GSPH Data Security & Computer Administrative Rights Training

- Public Health Technology Services
- Modified: September 7, 2020

What is the purpose of this training?

You have requested local administrator rights on one or more University computers. These rights will be granted after you have:

- Completed this educational module
- Successfully completed a post-test
- Signed and submitted via DocuSign the Computer Administrative Rights Agreement to Public Health IT

Training Content

- A definition of "local administrator rights"
- Responsibilities of local administrator users
- An introduction to cyber security threats, data security, and data security compliance
- A brief introduction to software licensing
- University data security policies
- Link to a Qualtrics post-test on course content

A definition of "local administrative rights"

- Allows user full control over all computer settings and software installations
- Allows user to run any / all programs, including software update programs
- Allows user to add and remove printers
- Allows changes specific to a user's account
- Allows direct access to operating system (WIN 10, Mac OS)

Responsibilities of users with "local administrative rights"

- **YOU** are to maintain the integrity of your workstation(s).
- **YOU** are a level of security to combat attackers.
- **YOU** are accountable for all software license maintenance and applicable license renewals on your workstation(s).
- Understand that local administrative privileges increase your and the University's exposure to risk.
- Administrative credentials are key targets of attackers looking to infiltrate and exploit a network .
- To combat increased risk, it is necessary to have a better awareness and understanding of how to both recognize and combat an attack.
- Data Security Compliance: understand the different categories of data, their associated risk, and how risk impacts their storage location.

Data Breaches in Higher Education

Photo credit: https://www.axiomhighered.com/blog/policies-must-prioritized-higher-education-data-breaches-skyrocket/

A Data Breach: What is it?

You've just added the final touches to an important document. You want to save a copy to another device, so you reach into your bag to pull out your USB flash drive. Where is it? You search through all of the pockets and compartments. Still no flash drive. Where did you see it last? WHEN did you see it last? You search your office. You search your car. You search your home. Still no flash drive. If it is indeed lost … you start to sweat. What did you have stored on it? Can you recall every file? Work files? Personal files? Tax files?

Has this happened to you? If so, then you have experienced a data breach.

Perhaps you didn't think of it as a breach. No one broke into your computer to access your information. However, if your information falls into the wrong hands, the result will be the same -- credit card information, bank records, tax records. All exposed for use by a cyber criminal.

The terms "data breach" and "cybercrime" are often used interchangeably, and though closely related they are not synonymous. For the purposes of this discussion:

- A cyber crime is criminal activity or a crime that involves the Internet, a computer system, or computer technology.
- A data breach is a confirmed cyber security incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed through unauthorized means. Data breaches may involve personal health information (PHI), personally identifiable information (PII), or intellectual property.

https://www.nw3c.org/docs/research/cyber-intrusion-and-data-breaches.pdf , https://www.dictionary.com/browse/cybercrime, https://searchsecurity.techtarget.com/definition/data-breach

Data Breaches in Higher Education: Rising Costs

When a data security breach occurs at an institution of higher learning, like the one suffered by Augusta University (GA), the financial impact on the institution, students, and faculty is measured in the millions of dollars. Ponemon Institute reported the average total cost of a data breach increased by 6.4% in 2018, and that the average number of records stolen increased by 2.2%.

In the education industry sector, the average cost of a data breach was $200 per compromised record. The average total cost of a data breach for an organization across all industry sectors amounts to over $7 million.

Also to be considered are the costs and long-term damage inflicted through student identity theft due to a data breach. Lasting impacts to students can include delay/cancellation of student loans, credit score downgrades, time invested in identity theft remediation rather than studies, and psychological stress.

https://managedmethods.com/blog/why-higher-education-cloud-security-2019/ ,
https://library.educause.edu/~/media/files/library/2018/10/cyberseconestop.pdf

Data Breaches in Higher Education: What Are the Costs?

- Harm to the University's reputation and erosion of trust
- Loss of productivity
- Increased expenditures due to systems recovery
- Down time
- Exposure of research data / IRB violations
- Intellectual property loss
- HIPPA fines / penalties
- Suspension or loss of a research study grant
- Sanctions against future grant awards

Data Breaches in Higher Education: How Does it Happen?

Most data breaches are attributed to hacking or malware attacks. Breaches do not happen overnight. It takes time before the attacker can extract data from a victim. The three phases of a data breach are:

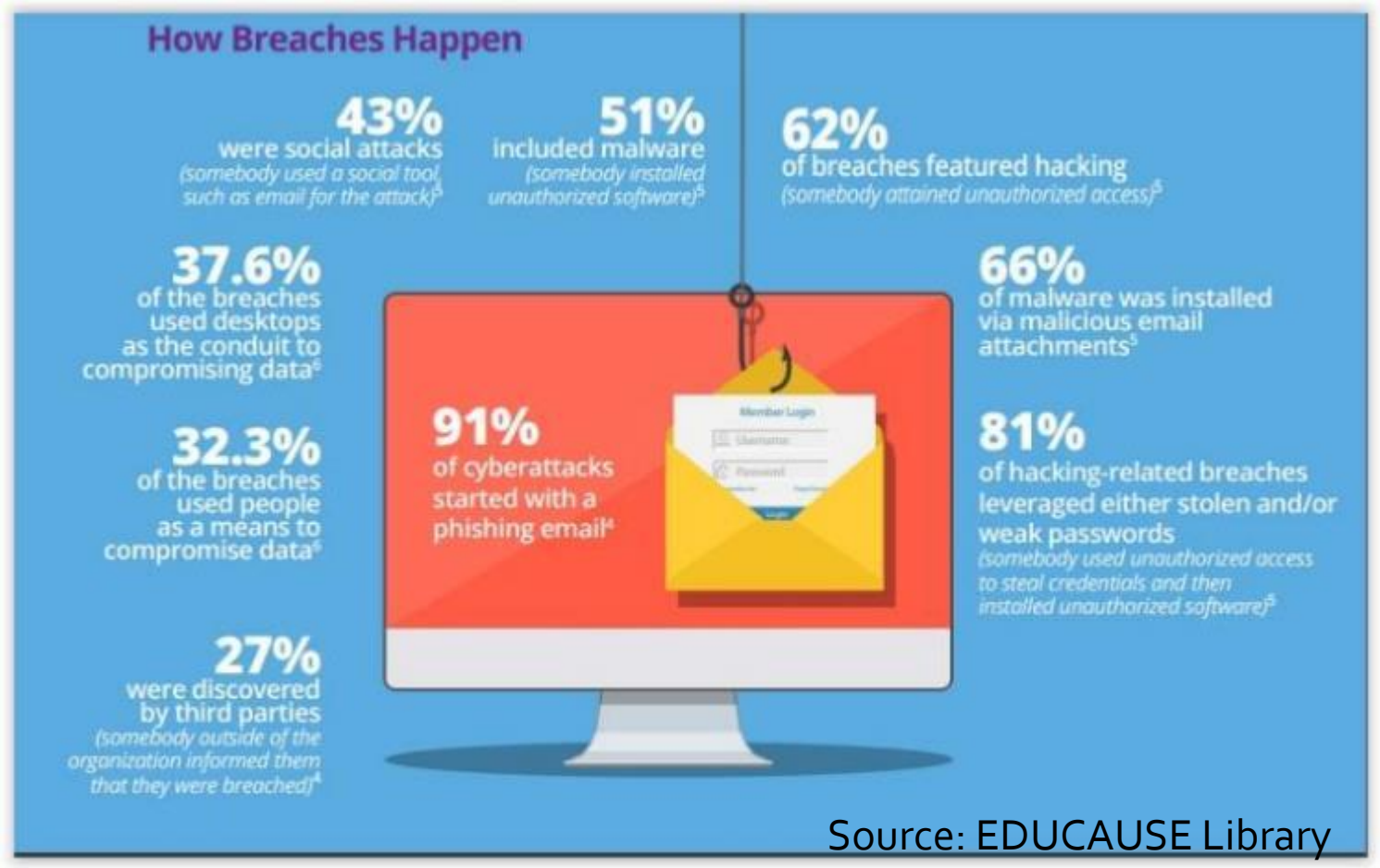
- **Research:** The attacker, having picked a target, looks for weaknesses to exploit: employees, systems, or the network. This entails long hours of research on the attacker's part and may involve stalking employees' social media profiles to discover what sort of infrastructure the company has.
- **Attack:** Having scoped a target's weaknesses, the attacker makes initial contact either through a network-based or social attack.

