Title page
Information Security 101. This training was created by the UW Office of the Chief Information Security Officer (CISO)

Instructions
Use this slide to adjust your speaker volume or headset.
It will take approximately 20 minutes to complete this training.
The resources mentioned are linked in this web page in the navigation bar. They are listed in the order referenced in the training.
A glossary of terms are available by clicking the “glossary” link.
An accessible transcript can be accessed by clicking the “transcript” link and a PDF version can be found on that page as well.

Scenarios
On Tuesday, the 15th of August, at 12:59 in the afternoon, a medium sized bee landed on the windshield of a car in a University Hospital parking lot. At that exact moment, a USB thumb drive was dropped nearby potentially exposing thousands of patient records.

Meanwhile over on the other side of the University campus, an unencrypted laptop containing employee and student records was stolen from a car putting hundreds of members at the UW community at risk for identity theft.

Simultaneously in an adjacent building, a University employee moved an old and ugly filing cabinet out in the hallway to be sent to surplus, but neglected to clear out the bottom drawer which contained valuable research papers.

Downstairs, a print out of an email left unattended on a multifunction device revealed an employee sick leave request to her boss (*gasp*), along with the fact that she has a bad case of athlete's foot (*gasp*).

And at the very same time on the campus lawn, Rudolph Willhem Von Weinerdog unable to resist the exciting promise of the new contact on Linkedin (*oohhh*), clicked on the link on an email from someone he never heard of was led to a phony phishing website that instantly downloaded malware onto his computer and then noticed his laptop was running slow.

Did all of those things really happen on August 15th at the very same time? No, they didn’t. But a variation of all of those things happen at some point at some University? Yes they have, except dogs don’t use computers! At least not that we know of.

Objectives
As a University of Washington employee, you are responsible for:
- Knowing and adhering to UW Administrative Policy Statements related to information security.
- Safeguarding UW data from unauthorized access and exposure.
- Reporting any suspected breach or misuse of University institutional information.

This training is intended to help you learn more about these responsibilities.

**Things to Know**
A plan to safeguard your personal and UW institutional data begins with knowing the following about the data you access, transmit, or store:

- How it is classified.
- Who should have access.
- What the threats and risks are.
- Methods of encrypting it.
- Where it is stored.
- And which UW policies apply.

**UW Data Classification**
At UW, data is classified as UW Confidential, Restricted, or Public.

UW Administrative Policy Statement (APS) 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions defines these data types.

Additionally, data classification definitions and examples can be found on the UW Privacy Office page linked on this web page. It’s important to understand the distinctions between the data types and secure data accordingly.

Note that electronic passwords, including your UW NetID credentials, are considered UW Confidential data and should be protected as such.

**Data Classifications**

**Access Privileges**
Once you determine what types of data you have you may want to consider who should have access to it.

UW APS 2.4 refers to the "principle of least privilege," which means that UW data, information, and information systems should be accessed only on a need-to-know basis. As a UW employee, you should only access the data needed to be able to fulfill your job functions and only allow access to data in your possession by those who have a need to know for their work responsibilities.
By observing this principle, you can help protect University and personal data from unnecessary disclosure, transmission, and storage and decrease the possibility of an incident or breach.

**Threats to Data**
Threats and risks to data are discussed throughout this training, but it is important to point out that one of the most common threats to your personal and UW institutional data is phishing.

Phishing is a form of Internet fraud in which cyber criminals send emails to entice victims into inadvertently surrendering UW NetIDs and passwords (credentials) and other personal information.

Phishing emails are sometimes used in tandem with malicious software, or “malware,” which can be downloaded through an infected attachment or url that is delivered with the phish. Malware can be used to disrupt a system’s normal operation or to help cyber thieves harvest valuable data on individual computers and devices, or on networks.

Ransomware is a form of malware that can be used to lock up computers and make data inaccessible until the owner of the device pays a ransom.

**Phishing training**
**Malware and Ransomware Risk Advisory**

**Accidental and Malicious Exposure**
Phishing and malware are two methods that cyber criminals might use to steal or access student, employee, and patient data. But there are other methods and various motivations for cybercriminals and other malicious hackers to infiltrate networks at universities.

They also target University credentials to access intellectual property, valuable research, and resources such as the UW's library system. Additionally, they can sell credentials and other valuable data on underground market places. "Hacktivists" can use stolen credentials to deface public-facing content on UW websites.

