

BASIC DIGITAL SAFETY

1 DIGITAL SAFETY AT WORK

1 Use of Strong Passwords and Multi-Factor Authentication (MFA): Employees are required to create strong, unique passwords for accessing company systems. Additionally, multi-factor authentication (MFA) is enforced to provide an extra layer of security, such as a verification code sent to the employee's phone or email.

2 Regular Software Updates and Patch Management: The IT department ensures that all software, including operating systems and applications, are up to date with the latest security patches. This helps protect the company's systems from vulnerabilities that cybercriminals could exploit.

3 Data Encryption: Sensitive company data (e.g., financial records, employee personal information) is encrypted both in transit and at rest. This ensures that even if data is intercepted or accessed unauthorized

2

DIGITAL SAFETY AT INTERNET

1 secure Wi-Fi Networks: Ensure your home Wi-Fi network is secured with a strong password, and avoid using public Wi-Fi for activities like online banking. If using public Wi-Fi, always use a Virtual Private Network (VPN) to encrypt your internet traffic and protect your privacy.

2 Use Antivirus and Anti-Malware Software: Installing and regularly updating antivirus software can help detect and remove harmful software, like viruses or malware, that could compromise your device and data.

3 Update Software and Devices Regularly: Keep all software, including web browsers and operating systems, up to date. Security patches and updates protect devices from vulnerabilities that cybercriminals could exploit.

3 DIGITAL SAFETY AT PUBLIC

1 Turn Off Sharing Settings: Public spaces often have devices or services that allow you to share your location or files with nearby devices. Ensure that file sharing, Bluetooth, and location services are turned off when not in use to prevent unauthorized access to your device.

2 Avoid Public Charging Stations (Juice Jacking): Public USB charging stations can be used by hackers to install malware on your device or steal data. It's safer to use your own charging adapter and plug into a wall outlet, or use a portable charger.

3 Log Out of Accounts After Use: After accessing sensitive information or accounts in a public space, always log out from all accounts, especially on shared or public computers. This prevents others from gaining access to your private data.



DIGITAL SAFETY AT HOME

1 Change the default username and password for your home Wi-Fi router. Use WPA3 or WPA2 encryption to secure your Wi-Fi network. Create a strong, unique Wi-Fi password and avoid using easily guessable information.

2 Ensure your devices have firewall protection enabled to monitor and block any unauthorized access to your network.

A router firewall adds an extra layer of protection to prevent external attacks.



DIGITAL SKILLS

University of Wales Trinity Saint Davis

Denis Cebotari

ID: 2410494