  In a **network-based attack**, the attacker exploits weaknesses in the target's infrastructure to instigate a breach. These weaknesses may include, but are not limited to SQL injection, vulnerability exploitation, and/or session hijacking.

  In a **social attack**, the attacker uses social engineering tactics to infiltrate the target network. This may involve a maliciously crafted email sent to an employee, tailored to catch that specific employee's attention. The email can phish for information, fooling the reader into supplying personal data to the sender, or come with a malware attachment set to execute when downloaded.
- **Exfiltrate:** Once inside the network, the attacker is free to extract data from the company's network. This data may be used for either blackmail or cyber propaganda. The information an attacker collects can also be used to execute more damaging attacks on the target's infrastructure.

https://www.trendmicro.com/vinfo/us/security/definition/data-breach

Data Breaches in Higher Education: How Does it Happen?



Source: EDUCAUSE Library

Cyber Security Threats: An introduction

Cyber Security Threats: A Perspective

When you think of the phrase "data breach," what comes to mind? The credit agency Equifax? Uber? Facebook? Marriott's Starwood Hotel chain? Capital One?

How about the phrase "cyber attack"? The city government lockouts of Baltimore, MD and Riviera Beach, FL? The name WannaCry? Perhaps Russia? Or China?

An August 2019 report published by Risk Based Security stated there have been more than 3,800 data breaches so far in 2019 – a 54% increase over the same period in 2018.

Now, what do the above have to do with University of Pittsburgh computer users? It turns out, more than you may think.

Gemalto.com reported successful data breaches in the education sector jumped 103% during the first six months of 2017, compared to the last half of 2016. In hard numbers, that was 118 data breaches. Only healthcare (228) and financial services (125) had more incidents. The actual number of attacks could be millions. Or more.

In 2019, the investor service Moody's characterized cyber risk for the higher education system as "medium" but increasing, and universities with medical centers were portrayed as the most vulnerable.

https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx

https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/ , https://www.moodys.com/research/Moodys-Cyberattacks-represent-growing-risk-for-the-global-higher-education--PBM_1176397

Cyber Security Threats: A Perspective

Why target education? Like all attacks, it's the opportunity to pilfer valuable data. In April 2019, Georgia Tech revealed that it was the target of a cyberattack. The result was stolen personal information of up to 1.3 million current/former students, employees and applicants.

Universities house a tremendous amount of personal data pertaining to students, staff and faculty. This means University databases contain Personally Identifying Information (PII) and financial data for thousands of people. A structured and rather sophisticated market for pilfered PII has been developed, and this information can be bought and sold in bulk. If information from a single credit card can be sold for $10, imagine the asking price for a one-time hack into a database containing thousands of them?

https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx

www.aabri.com/manuscripts/162377.pdf , https://www.enzoic.com/cyberattacks-risks-for-highered/

Cyber Security Threats: A Perspective

Large universities spend many millions of dollars conducting research in such fields as medicine, computing, and engineering. Important intellectual property is derived from this research. Sensitive, cutting-edge research is an appealing target for hackers. Any major technological development would be an enticing and lucrative objective for hackers who are sponsored by or sell to foreign governments, like China or North Korea.

More importantly, what makes educational institutions so alluring a target comes down to access: academic cultures are very open to communication and collaboration. Their computing environments are very similar, allowing a dizzying array of devices unrestrained access to internet content, mixed with restricted access to sensitive university data. Also, faculty and students demand more control over their data than private sector or government users who have limited web access and use only approved devices. Computing systems with so much freedom are difficult to secure. When you add the tremendous number of users (students, faculty, staff and research groups) to this equation, universities look very attractive to cyber criminals.

Let's look at some "tools of the trade" used by cyber attackers.

www.aabri.com/manuscripts/162377.pdf

Common Cyber Security Attacks

- Botnets
- Hacking
- Malware / Spyware
- Malvertising
- Phishing / Spoofing
- Pharming
- Ransomware
- Virus
- Wi-Fi Eavesdropping
- Wireless Intercept and "Wiphishing"

