



School of Public Health Data Security & Computer Administrative Rights Training

- Public Health Information Technology (PHIT)
- Modified: July 19, 2023

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:

- Submitted a short justification (maximum 240 characters in length).
- Completed this educational module.
- Successfully completed a post-test with a minimum score of 80%.
- 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.

Local administrative rights

- Allows user full control over all computer settings.
- Allows user to run any / all programs, including software update programs.
- Allows user to install any programs or browser add-ons.
- Allows user to add and remove printers.
- Allows changes specific to a user's account.
- Allows direct access to operating system (WIN 10/11, Mac OS X versions Big Sur, Monterey and Ventura).

Local administrative rights: User responsibilities

- **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?

When you think of the phrase “data breach,” what comes to mind? [Members of Congress](#) having their PII and health data compromised? The second massive breach at [Uber](#)? Or the [Solar Winds](#) breach and [the intelligence fail](#) it revealed?

Consider this scenario. 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 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 type of data breach.

Perhaps you didn’t think of it as a breach. No one broke into your computer to access your information. However, the loss of your laptop or other storage device leads to the same result– sensitive work data, 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>, https://www.zdnet.com/article/uber-security-breach-looks-bad-potentially-compromising-all-systems/?ftag=TRE-03-10aaa6b&bhid=%7B%24external_id%7D&mid=%7B%24MESSAGE_ID%7D&cid=%7B%24contact_id%7D

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 across all industry to be \$4.35M in 2022, an increase of nearly 12.7% over the 2020 report.

In the education industry sector, the average total cost of a data breach was \$3.9M, a nearly 3% increase over 2020. Many universities like Pitt have a well-established research relationship with healthcare entities. The average total cost of a data breach for those organizations jumped a staggering 29.5% to over \$9.23M.

Beyond hard dollars, there are intangible 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://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/>, [Cost of A Data Breach Report 2022](#), Ponemon Institute, IBM Security Publishing (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: What Are the Costs?

attacks between 2019 and 2020.²

What is the potential impact of cyberattacks on colleges and universities?

The risks posed by cyberattacks fall into three main categories:

- ▼ **Financial:** Cybercriminals can demand large ransoms because they know the premium that schools place on protecting student data and continuing their operations.
- ▼ **Reputational:** When a breach compromises sensitive student data, the breach erodes the trust and safety felt by the school's current and prospective students.
- ▼ **Operational:** Ransomware attacks can prevent students, staff and faculty from accessing key learning and financial systems, bringing business and educational operations to a halt.



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:** Having picked a target, the attacker looks for weaknesses to exploit through 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.

Data Breaches in Higher Education: How Does it Happen?



Cyber Security Threats: An introduction



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Article 1, Section 8, Clause 8; Article 202, Article 210 of the Criminal Code of U.S.A., provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through _____

To pay the fine, you should enter the digits resulting code, which is located on the back of your _____ in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address line@fbi.gov.



OK

Cyber Security Threats: A Perspective

When you think of the phrase “cyber attack,” what comes to mind? The ransomware attacks at the [University of California](#) and [University of Utah](#)? [Colonial Pipeline](#)? [Attacks plaguing businesses in Singapore](#)? Or the government lockout of [the pacific island nation of Vanuatu](#)?

Maybe the [ransomware gang REvil](#)? Links to Russia? Or China?

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

Recently, 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 especially vulnerable. Institutions of higher learning face a constant barrage of cyber attacks. In hard numbers, this could be tens of millions of attacks per day, “typical for a research university.”

For the third consecutive year, the Sophos ***State of Ransomware in Education*** has confirmed Moody’s prediction. Of institutions polled, 64% were hit by ransomware in the past year, and 74% of those attacked said cybercriminals succeeded in encrypting their data. Over the course of one year, this was a near 20% increase in both measurements. The overall cost to remediate the attack averaged \$1.42 million – a 40% decrease over the last two years – but still slightly higher than the global average of \$1.4 million.

What impact would a cyber attack have on University education and research?



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/>

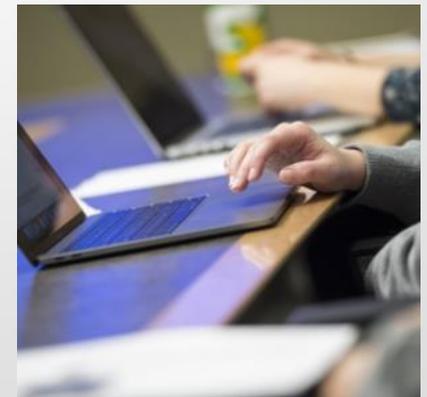
Cyber Security Threats: A Perspective

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) with differing levels of knowledge and understanding of cybersecurity to this equation, plus the changing face of the hybrid work environment, 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 , <https://www.emeraldgrouppublishing.com/calls-for-papers/cybersecurity-higher-education-sector-challenges-solutions-and-best-practices>



Common Cyber Security Attacks

- Botnets
- Malware / Spyware
- Malvertising
- Phishing / Spearfishing
- Pharming
- Ransomware
- Wi-Fi Eavesdropping
- Wireless Intercept and “Wiphishing”
- Smishing
- Juice Jacking

