

Cyber Security Awareness

دور أمن المعلومات لتجنب الهجمات السيبرانية
على البيانات الشخصية في المؤسسات التعليمية

Presented to:

PHILADELPHIA UNIVERSITY



Monday 3rd of Oct. 2022



The Presenter

- Lecturer @ Information Security and Cybersecurity Department
- Manage Philadelphia Cyber Centre
- Certified as
 - CEI | Certified EC-Council Instructor
 - CEH | Certified Ethical Hacking
 - ECSA | EC-Council Certified Security Analyst
 - CCNP | Cisco Certified Network Professional
 - MCSE | Microsoft Certified System Engineer



Ahmad Musleh

Session Agenda

- ▶ Education cares about cyber security awareness
- ▶ Cyber security awareness controls the threat
- ▶ Permissions and OS security settings/accounts
- ▶ Physical security and environmental controls
- ▶ Performance considerations for efficient use of laptops
- ▶ Security Devices, software, and terms
- ▶ Cyber Attacks
- ▶ Incident Preparedness and Management Planning
- ▶ Q&A

Education cares about cyber security awareness

- ▶ Official Statistics | Educational institutions findings annex - Cyber Security Breaches Survey 2022, Updated 11 July 2022
 - ▶ <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022>

- ▶ **Cybersecurity for Higher Education Institutes: Impact & Solutions**, Date: 5 April 2022
 - ▶ <https://www.cm-alliance.com/cybersecurity-blog/cybersecurity-for-higher-education-institutes-impact-solutions>

Permissions and OS security settings/accounts

Make changes to normal_user's account

- [Change the account name](#)
- [Change the password](#)
- [Change the account type](#)
- [Delete the account](#)
- [Manage another account](#)



normal_user
Local Account
Password protected

transport Properties

General | Sharing | Security | Previous Versions | Customize

Object name: E:\Program Files (x86)\Microsoft Azure Site Recovery

Group or user names:

- SYSTEM
- Administrators (SRTesting\Administrators)
- Users (SRTesting\Users)

To change permissions, click Edit. [Edit...](#)

Permissions for Users	Allow	Deny
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced. [Advanced](#)

OK Cancel Apply

Advanced Security Settings for transport

Name: E:\Program Files (x86)\Microsoft Azure Site Recovery\home\svsystems\transport

Owner: Administrators (SRTesting\Administrators) [Change](#)

Permissions | Auditing | Effective Access

domain, you can also evaluate the impact of potential additions to the security token for the account. When you add a group, any group that the intended group is a member of must be added separately.

User/ Group: normal_user (SRTesting\normal_user) [Select a user](#)

[View effective access](#)

Effective access	Permission	Access limited by
✗	Full control	File Permissions
👤	Traverse folder / execute file	
👤	List folder / read data	
👤	Read attributes	
👤	Read extended attributes	
👤	Create files / write data	
👤	Create folders / append data	
✗	Write attributes	File Permissions

Physical security and environmental controls

- ▶ Entry Controls
- ▶ Secure Work Areas
 - Clear Your Desk
 - Copiers and Printers
 - Fax Snooping
 - Shared Meeting Areas



Physical Security: Entry Controls

- ▶ Gates and Doors: Don't allow others to gain entrance to a secure or restricted location without using their own badge, access card or key code - this is known as tailgating or piggy-backing.
- ▶ Badges: Never leave your ID badge or access card unguarded.
- ▶ Visitors:
 - Visitors should be checked-in and escorted at all times
 - Visitors should not be allowed to use cameras or recording equipment without special permission
 - If a visitor requests Internet access, ensure he or she is only given limited guest access.

Physical Security: Secure Work Areas

- ▶ Clear your desk:
 - When leaving your desk, make sure all papers, removable media, and other items containing sensitive information are cleared from your desk and locked away.
 - Make sure to log off of or lock your computer to ensure it cannot be accessed when you are away
- ▶ Copiers and Printers:
 - Modern copiers and printers have hard drives and store every document ever copied or printed. Data from these devices should be digitally wiped clean before they are disposed.

Physical Security: Secure Work Areas

- ▶ Fax snooping:

- Malicious insiders might try to steal information by intercepting inbound faxes. Be sure to be at a fax machine before sending sensitive data to it.

- ▶ Shared meeting areas:

- Shared meeting areas should be kept free of sensitive information. Erase whiteboards, take all documents with you, and be careful of what you throw in the trash.