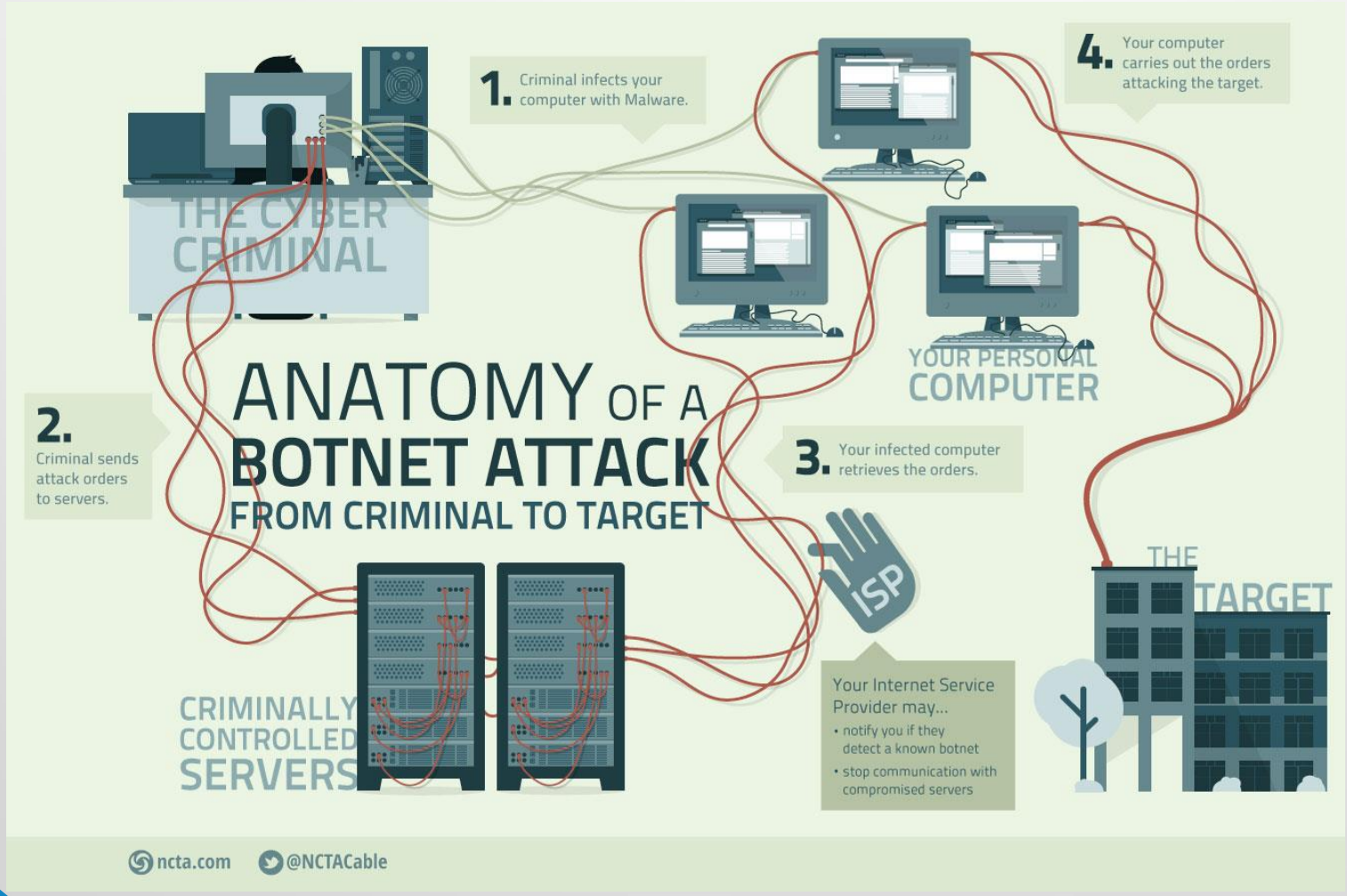
https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Common Cyber Security Attacks: Botnets

Botnets are a collection of software robots ("bots") that create an army of infected computers by exploiting security vulnerabilities. Remotely controlled by a malicious user, known as a "bot herder," this digital army is used for nefarious online purposes (e.g. to spread virus-infected spam or other malware, or to participate in wide-spread attempts to crash websites). See the next slide for a graphical view of a Botnet attack.

Prevention: use a strong password; install and regularly run anti-virus & anti-malware software; install OS updates; secure your home network; restrict file sharing; use secure VPN with public Wi-Fi.

Common Cyber Security Attacks: Botnets



Common Cyber Security Attacks: Hacking

Hacking is a term used to describe actions taken by a user to gain unauthorized access to a computer in order to undertake malicious activities, such as stealing sensitive information or planting malware for an attack at a later date.

Prevention: use a strong password; install and regularly run anti-virus & anti-malware software; install OS updates; secure your home network; restrict file sharing; use secure VPN with public Wi-Fi. See details here: Protect your computers, laptops, & tablets

Common Cyber Security Attacks: Malware / Spyware

Malware is a general term for malicious software knowingly or unknowingly installed and used to infiltrate or damage your computer. Examples of malicious activities include reformatting a hard drive; altering or deleting files; appropriating sensitive information; seizing control of email; or planting malware for an attack at a later date. In 2018, cryptocurrency mining malware (covertly installed while surfing the web) was the top malware threat, and it is predicted to remain the top threat in 2019.

Hacking or malware has been identified as the leading cause of higher education data breaches.

Spyware's purpose is derived from its name: it is designed to monitor user actions and collect personal data. That includes visited web sites, typed passwords, online banking / credit card account information, etc.

Prevention: use a strong password; install and regularly run anti-virus, anti-malware and anti-spyware software; install OS updates; secure your home network; restrict file sharing; use secure VPN with public Wi-Fi. See details here: What you can do to be more secure online.

https://www.csoonline.com/article/3269053/security/cryptomining-not-ransomware-the-top-malware-threat-so-far-this-year.html

Common Cyber Security Attacks: Malvertising

Malvertising (short for malicious advertising) is the use of online advertising to distribute malware with little or no user interaction. A tiny piece of code hidden deep in the ad -- maybe in the text or graphics, flash files (SWF) or video files -- directs your computer to criminal servers without ever clicking on the ad itself. Just by visiting the webpage that hosts the ad, malware is downloaded and installed. This is known as a "drive-by download."

This type of attack has been on the rise. From 2016 to 2017, the number of new mobile malware variants increased by 54%. In July 2018, a malvertising agent exploited the AdTerra online advertising network by masquerading as a legitimate web publisher. The scammers reportedly compromised some 10,000 websites, where users were redirected to malware download pages that spread viruses, ransomware and bots.

https://www.forbes.com/sites/forbescommunicationscouncil/2019/05/31/as-malvertising-grows-bolder-publishers-must-step-up-their-defense/#5630f7ee2841 , https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/ , https://www.cisecurity.org/top-10-malware-january-2018/

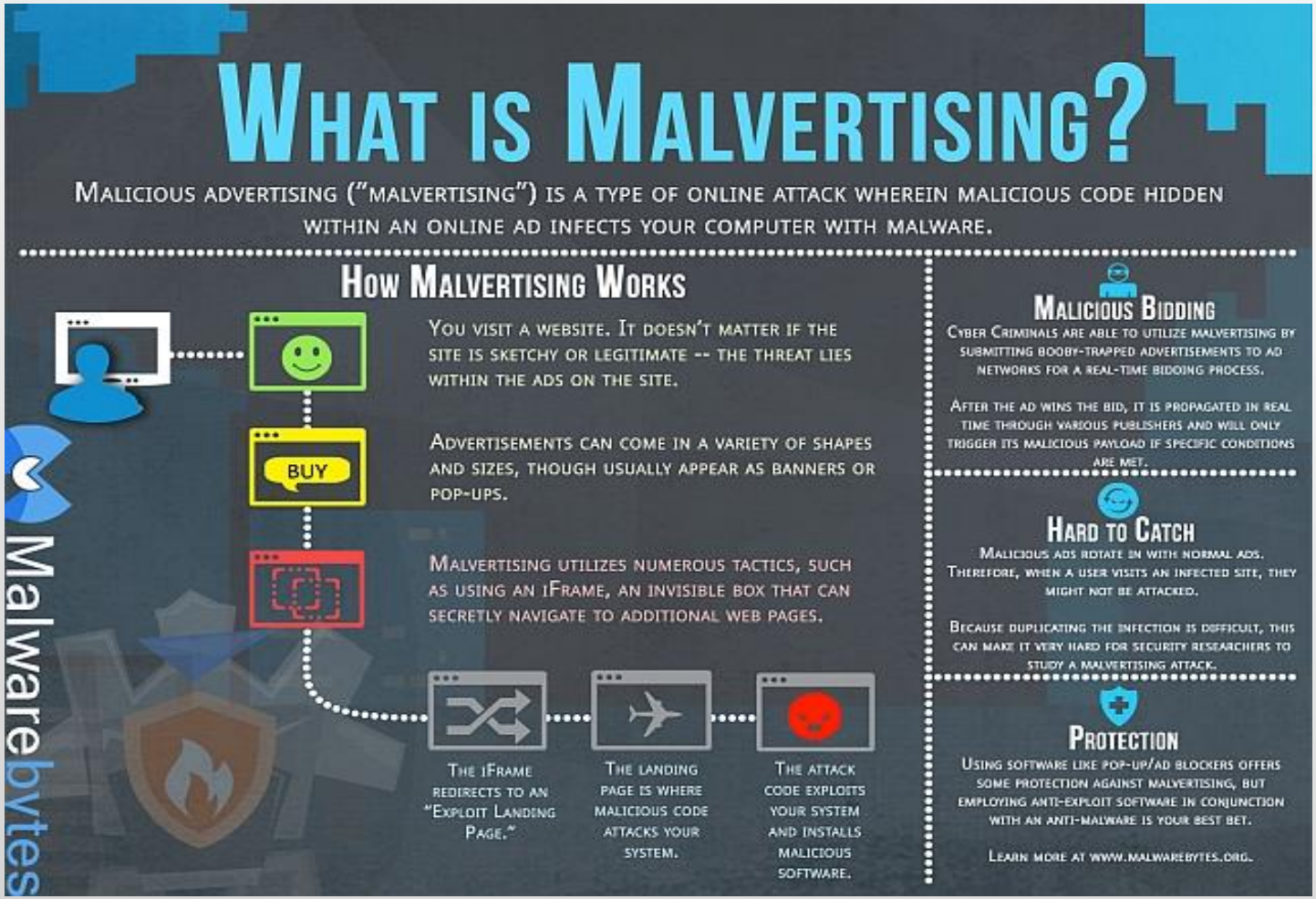
Common Cyber Security Attacks: Malvertising