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



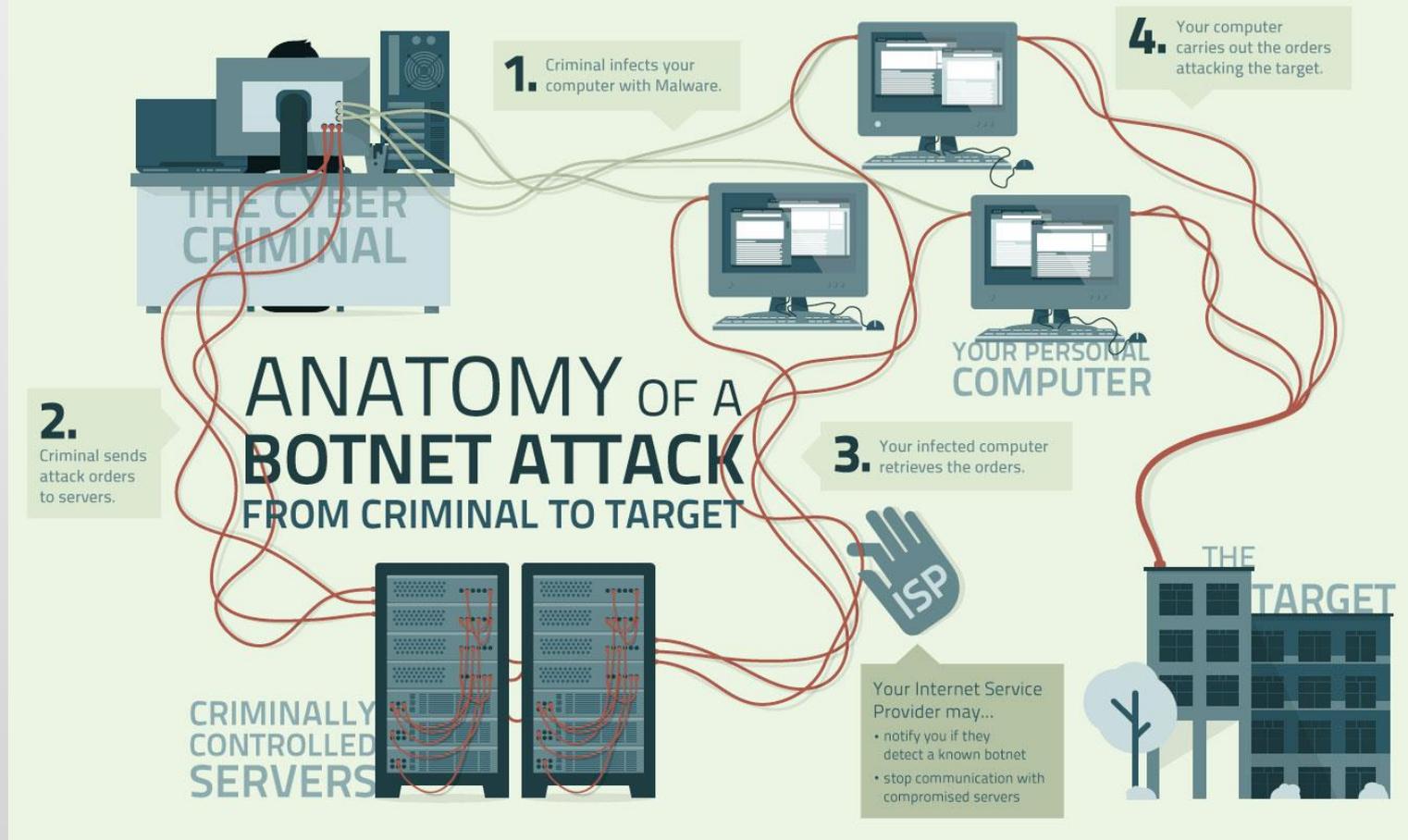
Common Cyber Security Attacks: Botnets

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: 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. Malware is an ever-changing threat. In 2018-19, the top threat was cryptocurrency mining malware, covertly installed while surfing the web. Today ransomware attacks have made the headlines of every major media outlet.

In the field of higher education, hacking or malware has been identified as a heavily used tactic to gain access. It often involved the use of a password-cracking algorithm (a technique known as "brute force") to break into a computer system and extract resources.

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/3627274/cso-global-intelligence-report-the-state-of-cybersecurity-in-2021.html> ,
<https://collegiseducation.com/news/technology/cybersecurity-higher-ed-understanding-vulnerabilities-preventing-attacks/>

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.”

<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/>

Common Cyber Security Attacks: Malvertising

WHAT IS MALVERTISING?

MALICIOUS ADVERTISING ("MALVERTISING") IS A TYPE OF ONLINE ATTACK WHEREIN MALICIOUS CODE HIDDEN WITHIN AN ONLINE AD INFECTS YOUR COMPUTER WITH MALWARE.

How MALVERTISING WORKS

YOU VISIT A WEBSITE. IT DOESN'T MATTER IF THE SITE IS SKETCHY OR LEGITIMATE -- THE THREAT LIES WITHIN THE ADS ON THE SITE.

ADVERTISEMENTS CAN COME IN A VARIETY OF SHAPES AND SIZES, THOUGH USUALLY APPEAR AS BANNERS OR POP-UPS.

MALVERTISING UTILIZES NUMEROUS TACTICS, SUCH AS USING AN IFRAME, AN INVISIBLE BOX THAT CAN SECRETLY NAVIGATE TO ADDITIONAL WEB PAGES.