Performance considerations

.. for efficient use of laptops

- ▶ Avoid Opening many heavy applications with many browsing pages (chrome) at the same time which affects on CPU and RAM. (You should close any unused services).
- ▶ Avoid Keeping your devices on for many long time (days) without restart or shut them down; otherwise it leads to crush some programs and services.
- ▶ Generally, do not keep multiple programs open if not needed
- ▶ Perform a disk cleanup periodically; e.g. every Thursday

Managing folders and file in your local machine

- ▶ Managing the capacity of c:/ drive
- ▶ Default saving of downloads to be on any other drive other than the drive that has the operating system
- ▶ Upon project completion, upload files fully to the drive and permanently delete the files from the device

Working with applications in a tuned and compatible way

- ▶ When you have multiple Adobe or heavy apps open, do not open multiple Chrome tabs; just the email would do. Youtube and such consumes the RAM and Cache for a while
- ▶ Do not share attachments over Microsoft Teams. It will significantly slow down computers and consume storage

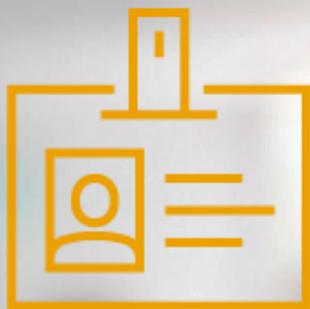
- ▶ Saving files on the smaller disk causes it to fill up, slowing down the computer and causing saving and crashing issues.
- ▶ Keeping numerous files and applications open while working on large files
- ▶ Keeping numerous files and applications open while working on large files
- ▶ Microsoft teams are significantly slowing down computers
- ▶ Opening a large number of tabs in Google Chrome
- ▶ Not cleaning up disks
- ▶ Keeping numerous files and applications open while working on large files
- ▶ Not turning off the pcs for a long while
- ▶ Not updating newer versions of Windows on a regular basis



Inform

- ▶ If you do not have an Antivirus
- ▶ If your Adobe version is not 2021, your MS Apps are not the 365 version
- ▶ If you do not have the following plug-ins: Flipping Tool, ToolsToo, Thinkcell
- ▶ If your machine needs Windows Activation





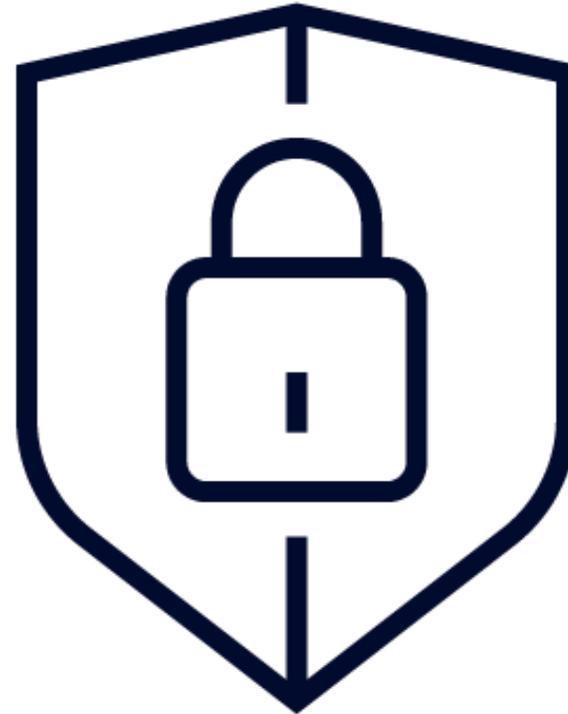
**What is Information security,
privacy and personal information?**

What is Information security?

- ▶ Information security encompasses all the ways we protect our information from unauthorized access, modification, destruction, or other forms of attack.
- ▶ It is how we defend our computer systems and our valuable information in both digital and hardcopy format, which is critical to our organization's success.

What is privacy?

- ▶ Privacy works alongside information security by ensuring **personal information** is collected, used and disclosed appropriately.
- ▶ Having robust information security and privacy programs helps our company maintain the trust of our employees, customers, and general public.