Do you think Apple users are immune? Think again! Over a 48-hour period in November 2018, a nationwide scam hit more than 300 million U.S. Apple iOS browser sessions. The criminals placed corrupted ads on legitimate websites, which enabled them to take over browsing sessions and redirect victims through a long chain of temporary websites. This redirection chain eventually landed on a site promoting a gift card scam or an adult-themed site.

Infection also occurs in the more traditional fashion: when users visit shady websites, click malicious links or download misleading apps. These malicious files can target any operating system and are capable of bypassing adblockers and other protective measures to deliver a malware payload.

https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/ , https://www.zdnet.com/article/us-ios-users-targeted-by-massive-malvertising-campaign/ , https://www.cisecurity.org/top-10-malware-january-2018/

Common Cyber Security Attacks: Malvertising



https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/

Common Cyber Security Attacks: Malvertising

Because attackers target high-traffic sites, you may think **Malvertising** is limited to use on dangerous or "shady" web sites. Yes and no. It is certainly found on these shady or NSFW (not-safe-for-work) sites, and these types of web sites should be avoided when browsing on University computers.

Examples of malvertising-prone websites:

- Varied pornographic sites
- Sites offering free software
- Sites offering coupons, savings and questionnaires
- Streaming sites
- Online dating sites
- Online betting / gambling sites

https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/ , https://www.makeuseof.com/tag/dont-victim-malvertising-stay-safe-tips/ , https://www.cisecurity.org/top-10-malware-january-2018/

Common Cyber Security Attacks: Malvertising

Malvertising can also invade legitimate, top tier, high-traffic websites, both on desktop and mobile, by injecting malware into ads without the user's or publisher's knowledge. In March 2016, MalwareBytes monitored a particular campaign that found malicious advertisements at the following sites:

- MSN.com
- NYTimes.com
- AOL.com
- NFL.com
- Realtor.com
- Theweathernetwork.com
- Newsweek.com

While malvertising seemed to be on the decline, the silent danger it presents while surfing legitimate web sites is still very real.

Prevention: practice safe browsing; use a web browser with built-in drive-by download protection (e.g. Firefox; Chrome after April 2019); install and regularly run anti-virus, anti-malware and anti-spyware software; install OS updates; remove any unneeded software (especially Java or Flash); enable click-to-play plugins within web browsers; run an effective anti-exploit program.

https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/ ; https://www.makeuseof.com/tag/dont-victim-malvertising-stay-safe-tips/ ; https://www.zdnet.com/article/google-chrome-to-add-drive-by-download-protection/

Common Cyber Security Attacks: Phishing and Spear Phishing

Also known as spoofing, **Phishing** is a social engineering method used to obtain information by disguising communication as being from a trusted source; the information can then be used to access devices or networks.

Spear Phishing is a phishing attack directed at a specific individual or organization. To increase the likelihood of success, these attacks are usually tailored by means of a cloned login interface on an organization's intranet, or the use of personal information about the targets gathered in advance.

Often presented in an official or intimidating manner, phishing schemes typically ask you to update / validate / confirm a banking or shopping account so cyber criminals can access your account and steal credit card information.

Source: Phishing and Spear phishing: An IT Pro's Guide, by James Sanders; Tech Republic, CBS Interactive, Inc. 2019

Common Cyber Security Attacks: Phishing and Spear Phishing

Phishing techniques can include: disguising a malicious link as pointing to a trusted source (e.g. exploiting misspelled URLs or using confusingly similar domains); website cloning, forgery and redirecting; and voice and text messages claiming account access has been disabled and instructing users to call a phone number or use a website created by attackers to collect account information.

Why be concerned about phishing? Because it affects **every user**. Attackers usually cast a wide net, hoping to catch any arbitrary victim to gain access to an account or an organization's network port of entry. From there, attackers can glean sensitive information. This strategy works: 91% of cyberattacks started with a phishing email.

Sources: Phishing and Spear phishing: An IT Pro's Guide, by James Sanders; Tech Republic, CBS Interactive, Inc. 2019; Why Cybersecurity Matters: and What Registrars, Enrollment Managers and Higher Education Should Do About It, National Student Clearinghouse, 2018 (EDUCAUSE Library)

Common Cyber Security Attacks: Phishing and Spear Phishing

Another reason for concern is traditional security software (i.e., anti-virus programs) adapts poorly to attacks that rely on an immediate, knee-jerk user responses to social engineering which convinces users to act before analyzing the situation.

In the end, the best defense against phishing is training users to recognize the characteristics of these attacks and testing their response through simulated phishing expeditions.

Prevention: be aware of fake emails requesting an update to your account logon information; be wary of unexpected email requests from supervisors / deans / associate deans instructing the purchase of gift cards on their behalf; beware of any email that contains embedded links. Can you spot a phishing attack? Here's a quiz to test your phishing defenses.

Source: Phishing and Spear phishing: An IT Pro's Guide, by James Sanders; Tech Republic, CBS Interactive, Inc. 2019

Common Cyber Security Attacks: Pharming

Pharming is a when a hacker invades a user's system and plants malicious software which will point the web browser to a bogus web site by redirecting specific legitimate URLs (most often banks, financial and payment services). This redirection occurs even if the URL is entered correctly.

When the target web site has been accurately reproduced, the user may be convinced the site is legitimate, and then tricked into entering personal information that can be collected by the cyber criminal.

Pharming can be thought of as Phishing without the email "lure."