THE IFRAME REDIRECTS TO AN "EXPLOIT LANDING PAGE."

THE LANDING PAGE IS WHERE MALICIOUS CODE ATTACKS YOUR SYSTEM.

THE ATTACK CODE EXPLOITS YOUR SYSTEM AND INSTALLS MALICIOUS SOFTWARE.

MALICIOUS BIDDING

CYBER CRIMINALS ARE ABLE TO UTILIZE MALVERTISING BY SUBMITTING BOOBY-TRAPPED ADVERTISEMENTS TO AD NETWORKS FOR A REAL-TIME BIDDING PROCESS.

AFTER THE AD WINS THE BID, IT IS PROPAGATED IN REAL TIME THROUGH VARIOUS PUBLISHERS AND WILL ONLY TRIGGER ITS MALICIOUS PAYLOAD IF SPECIFIC CONDITIONS ARE MET.

HARD TO CATCH

MALICIOUS ADS ROTATE IN WITH NORMAL ADS. THEREFORE, WHEN A USER VISITS AN INFECTED SITE, THEY MIGHT NOT BE ATTACKED.

BECAUSE DUPLICATING THE INFECTION IS DIFFICULT, THIS CAN MAKE IT VERY HARD FOR SECURITY RESEARCHERS TO STUDY A MALVERTISING ATTACK.

PROTECTION

USING SOFTWARE LIKE POP-UP/AD BLOCKERS OFFERS SOME PROTECTION AGAINST MALVERTISING, BUT EMPLOYING ANTI-EXPLOIT SOFTWARE IN CONJUNCTION WITH AN ANTI-MALWARE IS YOUR BEST BET.

LEARN MORE AT WWW.MALWAREBYTES.ORG.

Malwarebytes

Common Cyber Security Attacks: Malvertising

Malvertising seemed to hit a peak in 2018 when it was overshadowed by the influx of ransomware attacks. Then, induced by the work-from-home avalanche of the COVID pandemic, threat levels increased during spring and summer of 2020 with distinct surges around the July 4th and Labor Day holidays.

While these ad-based threats seem to fluctuate from year to year, 2022 saw another tremendous spike. The rate of malvertising violations has increased over 50% from 2021, with more than one in every 500 programmatic ad impressions identified as an attack.

Through the first six months of 2022, the three most-blocked ad categories by publishers were gambling (40%), pharmaceutical drugs (13%), and cryptocurrency (7%).

<https://www.clean.io/blog/q3-2020-malvertising-statistics-key-takeaways> , [Malvertising Violation Rate at Highest Level in Two Years, According to Confiant 2022 H1 Report \(prnewswire.com\)](#)

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 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
- Online dating sites
- Online betting / gambling sites

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. A 2016 campaign planted malicious advertisements at MSN.com, NYTimes.com, NFL.com, Realtor.com and Newsweek.com.

With attack vectors affecting both desktop traffic and mobile web traffic, malvertising is the silent danger lurking on both popular and NSFW web sites.

Prevention: practice safe browsing; install an ad blocker; install and regularly run anti-virus, anti-malware and anti-spyware software; maintain OS updates; remove any unneeded software (e.g., Java); 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.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 your access credentials so cyber criminals can capture them and access your banking or shopping account to 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 include: disguising a malicious link as pointing to a trusted source (e.g. exploiting misspelled URLs or using confusingly similar domains); playing on user emotions like curiosity or a sense of urgency; 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 don't know much about you, so they cast a wide net, hoping to catch any unsuspecting 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 that traditional security software (i.e., anti-virus programs) adapts poorly to attacks that rely on immediate, knee-jerk user responses precipitated by 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, then testing their response through simulated phishing expeditions.

Prevention: don't rush to click on every link, text or attachment; be skeptical of messages that seem odd or unexpected (e.g. email requests from the dean instructing the purchase of gift cards on their behalf); beware of any email whose tone is couched with an extreme sense of urgency; be alert to any message pressuring you to bypass or ignore policies and procedures, especially when concerning your password or account numbers; beware of embedded links—before clicking, hover your mouse pointer over the link to see the actual destination. Still uncertain? Forward the email to phish@pitt.edu. 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; <https://www.cnet.com/tech/services-and-software/how-to-avoid-a-spear-phishing-attack-4-tips-to-keep-you-safe-from-timeless-scams/>; <https://www.technology.pitt.edu/security/phishing-awareness-dont-take-bait>; <https://www.technology.pitt.edu/blog/avoid-getting-hooked-phishing>

Common Cyber Security Attacks: Phishing and Spear Phishing

Another reason for concern is that traditional security software (i.e., anti-virus programs) adapts poorly to attacks that rely on immediate, knee-jerk user responses precipitated by 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, then testing their response through simulated phishing expeditions, which is exactly what PITT IT does with its users. [Learn how to spot a phishing scam.](#)

PHISHING AWARENESS

Keep an Eye Out for Phishing Scams

- [Email to be Disabled and Internship Opportunity](#) scams both recently hit the University community
- [Job Opportunity Scam](#) appears to be from a Pitt email and advertises a fictitious administrative assistant job.
- [Tax Return Scams](#) are on the rise again - avoid being scammed this tax season
- [Fake Office 365 alert](#) claims the user has logged in from two universities and asks for their Pitt credentials.
- [Fake Help Desk email](#) scam looks like it's from Pitt IT and links to a fake Pitt Passport login page.

