

Class: Digital Skills LCLM4002
Lecturer: Hoang Nguyen Dang
Name: HERMINIA DABO
Student Number: 2332184
Date: 02/08/2024



Basic Digital Safety

Due to the social connections people make on the various platforms, security and safety in the work place have become crucial in the digital world. There is an increase in cyber threats, and it is crucial to secure information belonging to the company and its employees.

Here are some essential tips for maintaining basic digital safety in the workplace:

Strong Passwords

It is essential to choose different, complex passwords for all the accounts used in work activities. Do not use basic names like password, date of birth or your name as your passwords. Instead, develop complex passphrases of a dozen characters or more with upper and lowercase letters, numbers, and symbols like "CorrectHorseBatteryStaple!" It is recommended to use a password manager like LastPass or 1Password to create and safely store strong passwords.

Two-Factor Authentication

On your work-related accounts, always try enabling the two-factor or even the multi-factor sign in process whenever possible. This provides a second level of authentication, where, for instance, you enter your password and then a code that you get on your mobile device. This makes it difficult for intruders to gain unauthorized access to your accounts even if they come across your password. Almost all the workplace platforms such as Office 365, G Suite, and Salesforce have two-factor authentication options.

Be Wary of Phishing

Class: Digital Skills LCLM4002
Lecturer: Hoang Nguyen Dang
Name: HERMINIA DABO
Student Number: 2332184
Date: 02/08/2024



Phishing, where the attacker seeks to make the victim divulge certain information or download a malicious program, is one of the biggest dangers. Avoid clicking links in emails, texts, or messages that ask for any personal information or login details even if they seem to come from your superior or the company IT department. If you have any doubts concerning the legitimacy of a message, try to call the sender using the number that you have on your company's dialing list.

Secure Your Devices

Make sure all devices, including computers, mobile phones, and tablets that belong to work are secure. Ensure that the software and operating systems are updated with the latest security updates and use a good antivirus/anti-malware software like Malwarebytes or Norton. Always keep your devices within your sight when in a public area and be careful to avoid exposing client information or financial information to others.

Careful with Public Wi-Fi

Do not use public or open Wi-Fi networks when working with business information. Cybercriminals can easily breach the security of public Wi-Fi hotspots and get hold of your details. If you need to connect to public Wi-Fi, use VPN to encrypt your connection, including NordVPN or ExpressVPN.

Secure File Sharing

For sharing of confidential data, it is recommended to use organizational approved methods for instance, encrypted emails, Organization digital drives including OneDrive or Google Drive or file sharing services like Box or Dropbox. Specific do not use personal email and consumer grade file sharing application for business purposes.

Class: Digital Skills LCLM4002
Lecturer: Hoang Nguyen Dang
Name: HERMINIA DABO
Student Number: 2332184
Date: 02/08/2024



Regular Backups

For work documents, back up often to improve data security, either by using on an online backup service like Google Drive or Dropbox or an external hard drive, for example, WD My Passport or Seagate Backup Plus. This will improve on ways of protecting your information in case of a breach, system failure or any other disaster.

Security Awareness Training

Complete any security awareness training that may be provided for employees by your organization. These sessions can give the knowledge of new threats, some guidelines for safer use of Internet, and correct actions if such threat would be faced, so you can be a wiser and a more careful worker in the company.

Class: Digital Skills LCLM4002
Lecturer: Hoang Nguyen Dang
Name: HERMINIA DABO
Student Number: 2332184
Date: 02/08/2024

BASIC DIGITAL SAFETY

Due to the social connections people make on the various platforms, security and safety in the work place have become crucial in the digital world. There is an increase in cyber threats, and it is crucial to secure information belonging to the company and its employees.

Here are some essential tips for maintaining basic digital safety in the workplace:

Strong Passwords

It is essential to choose different, complex passwords for all the accounts used in work activities. Do not use basic names like password, date of birth or your name as your passwords. Instead, develop complex passphrases of a dozen characters or more with upper and lowercase letters, numbers, and symbols like "CorrectHorseBatteryStaple!" It is recommended to use a password manager like LastPass or 1Password to create and safely store strong passwords.

Two-Factor Authentication

On your work-related accounts, always try enabling the two-factor or even the multi-factor sign in process whenever possible. This provides a second level of authentication, where, for instance, you enter your password and then a code that you get on your mobile device. This makes it difficult for intruders to gain unauthorized access to your accounts even if they come across your password. Almost all the workplace platforms such as Office 365, G Suite, and Salesforce have two-factor authentication options.

Be Wary of Phishing

Phishing, where the attacker seeks to make the victim divulge certain information or download a malicious program, is one of the biggest dangers. Avoid clicking links in emails, texts, or messages that ask for any personal information or login details even if they seem to come from your superior or the company IT department. If you have any doubts concerning the legitimacy of a message, try to call the sender using the number that you have on your company's dialing list.

Secure Your Devices

Make sure all devices, including computers, mobile phones, and tablets that belong to work are secure. Ensure that the software and operating systems are updated with the latest security updates and use a good antivirus/anti-malware software like Malwarebytes or Norton. Always keep your devices within your sight when in a public area and be careful to avoid exposing client information or financial information to others.

Careful with Public Wi-Fi

Do not use public or open Wi-Fi networks when working with business information. Cybercriminals can easily breach the security of public Wi-Fi hotspots and get hold of your details. If you need to connect to public Wi-Fi, use VPN to encrypt your connection, including NordVPN or ExpressVPN.



Secure File Sharing

For sharing of confidential data, it is recommended to use organizational approved methods for instance, encrypted emails, Organization digital drives including OneDrive or Google Drive or file sharing services like Box or Dropbox. Specific do not use personal email and consumer grade file sharing application for business purposes.

Regular Backups

For work documents, back up often to improve data security, either by using on an online backup service like Google Drive or Dropbox or an external hard drive, for example, WD My Passport or Seagate Backup Plus. This will improve on ways of protecting your information in case of a breach, system failure or any other disaster.

Security Awareness Training

Complete any security awareness training that may be provided for employees by your organization. These sessions can give the knowledge of new threats, some guidelines for safer use of Internet, and correct actions if such threat would be faced, so you can be a wiser and a more careful worker in the company.