PHI\$HING SEAMS
90% OF HACKS

75% OF THE ENTIRE POPULATION
ONLINE BY 2022

6B ONLINE BY PEOPLE

50% MORE SMARTPHONES LARGEST THREAT VECTOR



WEAKEST LINK

COST: \$12.5B (SOURCE: FBI)



SECURITY AWARENESS FOR EMPLOYEES

RANSOMWARE ATTACK EVERY :14 SECONDS IN 2019

SPONSORED BY: aware GO



FAST · CLEAR · ENTERTAINING · MEMORABLE!

THE WORLD'S EMPLOYEES TO BE CYBERSAFE



RESEARCH BY CYBERSECURITY VENTURES

CYBERSECURITYVENTURES.COM

Network & Infrastructure Security

Advanced Threat Protection

Network & Infrastructure Security

Network Firewall

Deception

NAC

SDN

DDoS Protection

DNS Security

Network Analysis & Forensics

Web Security

Web Security

ICS + OT

Network Analysis & Forensics

Endpoint Security

Endpoint Security

Endpoint Prevention

Endpoint Detection & Response

Application Security

Application Security

WAF & Application Security

Application Security Testing

MSSP

MSSP

Traditional MSSP

Advanced MSS & MDR

Data Security

Data Security

Encryption

DLP

Data Privacy

Data Center Security

Risk & Compliance

Risk & Compliance

Risk Assessment & Visibility

Security Ratings

Pen Testing & Breach Simulation

GRC

Security Awareness & Training

Mobile Security

Mobile Security

Security Ops & Incident Response

Security Ops & Incident Response

SIEM

Security Incident Response

Threat Intelligence

Threat Intelligence

IoT

IoT

IoT Devices

Automotive

Connected Home

Identity & Access Management

Identity & Access Management

Authentication

IdaaS

Privileged Management

Identity Governance

Consumer Identity

Messaging Security

Messaging Security

Digital Risk Management

Digital Risk Management

Blockchain

Blockchain

Cloud Security

Cloud Security

Containers

Infrastructure

CASB

Security Consulting & Services

Security Consulting & Services

Fraud & Transaction Security

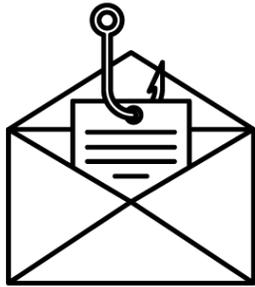
Fraud & Transaction Security



Understanding Information Security and Privacy Threats

Understanding Information Security and Privacy Threats

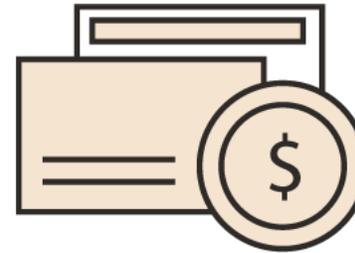
Three of the biggest threats to our organization today are:



Phishing



Social Engineering



Ransomware

Phishing

- ▶ Phishing refers to the practice of creating fake emails that appear to come from someone you trust, such as:
 - Bank
 - Credit Card Company
 - Popular Websites
- ▶ The email will ask you to “confirm your account details or your vendor’s account details”, and then direct you to a website that looks just like the real website, but whose sole purpose is for steal information.
- ▶ Of course, if you enter your information, a cybercriminal could use it to steal your identity and possible make fraudulent purchases with your money.

Social Engineering

- ▶ When attempting to steal information or a person's identity, a hacker will often try to trick you into giving out sensitive information rather than breaking into your computer.
- ▶ Social Engineering can happen:
 - over the phone
 - by text message
 - instant message
 - email

Ransomware

- ▶ Ransomware is a type of malware that restricts your access to systems and files, typically by encryption and then demands a ransom to restore access.
- ▶ Often, systems are infected by ransomware through a link in a malicious email. When the user clicks the link, the ransomware is downloaded to the user's computer, smartphone or other device. Ransomware may spread through connected networks.