Prevention: beware of fake emails requesting an update to your information; use strong passwords; beware of unknown / suspicious looking posts and links on social network sites. Here are 12 simple things you can do to be more secure online.

Source: https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx , https://study.com/academy/lesson/what-is-a-pharming-attack-definition-examples.html

Common Cyber Security Attacks: Ransomware

The attack with the highest profile in 2019, **Ransomware** is a type of malware that restricts computer access and demands payment (typically Bitcoin or Monero to avoid detection by authorities) in exchange for restored computer access. In some instances, the ransom message refers to the detection of illegal activity by authorities, with a fine demanded to avoid prosecution. The most common types of infection appear to be phishing emails with a malicious attachment and website pop-up advertisements.

Two common types of ransomware are:

- Window blockers (Lockscreen): a splash screen image blocks access to the computer.
- Encryption: access to files on your hard drive are blocked via encryption. USB-connected devices such as flash drives and external hard drives, network share folders, and some cloud storage could also be affected.

Ransomware victims include: individuals, businesses (e.g NotPetya, WannaCry), hospitals, universities, and governments, including the highly publicized August 2019 data network lock-out experienced by 22 state of Texas municipalities.

Common Cyber Security Attacks: Ransomware

Example of a "detection of illegal activities by authorities" Lockscreen

Common Cyber Security Attacks: Ransomware

Example of a Ransomware Encryption screen

Common Cyber Security Attacks: Ransomware

Ransomware: in case of attack, what can you do?

- Do not pay the ransom
- For a University computer, contact the Public Health Technology Services Group
- For a personal computer, have your device analyzed by a reputable IT technician / forensic specialist

Common Cyber Security Attacks: Ransomware

Ransomware: A Defense Strategy

- Ransomware makes use of older software vulnerabilities, so make certain both operating system and application software updates are kept current.
- Beware of a precursor malware attack. "Quiet" malware may infiltrate a system to assess an organization's assets. Stop the precursor, and ransomware may pass you by.
- YOU, the user, are the first defense: be diligent about suspicious emails. Phishing attacks that convince users to download the ransomware are the main avenue of attack. Do not click on links or open attachments from unknown sources.
- Be proactive: take advantage of MalwareBytes Premium available to Pitt users. Schedule and perform regular malware scans on your computer. If you need assistance, place a ticket with Public Health Technology Services.
- For your laptop or home computer, be **doubly** proactive: schedule and perform a regular backup (daily or weekly) to a removable external drive that is then disconnected from your computer. Ransomware will attack both your computer and any attached USB hard drive or flash drive.

Sources: https://www.techrepublic.com/article/6-tips-to-avoid-ransomware-after-petya-and-wannacry/?ftag=TRE684d531&bhid=20703190204224472846374027409551; https://www.techrepublic.com/article/10-tips-to-avoid-ransomware-attacks/

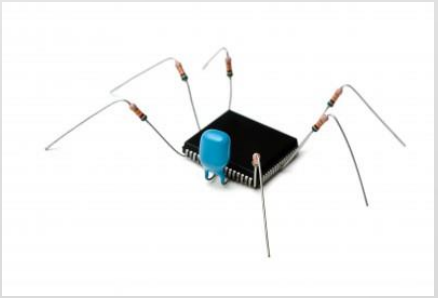
Common Cyber Security Attacks: Virus

A **virus** is a malicious computer program (e.g. worm, trojan horse) that infects your computer and the computers of those in your contact list. These programs are often sent as an email attachment, but a virus can also be picked up from an infected web site that triggers an automatic virus download.

Once a virus has taken control of a computer it can:

- Send spam
- Provide criminals access to your computer and contact lists
- Scan the hard drive for personal information (passwords, credit card info)
- Disable your security software & security settings
- Corrupt the operating system
- Hijack your web browser
- Display unwanted ads

Once installed, a virus can infiltrate your hard drive and spread to USB-connected devices, like external hard drives and flash drives. Also, any attachment sent via email is likely to be infected.



Common Cyber Security Attacks: Virus

Symptoms of a virus-infected computer:

- Longer than usual computer start up / restarts on its own / won't start
- Applications take longer to load
- Files and data have disappeared
- System and / or programs crash constantly
- Web browser home page has been reset
- Web pages are slow to load
- Computer screen looks distorted
- Programs are running without your control

If you suspect a virus infection on a University computer, contact the Public Health Technology Services Group immediately. If not available, contact the Pitt help desk (helpdesk@pitt.edu or 412-624-HELP).

Common Cyber Security Attacks: Wi-Fi Eavesdropping

Wireless (Wi-Fi) networks use radio waves to connect mobile devices to the internet. **Wi-Fi Eavesdropping** is a method to capture personal information by virtual "listening in" over an unsecured (unencrypted) wireless network. Using the right snooping equipment on an unsecured public wireless network, cyber criminals can potentially access your computer, capturing passwords and login information.

Prevention: never trust public Wi-Fi networks; enable your firewall; visit the HTTPS version of websites; enable SSL encryption of web sites; be mindful of the website URL – if the "s" in "https:" disappears, log off immediately; erase your browsing history and cookies as if you were using a public computer in a library or hotel.

Common Cyber Security Attacks: Wireless Intercept and "Wiphishing"

A wireless transmission intercept occurs when unencrypted Wi-Fi traffic is commandeered by a rogue Wi-Fi access device, leading to a compromised data situation.

- **"WiPhishing"** (pronounced "why fishing") involves covertly setting up a wireless-enabled laptop or access point that connects with other wireless-enabled laptops as a prelude to hacking attacks. Some WiPhishing access points download viruses, worms, and keyloggers (programs that send your recorded keystrokes to a cyber criminal). Others are used to intercept network traffic in order to intercept sensitive information (e.g. user IDs, passwords, credit card numbers)
- **A Rogue wireless access point** is a wireless base station set up on a network without permission. Rogue wireless access points typically intercept transmissions and circumvent network security controls, like firewalls, that protect University users from hackers, worms, and other computer threats

When using wireless network connections on campus, use only University-supported Web access points. The University's Wireless PittNet network requires authentication before University network resources can be accessed.

http://technology.pitt.edu/security/wireless-intercept-and-wiphishing

Data Security: What is it?

A common definition of **Data Security** is protective digital privacy measures that are applied to prevent data corruption and the unauthorized access to computing devices, databases and websites.

Data security technologies can include backups, data masking, de-identification of data or data erasure. Another is encryption, where digital data are rendered unreadable to unauthorized users.

A common data security practice is the use of authentication, where users must provide a password, code, biometric data or some combination of these to allow access to a system or data set.

Data security can also mean policies and procedures, the best ways to keep your data and devices safe from harm or invasion.

https://www.techopedia.com/definition/26464/data-security

Data Security:
Public Wi-Fi Security

Public Wi-Fi is seemingly available everywhere: airports, restaurants, coffee shops, etc. Awareness of the dangers when using public Wi-Fi networks is extremely important. These networks are not secure and can be accessed by many different people. **DO NOT** treat them as you would your home Wi-Fi.

To put this in perspective for users, one cybersecurity official drew a comparison of public Wi-Fi networks to public restrooms: some are clean; some are dirty; all of them are suspect.