[LEARN HOW TO SPOT A SCAM](#)

Common Cyber Security Attacks: Phishing and Spear Phishing

Prevention: don't rush to click on every link, text or attachment; be skeptical of messages that seem odd or unexpected (e.g. email requests from the dean instructing the purchase of gift cards on their behalf); beware of any email whose tone is couched with an extreme sense of urgency; be alert to any message pressuring you to bypass or ignore policies and procedures, especially when concerning your password or account numbers; beware of embedded links—before clicking, hover your mouse pointer over the link to see the actual destination. Still uncertain? Forward the email as an attachment to phish@pitt.edu for analysis.

[Click here to see how and to increase your phishing awareness.](#)

For some practice, can you spot a phishing attack? [Here's a quiz to test your phishing defenses.](#)

Source: <https://www.cnet.com/tech/services-and-software/how-to-avoid-a-spear-phishing-attack-4-tips-to-keep-you-safe-from-timeless-scams/>, <https://www.technology.pitt.edu/security/phishing-scams>, [Phishing Awareness: Don't take the bait. | Information Technology | University of Pittsburgh](#)

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: [Glossary - Get Cyber Safe](#), <https://study.com/academy/lesson/what-is-a-pharming-attack-definition-examples.html>

Common Cyber Security Attacks: Ransomware

By far, **Ransomware** has the highest profile of any computing attack, and it's for good reasons. According to the U.S Treasury Department's Financial Crimes Enforcement Network, in 2021 there were 1,489 incidents costing \$1.2 billion. Victims include individuals, businesses (e.g. [Colonial Pipeline](#)), hospitals, universities, and governments ([U.S. Marshals Service](#))

The global computing environment continues to experience an increase in the volume and complexity of cyber attacks, and ransomware is by far the most common across all sectors of industry. A Sophos State of Ransomware report revealed that universities continue to be a popular attack target, with 79% reporting an attack (N=200), a 14% increase over 2022. The rate of data encryption for higher education was reported at 73% (N=157), a slight 1% decrease from 2021.

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

Sources: [U.S. banks processed about \\$1.2 billion in ransomware payments in 2021 \(cnbc.com\)](#); [Ransomware: A cheat sheet for professionals | TechRepublic](#); That State of Ransomware 2023 (SOPHOS whitepaper) PDF

Common Cyber Security Attacks: Ransomware

Example of a “detection of illegal activities by authorities” Lockscreen

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.



Common Cyber Security Attacks: Ransomware

Example of a Ransomware Encryption screen



The screenshot shows a ransomware interface with a dark background and a binary code pattern. At the top, there is a navigation bar with the logo "PETYA RANSOMWARE" (a hammer and sickle icon) and links for "Start", "Payment", "FAQ", and "Support". A language dropdown menu is set to "English".

The main text reads: "Your computer has been encrypted". Below this, a paragraph explains: "The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer."

A timer is displayed with the text: "⌚ The price will be doubled in:" followed by "6 days 13 hours 43 minutes 10 seconds".

At the bottom, there is a red button with a white envelope icon and the text "Start the decryption process".

Common Cyber Security Attacks: Ransomware

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

- Do not pay the ransom
- For a University computer, immediately contact either the Public Health Information Technology Group (phit@pitt.edu) or PITT IT (helpdesk@pitt.edu)
- For a personal computer, have your device analyzed by a reputable IT technician / forensic specialist

Common Cyber Security Attacks: Ransomware

Ransomware: A Defense Strategy

- In higher education sector, the root cause of ransomware is the exploitation of 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. Compromised credentials are the second leading cause of ransomware attacks. Do not click on links asking you to verify your username or password. PITT IT and credible businesses will never ask you to verify your system credentials.
- Be proactive: make certain MalwareBytes Endpoint has been installed onto your University computer -  in task bar. If you need assistance, [place a ticket](#) with Public Health Information Technology. Mac users: take advantage of [MalwareBytes Premium available to Pitt users](#). Perform regular malware scans on your computer.
- For your laptop or home computer, be **doubly** proactive: schedule and perform a regular backup (daily or weekly) to a removable external device 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/10-tips-to-avoid-ransomware-attacks/> , [Ransomware: A cheat sheet for professionals | TechRepublic](#) ; [How to Protect Yourself from Ransomware \(kaspersky.com\)](#) ; The State of Ransomware 2023 (SOPHOS whitepaper) PDF

Common Cyber Security Attacks: Wi-Fi Eavesdropping

Wireless (Wi-Fi) networks use radio waves to connect mobile devices to the internet. This leaves them vulnerable to **Wi-Fi Eavesdropping**, also known as a **packet sniffing or snooping attack**. This is a method to capture data as it is being sent or received by its user through virtual “listening in” over an unsecured (unencrypted) wireless network. Using the right equipment on a vulnerable network, cyber criminals can potentially access your computer, capturing passwords and login information.

This type of attack can be difficult to detect because the network transmissions will appear normal. To be successful, an eavesdropping attack requires a weakened connection between client and server that the attacker can exploit to reroute network traffic. The attacker then installs the monitoring software (packet sniffer) onto your device to intercept data in transit.

Prevention: never trust public Wi-Fi networks; use a strong password and change it frequently; use a personal firewall; use a virtual private network (VPN); verify the HTTPS version of websites – 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.

