IT SERVICES

CYBERSECURITY INTRODUCTION

Ronise C. Zenon
ITS – Security

cybersecurity.ucsd.edu
Cybersecurity is a set of principles and practices designed to safeguard computing assets and online information against threats.
WHY THIS MATTERS

As an end-user, you are the last line of defense and have these responsibilities:

- Avoid risky behavior online
- Safely manage your passphrase
- Safely manage your email account
- Secure your computer
- Protect the data you handle
- Avoid risky behavior online – yes again!
Avoid Risky Behavior Online

- Be cautious when browsing the web; misspellings can direct you to undesired websites
- Be cautious when handling attachments and links in chatrooms or instant messages (IM)
- Avoid responding to questions or clicking links in pop-up windows

Image source: Symantec Threat Report 2017
Safely Manage Your Passphrase

- Create and maintain a strong passphrase
  - Manage with LastPass
- Do not share your passphrase with anyone
- Do not reuse the same passphrase for multiple accounts and when changing
- Do not store your passphrase where others can see it, or electronically in an unencrypted format
- Do not use automatic login functionality
Safely Manage Your Email Account

- Send all university business correspondence from an official UC San Diego email address
- Be wary of email phishing scams
  - Avoid opening attachments and/or clicking links in email from untrusted sources
  - Avoid providing any credentials or other confidential information in email

Image source: Symantec Threat Report 2017
Secure your computer

- Lock your computer when not attended
- Log off or shutdown when going home
- Patch and update your operating system
- Install and update anti-virus and anti-malware security definitions
- Enable pop-up blocker in your web browser
- Make an informed and rational decision prior to installing or downloading software

Image source: Symantec Threat Report 2017
Protect the data you handle

- Know which types of data are stored on your computer
  - What do you think should be kept private?
- Segregate your personal files from business files
- Back up your data regularly
- Use secure file storage (option may depend on unit)
  - network drives
  - Google Drive for Business (G Drive)
  - OneDrive

In the last 8 years more than 7.1 billion identities have been exposed in data breaches
Avoid Risky Behavior
Online – yes, again!

"spyware" bugs (AKA trojanware, snoopware and trespassware) are stealthy stand-alone programs potentially capable of
• secretly monitoring your keystrokes
• snooping your computer files/applications
• reading your browser cookies
• changing your default homepage
• logging all the websites you visit
Resources

- cybersecurity.ucsd.edu
- https://security.ucop.edu/resources/security-awareness/index.html
- https://security.ucop.edu/resources/security-awareness/new-school-year.html
- https://its.ucsc.edu/security/pii-training.html
- https://its.ucsc.edu/security/restricted.html
- http://er.educause.edu/blogs/2015/10/youre-an-important-piece-of-the-puzzle
IT SERVICES

Ronise C. Zenon
IT Policy Coordinator
IT Services – Security
ronise@ucsd.edu
858.534.8421
cybersecurity.ucsd.edu
IT SERVICES
its.ucsd.edu