Here are some suggested precautions:

- Stick to wireless networks and hotspots that you know, where they provide you with a password to use Wi-Fi. Unknown or unsecured public Wi-Fi doesn't require a password, so anyone can connect to it
- Verify that you're connected to the correct network
- Why confirm you're on the right network? Hackers have been known to set up a phony parallel network near legitimate public Wi-Fi specifically to capture unsuspecting users' personal data and hijack information

https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/cmptrs-tblts/wf-ntwrks-en.aspx

Data Security:
Public Wi-Fi Security

So you're on a trusted, legitimate network. Now you also need to protect yourself from others connected to the same public network. Here are some tips for public Wi-Fi security:

- If you're using your computer in a public Wi-Fi zone but you're not on the Internet, turn OFF your Wi-Fi card (click the wireless icon in your main menu bar or manually adjust this on the device hardware).
- Never surf without your firewall enabled – especially on a public Wi-Fi network
- Public Wi-Fi is not a safe network to share files, so turn off sharing, either manually or by choosing the "Public" option at first connection.
- Never trust the wireless encryption on a public Wi-Fi. Instead, make certain your websites scramble your data by enabling the SSL encryption in the settings of the sites you visit (like your email).
- Visit the secure HTTPS version of sites and not the unsecure, regular HTTP site. Adjust the site URL with an extra 'S' in your browser's address bar if needed. Be mindful of the URL in the address bar while you're exchanging sensitive data – if the 'S' disappears you should log out right away.
- Surfing social media on a public Wi-Fi network can be riskier than visiting normal websites. For instance, once you log in, criminals on the same network can also log in as you. Take extra precautions by erasing your browsing history, your cookies, etc. as if you were using a public computer (library or hotel).
- If you find yourself on public Wi-Fi a lot, consider using a Virtual Private Network (VPN). It will direct all your web activity through a secure, independent network that encrypts and protects all your data. A VPN is offered by most Internet Service Providers as a secondary service.

https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/cmptrs-tblts/wf-ntwrks-en.aspx

Data Security:
Virtual Private Network

A **Virtual Private Network (VPN)** is an encrypted tunnel between your computer and a remote server operated by a VPN service. Once activated, all internet traffic is routed through this secure tunnel and away from potential eavesdroppers. Because all traffic exits the server, your computer's IP address appears the same as the VPN server, masking your computer's identity and location.

Advantages to using a VPN:

- Increased security and peace of mind when using public Wi-Fi networks (coffee shops, hotels, airports)
- Keeps user data private from your home ISP who has the ability to sell customer anonymized data
- When traveling outside the US, a VPN can allow for a (mostly) normal browsing experience

Disadvantages to using a VPN:

- Not all apps will run over a VPN
- Some popular sites and services (e.g Netflix) block many VPNs
- VPN usage degrades upload and download speeds

PC Magazine recently surveyed 1000 readers and found that 62.9% didn't want to pay more than $5 a month for a VPN service, while 47.1% wanted a free service. However, be wary of **free** VPNs. Many have been found to contain malware. To learn more about VPNs, see the links below. For help in choosing a VPN, read about the Best VPN Services for 2020.

https://www.pcmag.com/article/352757/you-need-a-vpn-and-heres-why , https://www.pcmag.com/how-to/how-to-set-up-and-use-a-vpn

Data Security:
Home Wi-Fi Security

When using Wi-Fi, the absolute minimum security you should enable is wireless encryption and password protection (WPA2 where available, otherwise WPA) on all your devices including your wireless router. Here's why you should secure your home Wi-Fi network from strangers and trespassers:

- An unsecured network means anyone with a Wi-Fi device in your coverage area can access your personal Internet connection and your devices
- You could be providing "free" Wi-Fi for all your neighbors. Many dishonest users also hunt for unsecured Wi-Fi to exploit
- Trespassers can steal your bandwidth and usage capacity to download large files like movies or games, leaving you stuck with a big bill or restricted usage and download speeds
- You could be liable for any criminal actions that were conducted using your unsecured network – even if you knew absolutely nothing about it!

Data Security:
Home Wi-Fi Security

More reasons to keep your home Wi-Fi secure:

- Your unsecured browsing history, passwords, log in information and email content can all be easily accessed
- Your unsecured shared files can be accessed, copied or deleted
- Your unsecured Wi-Fi enabled peripherals like printers or video game systems can all be easily accessed
- Unsecured networks show up immediately as unlocked and vulnerable on wireless network scans on devices. They're easy prey
- Even a secured WPA2 network can be compromised by a Key Reinstallation Attack, which can leave sensitive information vulnerable

Data Security:
Home Wi-Fi Security

Now that you know why securing your Wi-Fi network is so important, here are a few other things to keep in mind:

- When setting the password for your home Wi-Fi network, always use a strong password
- Keep your coverage area limited to your house by placing your router as close to the middle of your space as possible, rather than placing it near windows
- Make sure that every device on your network, including routers, computers, smartphones, and smart devices, have updated software and operating systems to keep your entire network protected
- Not using wireless encryption? Make certain SSL encryption is active in the settings of the sites you visit (like your email). How? Look for the  in your URL bar
- There are optimal settings for your router to maximize the security that is available to your particular setup. You may have to refer to your router manual or contact your provider

https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/hm-ntwrks-en.aspx

Data Security: University Practices

- Create a strong password and change it regularly
- Use a current version of Windows (WIN 10) and Mac (Catalina) OS
- Restrict computer access by activating Ctrl+Alt+Delete logon requirement
- Ensure data encryption over the Pitt network by using Secure Remote Access / Pulse; transfer files via Secure File Transfer Protocol (SFTP)
- Physically and digitally protect your portable device
- Use email with caution: never open attachments from an unknown source; be wary of an unexpected attachment that looks suspicious from a known source
- Avoid file sharing and suspicious web sites
- Store important and sensitive data on the Pitt network; use Pitt-approved cloud services for all non-sensitive, shared Pitt data; perform a daily backup of remaining local computer data

For more information see Pitt's information Technology page on Security

Data Security:
Safe Password Usage

Previous slides have contained the phrase, "use a strong password. " What does that mean? Here's a list of commonly accepted practices for a strong password:

- Should contain a minimum of eight characters (longer is better)
- Must consist of some combination of upper and lower case letters, numbers, and at least one special character
- Do **NOT** use any portion of your name, username or email address
- Do **NOT** use words from the dictionary
- Do **NOT** use names of children, a significant other or someone close to you that could be traced through social media
- Do not use a common phrase

Remember:

- **Never** share your password
- No reputable organization will ask for your password
- Use different passwords for different web sites

Data Security:
Password Manager

Just about every web site controls your access with a username (unique or email address) and a password. As stated in the previous slide, the use of a strong password is a must, as well as having a unique password for each site. There's just one problem: the human mind simply cannot recall the dozens of passwords used in everyday life. So, now what?

First, let's look at how NOT to keep track of passwords:

- Sticky notes on monitor **– NO!**
- Small, hand-written list taped to keyboard bottom **– NO!**
- On a card in your wallet **– NO!**
- In an Excel spreadsheet on Dropbox™ **– NO!**

So, how do you remember these passwords?