Sources: [How To Prevent Wireless Network Attacks \(purplesec.us\)](https://purplesec.us) ; [Wi-Fi Eavesdropping: what is it and how to avoid this problem \(techunwrapped.com\)](https://techunwrapped.com)

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>

Common Cyber Security Attacks: Report A Security Concern to PITT IT

A screenshot of the PITT IT Security page. The page has a blue header with navigation links: HELP DESK, SECURITY (highlighted), SERVICES, SOFTWARE, TRAINING, and ABOUT. There are social media icons for Facebook, Instagram, Twitter, and YouTube. The main content area is white with the heading "Security". Below the heading is a paragraph: "Students, faculty, and staff of the University of Pittsburgh have access to many security services and tools that protect devices, safeguard personal information, and secure sensitive data. [Contact PITT IT](#) for 24/7 support, security guidance, and to request personalized consultations from the PITT IT Security team." Below this is a section titled "24/7 IT SECURITY SUPPORT" with the heading "Report a Security Concern". The text says: "If you have any reason to suspect a security issue, contact the Pitt IT Security team immediately so that we may assess the issue." Below this is a section titled "Possible security issues include:" followed by a bulleted list: "Lost or stolen equipment", "Virus, spyware, or other malicious programs found on your computer", "Unauthorized disclosure of sensitive information stored on a computer", "Accidentally opened attachments or clicked links that appear malicious", and "Suspected phishing email". At the bottom of this section is a blue button that says "HOW TO REPORT A SECURITY ISSUE". To the right of the text is an image of a young woman with dark hair sitting at a computer workstation, smiling at the camera. The computer screen shows a website with the heading "Are You Safe?".

Security

Students, faculty, and staff of the University of Pittsburgh have access to many security services and tools that protect devices, safeguard personal information, and secure sensitive data. [Contact PITT IT](#) for 24/7 support, security guidance, and to request personalized consultations from the PITT IT Security team.

24/7 IT SECURITY SUPPORT

Report a Security Concern

If you have any reason to suspect a security issue, contact the Pitt IT Security team immediately so that we may assess the issue.

Possible security issues include:

- Lost or stolen equipment
- Virus, spyware, or other malicious programs found on your computer
- Unauthorized disclosure of sensitive information stored on a computer
- Accidentally opened attachments or clicked links that appear malicious
- Suspected phishing email

[HOW TO REPORT A SECURITY ISSUE](#)



Click [here](#) for guidance on how to report a security incident with your laptop.

Mobile Security Attacks: Smishing

The Coronavirus pandemic brought an increase in regular phishing attacks through email. With an increased dependence upon smartphones, attackers set their sights upon the device that is kept within arm reach of hundreds of millions of users. That means just about everyone has been subjected to an SMS-based scam, popularly known as **Smishing**.

Data from the anti-spam firm Teltech shows 11.6 billion scam texts were sent over US wireless networks during the month of March 2022. According to Robokiller, that meant the average US mobile customer received 42 scam texts during that same month.

While Smishing is hardly new, the increased use of the personal smartphone in the workplace has created a new sophisticated variant called the boss text. Here attackers spoof a supervisor's phone number to trick subordinates into purchasing gift cards. Targeting employees on their personal devices helps bypass security protections that have been activated on employer-run systems and devices.

Combating this social engineering-based attack is a challenge. The saying, "It's easier to hack a person than to hack technology," is a reality. Complacent users and the absence of any real spam filtering on SMS carrier systems virtually guarantees delivery of these bogus messages. Then, it's up to the human factor – how educated and vigilant is the user – to combat these increasing attacks.

Mobile Security Attacks: Smishing



Example of malicious SMS attacks on mobile

Mobile Security Attacks: Smishing

How to combat against smishing?

- Use an employer-provided device with managed security
- User training to educate on the identification of scam texts
- Preview links before clicking on them. Make certain there are no misspellings in the URL and proper domains are used (.edu, .com, .net)
- Be suspicious of out-of-the-blue messages and emergency notifications connected to credit cards and bank accounts. Don't be afraid to question any email, text, phone call or SMS message
- Independently verify claims made by an unsolicited message

Mobile Security Attacks: Juice Jacking

Here's a common scenario: you are at the airport, and you've been using your phone while waiting on your flight. Then you're notified the flight has been delayed for three more hours. Your phone battery is low, so you walk over to an airport charging station to give your phone a boost.

WAIT! You could be a victim of **Juice Jacking**.

Juice Jacking is a security exploit in which an infected USB charging station is used to compromise connected devices. While your phone is charging, a perpetrator could be loading your device with a virus or malware that could track your keystrokes or steal your data.

When your device is connected to another destination, it becomes vulnerable because power and data stream through the same cable. If someone is on the other end, they may be able to move data between your device and theirs.

If the perpetrator completes a successful transfer, he may obtain enough personal information to impersonate you or gain access to your financial accounts. Or he could install malware which gathers data like GPS location, purchases, pictures, social media interactions, or a program that clones your phone and transfers it back to the perpetrator's device.

[What is juice jacking? Think twice before using public USB ports | NortonLifeLock](#)

Mobile Security Attacks: Juice Jacking

Do you often charge your mobile device from public ports while travelling? Did you know this can lead to "**Juice Jacking**" ?

Beware of Juice Jacking

Attackers use USB charging ports available at public places to install malware, steal data or even take complete control of your device.



