safety



- Protecting devices
- Protecting personal data and privacy
- Protecting health and well-being
- Protecting the environment

Problem solving



- Solving technical problems
- Identifying needs and technological responses
- Creatively using digital technologies
- Identifying digital competence gaps