The answer ? Use a password manager to create a strong, secure password for every web site.

Data Security: Password Manager

How does this work?

A typical password manager uses a browser plug-in to first record and then relay your password to a site. When you return to the site, it offers to automatically insert your credentials. Once you've entered all of your passwords, you need to identify the weak and duplicate passwords and replace them with tough ones. Once completed, you use one password to access the vault that houses all of your passwords.

https://www.pcmag.com/roundup/300318/the-best-password-managers?utm_source=email&utm_campaign=lab-report=utm_medium=title

Data Security: Password Manager

Why use a password manager?

- Your passwords are too simple – simple passwords are easy to crack, putting your information in jeopardy. Given the correct tools, hackers can crack simple passwords in minutes or even seconds.
- Password managers include random password generators, which will create long, complicated passwords that will keep your data safe.
- Use a password manager and you need to remember just one password – the one needed to access your password vault. Make certain your vault password is not obvious.
- How many accounts do you have that require a password? Tens? Hundreds? You're not going to remember all of those passwords, especially if they are strong, complicated passwords.
- Many password managers allow you to sync across your Windows, Mac ,iOS, and Android devices. This way you always have your passwords at the ready.

Pitt has partnered with the password manager LastPass. Visit the Pitt Password Manager page to get started. You can view video tutorials here.

https://www.techrepublic.com/article/5-reasons-why-you-should-use-a-password-manager/?ftag=TRE684d531&bhid=20703190204224472846374027409551

Data Security:
Compliance and Administrative Rights

As mentioned, users with administrative rights can allow unintentional access to data. Understanding data compliance (the categories of data and how this impacts their storage location) can help prevent loss that could be costly to you and the University.

Data Security Compliance

When it comes to data security, keep these thoughts in mind:

- Data confidentiality has top priority over user access/convenience
- University policies concerning secure data storage **are to be enforced**
- Passwords should follow University minimum requirements (see video Choose a strong password)
- Do NOT share your Pitt password and/or local admin password
- Be aware of the location of your data files: *On the local drive? On your network file share? On Box? On OneDrive? Elsewhere?*
- What are identifiers? *Personally Identifiable Information [PII]* *(See next slide)*
- Data files with identifiers: where are they located? *Only on the network file share*
- Data files with identifiers MUST be encrypted & password protected
- Off-network storage of data files with identifiers is permitted on ENCRYPTED external storage devices ONLY

Data Security Compliance: Personally Identifying Information

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) includes:

"(1) *any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information*."[1]

[1] http://www.technology.pitt.edu/security/guide-to-identifying-personally-identifiable-information-pii

Data Security Compliance: Personally Identifying Information

Examples of PII include, but are not limited to:

- Name: full name, maiden name, mother's maiden name or alias
- Personal identification numbers: Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number or credit card number
- Personal address information: street address or email address
- Personal telephone numbers
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Information identifying personally owned property: VIN number or title number
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

http://www.technology.pitt.edu/security/guide-to-identifying-personally-identifiable-information-pii

Data Security Compliance: Personally Identifying Information

The following examples on their own do not constitute PII, as more than one person could share these traits. However, when linked or linkable to information shown on the previous slide, the following could be used to identify a specific person:

- Date of birth
- Place of birth
- Business telephone number
- Business mailing or email address
- Race
- Religion
- Geographical indicators
- Employment information
- Medical information (maybe subject to additional HIPPA requirements)
- Education information (maybe subject to additional FERPA requirements)
- Financial information

http://www.technology.pitt.edu/security/guide-to-identifying-personally-identifiable-information-pii

Data Security Compliance: Data Risk Categories

- "The University of Pittsburgh takes seriously its commitment to protect the privacy of its students, alumni, faculty and staff, as well as to protect the confidentiality of information important to the University's academic and research mission. For that reason, we classify our information assets into **risk categories (high, moderate, low)** for the purpose of determining who is allowed to access the information and what minimum security precautions must be taken to protect it against unauthorized access"
- **Note**: "All systems that transmit, process, or store data classified as high risk should be assessed by the CSSD Security team. Please contact the Help Desk with any questions about appropriate protection of information"
- YOU are responsible for safeguarding University of Pittsburgh data stored on the computers, devices, and online services you use and access

http://technology.pitt.edu/security/data-classification-matrix

Data Security Compliance: Data Classification Matrix

Risk	High Risk	Moderate Risk	Low Risk
Description	Protection of the data is required by law/regulation, or The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.	The data is not generally available to the public, or The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.	The data is intended for public disclosure, or the loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the University's mission, safety, finances, or reputation.
Data Examples	Social Security Number Date of Birth Driver's License/State ID Number Bank/Financial Account Number Credit/Debit Card Number Visa/Passport Number Electronic Protected Health Information (ePHI) Export controlled information under U.S. laws Donor contact information and non-public gift information	Student records and admission applications Faculty/staff employment applications, personnel files, benefits, salary, personal contact information Non-public policies, manuals, and contracts Internal memos and email, non-public reports, budgets, plans, financial info University and employee ID numbers Engineering, design, and operational information regarding infrastructure	Directory Information Policy and procedure manuals designated by the owner as public Job postings Information in the public domain
Human Subject Research Data Examples	Identifiable sensitive human subject data*	Identifiable non-sensitive human subject data * De-identified sensitive human subject data*	Anonymous human subject data De-identified non-sensitive human subject data*
Storage, Transmission, and Collaboration	Storage of high risk data is prohibited on computing equipment unless registered with and approved by CSSD. Encryption in transit and at rest is required. Legal, ethical, or other constraints prevent access without specific authorization.	Medium risk data may be stored on departmental, CSSD hosted, or approved cloud-based systems. Encryption in transit is required. May be accessed by Pitt affiliates and non-employees with appropriate authorization.	Low risk data may be stored on departmental, CSSD hosted, or approved cloud-based systems. Encryption in transit is not required, but is recommended. No specific access restrictions.

*Sensitive human subject research data is defined as any data whose disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

Data Security Compliance: Mobile Devices

The convenience of mobility and "always on" wireless technology increases security vulnerabilities over a variety of attack avenues. Therefore, laptops / mobile devices have a higher rate of security issues. Be proactive and use these preventive safeguards:

- Do not leave laptops / mobile devices unattended. The numbers are staggering: one in ten laptops are stolen; 50% are stolen from an office or classroom; 98% are never recovered
- Make certain your mobile device is physically secure behind a locked door and/ or by a secure tether system
- Turn off Bluetooth when not in use to prevent outside attacks, like the BlueBorne Bluetooth attack.
- Public WiFi (Starbucks, airport, etc.) use is a high security risk. **ONLY connect to public WiFi when absolutely necessary**. If you travel often, use a Virtual Private Network (VPN)
- To avoid these always-present threats, verify your home wireless network is password protected and your router's software has been updated/patched
- If laptop / mobile device is stolen, contact Pitt Police immediately (4-2121)

https://www.technology.pitt.edu/security/cyber-security-awareness

Data Security Compliance: Mobile Devices

- **NEVER store sensitive or confidential data directly onto a mobile device** unless you have been authorized by CSSD to do so
- Use the Qualtrics Survey System to collect data on mobile devices
- If you must use a mobile device to access restricted University resources (data stored on the network), use of Secure Remote Access via Pulse Secure software (at least version 9.1.8) is mandatory

https://my.pitt.edu/task/all/qualtrics , https://pitt.co1.qualtrics.com/Q/MyProjectsSection