Tips to stay safe



Disable data transfer feature on your mobile phone while charging



Get a charge only cable instead of cable supporting charging and data transfer capabilities



Try to carry a power bank



If possible, switch off the device while charging from public ports

Mobile Security Attacks: Juice Jacking



An April 2023 tweet by the FBI advised all travelers and commuters to avoid suspiciously free charging stations for fear of juice jacking.

Mobile Security Attacks: Juice Jacking

The number one solution to this danger: Do **NOT** charge your device through a public outlet. Although hacked USB ports are less likely in a high-security area like an airport, **there is no guarantee** these kiosks have not been tampered with. Juice jacked chargers are quickly installed and difficult to detect.

But when the need arises, be prepared to take charge of charging your device!

You can protect yourself from **Juice Jacking** by:

- avoid third-party public charging stations or public kiosk chargers
- carry a personal charge bank
- if you must use a public charging station, use a [USB data blocker](#) (aka USB condom) which disables the data pin on the pass through between device and the USB charger
- use a wall outlet in a public area

[What is juice jacking? Think twice before using public USB ports | NortonLifeLock](#) , [FBI warns of public 'juice jacking' charging stations that steal your data. How to stay protected | ZDNET](#)

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/cmpters-tblts/wf-ntwrks-en.aspx>;

[How To Prevent Wireless Network Attacks \(purplesec.us\)](http://purplesec.us)



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> ; [How To Prevent Wireless Network Attacks \(purplesec.us\)](http://purplesec.us)

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 2023](#).

<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>; [Is Your Home Wi-Fi Secure? Here Are 10 Tips to Lock Down Your Network - CNET](#)

Data Security: University Practices

- Create a strong password and change it regularly
- Use a current version of Windows (WIN 10/11-22H2) and Mac OS (Monterey / Ventura)
- 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 (twelve or 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

[Password Best Practices and Standards | Information Technology | University of Pittsburgh](#); [Eliminate Cyberfilth — 7 Password Hygiene Tips | Information Technology | University of Pittsburgh](#)

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 typical 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 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/picks/the-best-password-managers>

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 features and 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 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

<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

Data Security Compliance: Data Risk Categories

- “The University of Pittsburgh takes seriously its commitment to protecting the privacy of its students, alumni, faculty and staff, and protecting the confidentiality, integrity, and availability of information essential to the University's academic and research mission. For that reason, we classify our information assets into **risk categories (high, moderate, low)** to determine who may access the information and what minimum security precautions must be taken to protect it against unauthorized access.”
- **Note:** “The PITT IT Security team must assess all systems that transmit, process, or store data classified as Restricted. Please contact the 24/7 IT Help Desk with questions about the 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

Data Security Compliance: Data Risk Classification Matrix

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

*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: Data Classification Compliance

- “Protecting sensitive data is a shared responsibility. Pitt IT provides guidance and resources to store data securely. You are responsible for ensuring that your use of permitted services complies with laws, regulations, and policies where applicable. Entering data into AI tools such as ChatGPT carries the inherent risk of that data being compromised or mishandled, potentially leading to serious consequences such as privacy violations, financial loss, or reputational damage. The use of restricted or private data in these tools is prohibited.” **Please contact the 24/7 IT Help Desk with questions about the appropriate protection of information.**
- **Note:** The PITT IT Security team must assess all systems that transmit, process, or store data classified as Restricted. Please contact the 24/7 IT Help Desk with questions about the 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.

Data Security Compliance: Data Classification Compliance Matrix

Key						
	Data type is permitted. Please follow the Security Guide where available.					
	Data type is generally permitted. Contact Pitt IT for a security consultation before use.					
	Data type is not permitted due to regulatory compliance or high risk.					
Data Classification Levels						
Restricted	High risk, sensitive data – Disclosure may cause severe harm					
Private	Moderate risk, confidential data – Disclosure may cause harm					
Public	Low risk internal or public data – Disclosure poses little to no harm					
Service Security Guide	Maximum Acceptable Data Class	REGULATED DATA				
		FERPA Non-Directory Student Records	GLBA Student Financial Information	HIPAA Protected Health Information	NIST 800-171 Controlled Unclassified Information	PCI DSS Payment Card Information
Enterprise Cloud Computing Amazon Web Services, Google Cloud Platform, Microsoft Azure	Restricted					
Cloud Storage OneDrive/SharePoint <ul style="list-style-type: none"> ▪ OneDrive Security Guide ▪ SharePoint Security Guide 	Restricted					
Cloud Storage G Suite/Google Drive <ul style="list-style-type: none"> ▪ Google Drive Security Guide 	Public					
Document Management Perceptive Content/ImageNow	Restricted					
eFax	Restricted					

**Note: this is only a partial listing of regulated data services. The complete list can be found at <https://www.technology.pitt.edu/security/data-risk-classification-and-compliance>

Data Security Compliance: Data Classification Compliance and PITT Services

From cloud storage to Zoom for HIPPA, protecting sensitive data while using the plethora of digital services made available to Pitt users is a shared responsibility. How and when to use which service can be a complicated undertaking. Can you answer any of the following off the top of your head?

- Which cloud services are approved for storage of Protected Health Information (PHI)?
- Is DropBox® an approved University cloud data storage service?
- Can PHI be collected through the Qualtrics survey system?
- Pitt email service is offline. Can I send important student financial information through my personal Gmail account?
- Can HIPPA Zoom conferences be recorded? If so, where can these recordings be securely stored?