Safe Computing Best Practices

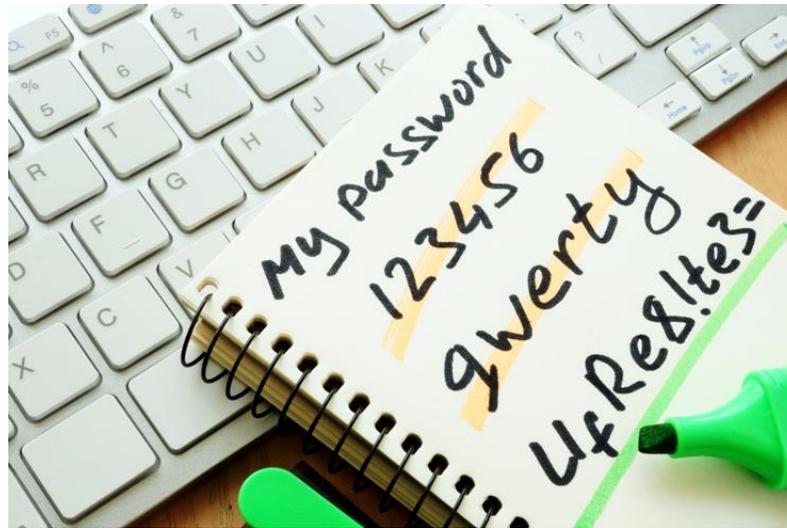
Safe Computing Best Practices

- ▶ Password Hygiene
- ▶ Avoiding Malware
- ▶ Avoiding Social Engineering
- ▶ Avoiding Phishing



Safe Computing Best Practices: Password Hygiene

- ▶ To help secure our network and your own identity, you should:
 - create a strong password
 - change it often
 - keep it secret



Safe Computing Best Practices: Password Hygiene

- ▶ A strong password should:
 - Be as long as possible
 - Not contain words found in a dictionary in any language, since password crackers will try those first
 - Use a mix of upper and lower case letters, numbers, and special characters, such as “#” or “&”, and
 - Not contain any easily guessed personal information, such as your birthday or the name of your pet.

Safe Computing Best Practices: Avoiding Malware

- ▶ While there are many defenses that can be put in place to protect you from malware such as antivirus and antispyware software, firewalls, and spam filters but these tools cannot protect you if you unwittingly install malware on your computer. To avoid malware:
 - Think before you click. Report suspicious emails to your supervisor, IT helpdesk, or information security teams
 - If you think your computer does not have an up to date operating system or antivirus or antispyware program or is infected by malware, alert the IT department.
 - If you're able to download and install applications on your computer, only install application approved by your IT/Security department to avoid accidentally installing malware.

Safe Computing Best Practices: Avoiding Social Engineering

- ▶ Verify the identity of those who ask for your sensitive information in person or over the phone before you release it
- ▶ Do not give out system data or sensitive information about other employees, remote network access, organizational practices, or strategies to any unknown individual
- ▶ If you think you are the victim of social engineering, gather as much information as you can, such as the person's name, telephone number, and what they are asking for and report it to your supervisor or information security team.

Safe Computing Best Practices: Avoiding Phishing

- ▶ Never respond to unsolicited email messages that request personal information. A reputable organization will never ask for your password or other sensitive information.
- ▶ Be suspicious of emails that don't address you by name or that have misspellings or simply don't look professional
- ▶ Do not navigate to websites by clicking on links in email messages.
- ▶ Keep in mind that phishing messages can also be sent via SMS text messages. Faxes and even automated voice response systems
- ▶ Be aware that phishing emails may not always be designed to steal information - their goal may be to install malicious software on your computer. This can happen by simply clicking on an infected link or downloading an infected attachment.

Social Media & Networks Dangers





Mobile and Remote Computing Best Practices

Protecting Mobile Data and Devices

- ▶ Protecting Smartphones and Tablets
- ▶ Working in Public Best Practices
- ▶ Remote Access Best Practices



Protecting Smartphones and Tablets

- ▶ Ensure your mobile operating system is up to date with the latest software updates
- ▶ Only use trusted, regulated app stores
- ▶ Never jail-break an iPhone or root an android phone - this will create additional risks
- ▶ Report lost devices that contain or can access workplace information immediately to your IT department. They may be able to remotely delete data from the device

Working in Public Best Practices

- ▶ Never discuss confidential information in public places
- ▶ Be careful when displaying workplace information on your screen in public places. Someone could be shoulder surfing (reading over your shoulder)
- ▶ Refrain from using public Wi-Fi networks that do not have a password
- ▶ Never leave mobile devices in view where they could lure thieves
- ▶ Keep your computer bag on you at all times
- ▶ Use a computer privacy screen when possible

Remote Access Best Practices

- ▶ The same security policies and standards apply when working remotely as in the workplace
- ▶ Only company issued computers should be used to remotely access the network
- ▶ Remote access to the workplace network must be over a VPN connection which secures all communications





