Wayne State University
IT Security Awareness
Quick Reference

Protect Your Data

Losing University data could result in financial and reputational damages. Keep your data away from unauthorized access by:

• **Maintaining** an inventory of the different kinds and types of data you work with.
• **Deleting** old data and records that are no longer needed.
• **Being aware** of the WSU Confidential Information Policy.
• **Encrypting** sensitive information such as SSNs with software like BitLocker or AxCrypt.
• **Restricting** the recipients of your data to only those with legitimate business needs.
• **Locking** your computer and your work area when you are not around.
• **Securing** your mobile devices by using a passcode, device locking, and remote tracking.

Safeguard Your Credentials

Your AccessID and Password are the keys to the kingdom, as well as your data. Keep attackers out of your accounts by:

• **Using** strong passwords that include uppercase and lowercase characters, numbers, and special symbols.
• **RefRAINING** from using dictionary words.
• **Changing** your passwords at least twice a year.
• **Managing** your passwords using a password manager that you trust, such as KeePass.
• **Creating** a password scheme.
• **Connecting** to “WSU-SECURE” for your on-campus Wi-Fi network access.
• **Never sharing** your password with anyone.
• **Never saving** passwords in your web browser.
• **Never reusing** passwords between systems.

Identify Fraudulent Emails

Fraudulent or “phishing” emails are very popular and successful ways attackers can compromise your computer. Eliminate this threat by:

• **Opening** attachments only when you expect them and they are from a person you trust.
• **Watching** for poor grammar, capitalization, or abnormal writing styles.
• **Never sending** your password via email.
• **Hovering** over email links before you click them.
• **Checking websites** for a padlock symbol and green text before logging in.
• **Confirming** thru secondary means suspicious messages.
• **Deleting** messages you know are malicious.
• **Reporting** new phishing attacks using the Wayne Connect Zimlet.

Combat Malicious Software

Malware can be sophisticated, difficult to remove, and is used to gather your data and take over your computer. Keep malware away by:

• **Knowing** malware can arrive via USB sticks, email, and web browsing.
• **Keeping** the software on your desktops, laptops, and servers up to date.
• **Watching** what you click in emails and websites.
• **Browsing** trusted websites only.
• **Running** antivirus software on your computer.
• **Asking** your IT support staff to install software for you.
• **Contacting** your IT support staff if you think you may be infected.

Information Security is everyone’s responsibility.
Report possible breaches and suspicious activity to the C&IT Helpdesk. helpdesk@wayne.edu or (313) 577-4778
Security Exercise: Create a Data Inventory
Brainstorm and create a listing of the different types of data that your area handles.

Security Exercise: Create an Account Listing
Brainstorm and create a listing of the different systems and services that you have an online account for. Don't list your credentials!

NOTES
Jot down any additional notes or questions you may have.

Find additional tips, tricks, and security information at https://security.wayne.edu.