Remember: YOU are **responsible** for ensuring that YOUR use of permitted University services complies with laws, regulations, and policies where applicable. Pitt IT provides guidance and resources to store data securely. Start by consulting the Data Classification Compliance services table located here:

<https://www.technology.pitt.edu/security/data-risk-classification-and-compliance>

Generally, you should contact PITT IT for a security consultation before storing data in the cloud. Please contact the 24/7 PITT IT Help Desk with questions about the appropriate storage and protection of University information.

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)

[How To Prevent Wireless Network Attacks \(purplesec.us\)](#); <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 PITT IT 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 the Global Protect app is mandatory.

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

Data Security Compliance: University of Pittsburgh OneDrive

Microsoft OneDrive is the approved cloud storage service of the University of Pittsburgh. It offers convenience to users, especially those using a mobile device. However, be aware of the following:

- OneDrive uses 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 OneDrive** (e.g. SSNs and payment card information).
- If you must use a third party-developed app for OneDrive, you should take steps to ensure that the app transfers data using a secure method.
- Some users may have a personal Microsoft account. Make certain University data is stored inside your University of Pittsburgh OneDrive folder.
- See [how OneDrive works](#) and learn more about University OneDrive [here](#).

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: Other Cloud Storage Services

Box and Dropbox are other cloud collaboration solutions used by some students, faculty, and staff. Before considering the use of Dropbox or Box, please keep in mind that they are not an enterprise service offered through or supported by the University of Pittsburgh. Box and Dropbox offer similar features to OneDrive, but OneDrive offers several advantages for University use.

Feature	OneDrive	Box	Dropbox
Anytime, anywhere access to cloud files	Yes	Yes	Yes
Simple sharing and collaboration features	Yes	Yes	Yes
File versioning	Yes	Yes	Yes
Integrates seamlessly with other Office 365 collaboration tools like Teams and SharePoint	Yes	No	Yes
Automatically integrates with the University's Multifactor Authentication (Duo) service for enhanced security	Yes	Yes	No
Can be approved as storage solution for certain classes of restricted data after consultation with Pitt IT	Yes	Yes	No
Fully supported by Pitt Information Technology	Yes	No	No
Cost	Included in Microsoft Campus Agreement	Purchased separately by users/departments	Purchased separately by users/departments

Dropbox is not supported by Pitt information Technology, nor is it approved for University data storage use.

<https://www.technology.pitt.edu/services/cloud-collaboration-box-and-onedrive>

Data Security Compliance: Other Cloud Storage Services

Google Drive

Google Workspace (formerly G Suite) is a cloud-based suite of productivity and collaboration tools. It brings together popular Google apps, such as Drive, Classroom, Meet, Calendar, and Docs, into a single integrated workspace.

The Google Workspace referenced here is **NOT** your personal Google account. This is an account created with and connected to your Pitt user account. Remember the best practice is to keep personal files separate from official University business files.

When using Google Workspace with your Pitt username and password, the University's single sign-on service (Pitt Passport) and Multifactor authentication (Duo Security) provide an increased level of protection and security for your Google Workspace information and data when compared to personal access to Google Workspace

While this service is available to University faculty, staff and students, **Pitt IT strongly discourages the use of [Google Drive](#) for several reasons:**

- It is not permissible to store Protected Health Information (see the University's [Data Risk Classification and Compliance matrix](#)).
- Google has made changes that restrict options for storing flexible, large volumes of data.
- Free Google Drive accounts include only 15 GB of free storage.

Due to these and other limitations, PITT IT does not endorse Google Drive as a viable, long-term solution for most University users.

<https://www.technology.pitt.edu/services/cloud-collaboration-box-and-onedrive> ; <https://www.technology.pitt.edu/services/google-workspace>

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:

- [AO 35-University Administrative Computer Data \(UACD\) Security & Privacy](#)
- [AO 10-Computer Access and Use](#)
- [AO 11-Computer Data Administration](#)
- [AO 38-University Network](#)
- [CS 23-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>



HELP DESK SECURITY SERVICES SOFTWARE TRAINING ABOUT

Security

Students, faculty, and staff of the University of Pittsburgh have access to many security services and tools that protect devices, safeguard personal information, and secure sensitive data. [Contact Pitt IT](#) for 24/7 support, security guidance, and to request personalized consultations from the Pitt IT Security team.

24/7 IT SECURITY SUPPORT

Report a Security Concern

If you have any reason to suspect a security issue, contact the Pitt IT Security team immediately so that we may assess the issue.

Possible security issues include:

- Lost or stolen equipment
- Virus, spyware, or other malicious programs found on your computer
- Unauthorized disclosure of sensitive information stored on a computer
- Accidentally opened attachments or clicked links that appear malicious
- Suspected phishing email