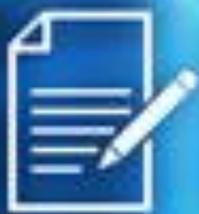


REGULATIONS

RULES



STANDARDS



COMPLIANCE



POLICIES



LAW

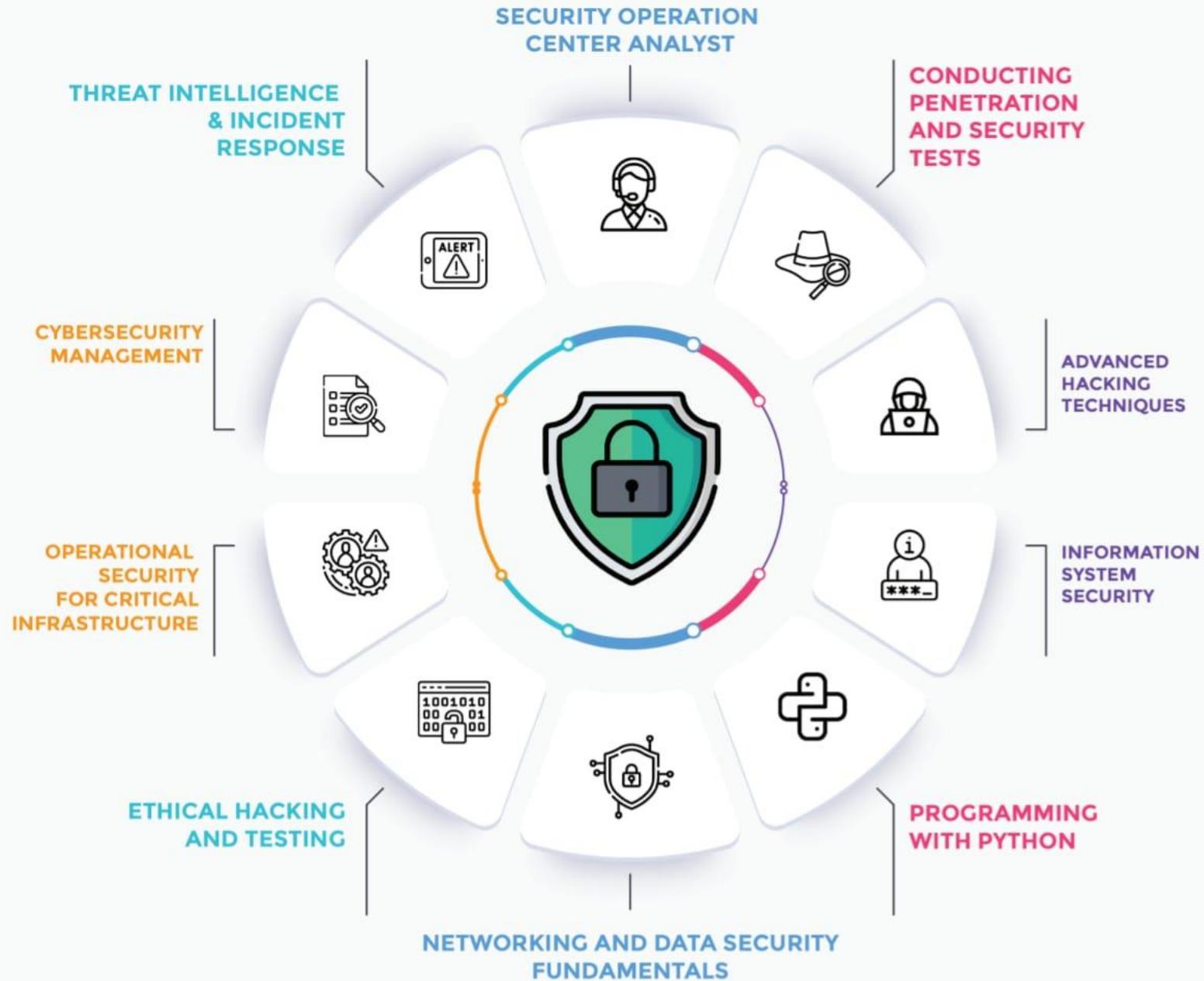


REQUIREMENTS



Philadelphia Cyber

APPLIED TRAINING
CYBER SECURITY DIPLOMA





Thank You ;;

DEVELOPMENT AND TRAINING CENTER

<https://www.philadelphia.edu.jo/centers/development-and-training-center>