Data Security Compliance: Pitt Box & OneDrive

Pitt Box and OneDrive offer convenience to users, especially those on a mobile device. However, be aware of the following:

- Box and OneDrive use state-of-the-art technology and industry-best practices to encrypt data stored or transmitted to and from the cloud.
- **Some types of data should not be stored on Pitt Box or OneDrive** (see cloud storage data matrix on next slide).
- CSDD recommends you use only the web interface (https://pitt.box.com or http://www.office.com/) or official apps to transfer data securely. Avoid third party apps.
- If you must use a third party-developed app for Box or OneDrive, you should take steps to ensure that the app transfers data using a secure method.

http://technology.pitt.edu/services/cloud-storage-box-and-onedrive

Data Security Compliance: Pitt Box, OneDrive, Mobile Devices, and External Drives

Data Type	Permitted	Not-Permitted	Examples
Non-confidential or general business	•		
De-identified human subject research	•		Data that does not include any information which could be used to identify the individuals involved in the research.
Sensitive identifiable human subject research		•	Any individually identifiable research data containing sensitive information such as information about mental health, genetics, alcohol and drug abuse, or illegal behaviors.
Student educational records (FERPA)	•		Grades, student transcripts, degree information, disciplinary records, and class schedules.
Protected health information (ePHI-HIPAA)		•	Any unique identifying attribute, characteristic, code, or combination that allows identification of an individual, and that is combined with medical or health information. Examples include, but are not limited to, date of birth, date of death, email addresses, telephone numbers, and device ID numbers.
Social Security Numbers		•	123-45-6789
Gramm Leach Bliley (GLBA) student loans application information		•	Student loan information, payment history, and student financial aid data.
Payment card information (PCI)		•	Cardholder name, account number, expiration date, verification number, and security code.
Export controlled research (ITAR, EAR)		•	Data containing research on things such as chemical and biological agents, satellite communications, certain software or technical data, and work on formulas for explosives.
FISMA data		•	Any government data that is regulated by the Federal Information Security Management Act, including VA, FDA , and Medicare data.

Data Security Compliance: Software Licensing

- Without proper licensing, software cannot be updated.
- Unpatched software security flaws increase the potential for data theft.
- All University computers require the appropriate licensed software from Pitt Software Distribution Services (SDS) or approved software vendors via purchase requisition. All terms of the license agreement are to be enforced. Read the terms and conditions for departmental use of licensed university software.
- Any annually renewable SDS software license fee is to be paid promptly. Expired software titles must be removed from the applicable workstation.
- Illegally installed software discovered on a University-purchased computer will be removed immediately and the user will be required to purchase the appropriate license for installation.
- Installation of Pitt student-licensed software onto ANY University-purchased device is forbidden! Student-licensed software is intended for individual student use on said individual's personal device. Violation of the Software Compliance for Students policy can result in disciplinary action.
- Click here for more information on how to order Pitt licensed software titles.

Data Security Compliance: University and Public Health Policies

Be familiar with University data security policies:

- 10-02-06-University Administrative Computer Data (UACD) Security & Privacy
- 10-02-05-Computer Access and Use
- 10-02-04-Computer Data Administration
- 10-02-13-University Network
- 10-02-08-Use & Management of SSNs & University PIDs

School of Public Health computer and data policies:

https://www.publichealth.pitt.edu/ph-it-policies

Data Compliance: Starts Here

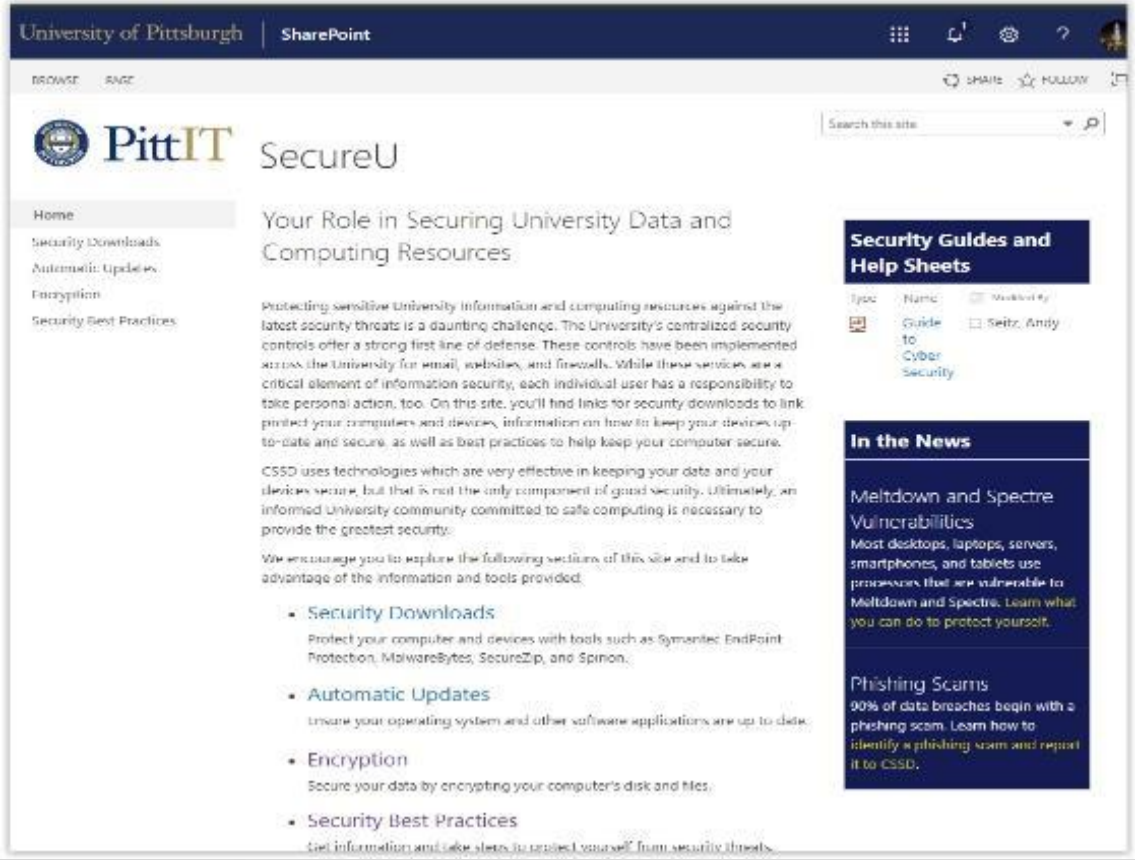
Have questions? Visit and read through this web page:

http://technology.pitt.edu/security

Data Compliance:
And Here

What's my role in securing University data and devices? Visit and read through this web page:

https://pitt.sharepoint.com/SecureU/SitePages/Home.aspx



What's next?

- Click on this link to access the Qualtrics post-test
- Contact your Public Health IT specialist for the Administrative Rights Waiver form. Sign it through DocuSign and submit it !