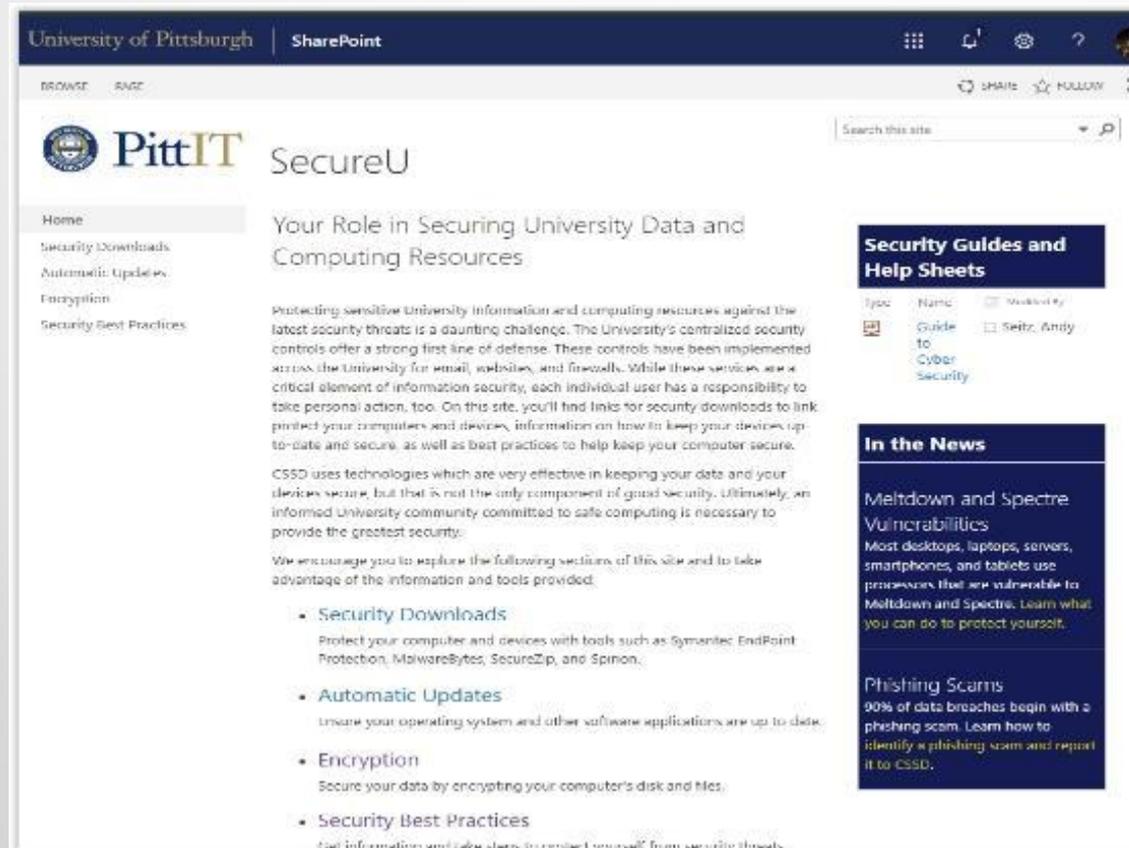
[HOW TO REPORT A SECURITY ISSUE](#)



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>



The screenshot shows the SharePoint interface for the University of Pittsburgh's SecureU site. The header includes the University of Pittsburgh logo and the text "SharePoint". Below the header, there is a navigation menu with "Home", "Security Downloads", "Automatic Updates", "Encryption", and "Security Best Practices". The main content area features the title "Your Role in Securing University Data and Computing Resources" and a detailed introduction about the challenges of securing university information. A list of resources is provided, including Security Downloads, Automatic Updates, Encryption, and Security Best Practices. On the right side, there are two featured sections: "Security Guides and Help Sheets" and "In the News".

University of Pittsburgh | SharePoint

BROWSE PAGE

SHARE FOLLOW

Search this site

PittIT SecureU

Home

- Security Downloads
- Automatic Updates
- Encryption
- Security Best Practices

Your Role in Securing University Data and Computing Resources

Protecting sensitive University information and computing resources against the latest security threats is a daunting challenge. The University's centralized security controls offer a strong first line of defense. These controls have been implemented across the University for email, webfiles, and firewalls. While these services are a critical element of information security, each individual user has a responsibility to take personal action, too. On this site, you'll find links for security downloads to link protect your computers and devices, information on how to keep your devices up-to-date and secure, as well as best practices to help keep your computer secure.

CSSD uses technologies which are very effective in keeping your data and your devices secure, but that is not the only component of good security. Ultimately, an informed University community committed to safe computing is necessary to provide the greatest security.

We encourage you to explore the following sections of this site and to take advantage of the information and tools provided.

- Security Downloads**
Protect your computer and devices with tools such as Symantec EndPoint Protection, MalwareBytes, SecureZip, and Spinon.
- Automatic Updates**
Ensure your operating system and other software applications are up to date.
- Encryption**
Secure your data by encrypting your computer's disk and files.
- Security Best Practices**
Get information and take steps to protect yourself from security threats.

Security Guides and Help Sheets

Type	Name	Availability
Guide	Guide to Cyber Security	Seitz, Andy

In the News

Meltdown and Spectre Vulnerabilities

Most desktops, laptops, servers, smartphones, and tablets use processors that are vulnerable to Meltdown and Spectre. Learn what you can do to protect yourself.

Phishing Scams

90% of data breaches begin with a phishing scam. Learn how to identify a phishing scam and report it to CSSD.

What's next?

- [Click on this link to access the Qualtrics post-test](#)
- Contact your Public Health IT specialist to request the Administrative Rights Waiver form.
- Submit your justification statement (240 characters max.) to be added by your Public Health IT specialist.
- Sign it through DocuSign and submit it !
- Schedule a time with your Public Health IT specialist to update the account on each of your computers.