But don't just think of cybercrime when it comes to data loss. Each year there are scores of reported incidents of accidental loss or disclosure of data at universities. Sometimes it is because of flaws or vulnerabilities inherent in technological systems, but these incidents and data breaches often involve a human element.

**Two States of Data**
When we talk about threats to data--whether by malicious access or accidental exposure--and what to do to mitigate those threats, it's helpful to think about the states of data usage.
Data stored on computers, laptops, mobile devices, and in spreadsheets, databases and information systems is termed "data at rest."

When it is transmitted via the Internet, email, or private or public networks, it is termed "data in transit" or "data in motion."

The distinctions between these two states aren't completely clean--data that is stored in a browser might also be in transit via wireless transmission.

**Data Encryption**

One way to prevent unauthorized access to data at rest or in transit states is by using encryption.

Encryption is the process of encoding either data or communications so that only authorized parties can access it.

Encryption uses a mathematical algorithm or cipher to transform information from a readable form (plaintext) into a form (ciphertext) that is unreadable by anyone that does not have the electronic password, or key. Decryption is the reverse process.

There are multiple ways to use encryption with digital communications: for data at rest, individual files and folders may be encrypted, and so can hard drives, mobile devices, and other types of data storage. For data in transit, encryption can be used for email, network, Internet, and wireless communications.

There are risks involved in using encryption. If you lose track of your key when using whole disk encryption, for instance, the data on it will be unrecoverable. Keeping track of electronic keys as well as backups for important data is vital.

**Know Where Your Data is Stored and Lock it Up**

When you want to protect something of value, it's typical for locks and keys to be involved. Encryption, along with things like strong passwords and access privileges, is a good way to lock up your data to keep it secure.

Think all of the places we store data—on desktop computers, mobile devices, portable storage media, and on paper and in filing cabinets—just for starters.

Now think of all of the places that data can be stored on just one machine or device—in email, browser history, applications, text files, spreadsheets, temporary files, and other places that may or may not be obvious.

Each of those types of storage is a way that data can be maliciously stolen or accidently exposed. First let's consider some of the specific risks of data at rest and ways to lock it up.
Desktop Computers
Desktop computers store data in ways you may not be aware of. For instance, even after you delete a file, the information may still be accessed on your computer by cyber thieves and other interested parties. Protect desktops with a strong password, encrypt the hard drive, wipe data from the drive before sending it to surplus, and use physical security measures to keep them from being stolen. More information can be found by clicking the “securing your computer” link on this web page.

Mobile Devices
Using your smartphone to respond to work emails, download files with institutional information, and access University applications represents potential risks to UW data that you are responsible for managing. As with desktop computers, data may be stored and/or exposed in unexpected ways. Click the “mobile devices” link for more information.

Portable Storage Devices
USB devices, such as thumb drives and external storage drives, pose various risks.

- Data stored on the device could be exposed if it is misplaced, lost, or stolen.
- You could infect your computer if you insert a USB device that carries malware.
- By the same token, attached storage devices could be infected by malware on your computer. If your computer is infected by ransomware, for instance, any connected devices may be impacted as well.

Browsers
Information entered on a browser may be stored in places such as in the browser cache, in temporary files, and on merchant and application servers and databases. This information may be discovered by thieves who know where to look.

- Don't enter personal or financial information in browsers on public or unfamiliar devices.
- Don't have online accounts and applications remember credit card numbers, passwords, and other financial or personal information--even on your personal computer or device.
- Enter only the minimum amount of information needed for transactions.
- Only enter personal and financial information on secure websites - look for "https" and a lock symbol.
Click the “https” link for more information.

Applications
As with browsers, data entered into applications on computers and smartphones may be stored in unexpected places. Only use trusted applications, delete ones you no longer use, and only enter the minimum data needed to use the application.

Paper and Filing Cabinets
Some breaches involve data that is on paper. In fact, one of the first settlements for $1,000,000 related to a HIPAA violation occurred because of patient data in paper form that was left on a subway.

[More information about that case]

Remember to clean out filing cabinets before sending them to surplus and keep printers and common areas clear of confidential and restricted data. Additionally,

- Purge data you are no longer required to keep.
- Check all drawers before sending cabinets to surplus.
- Secure confidential and restricted data in locked cabinets as appropriate.
- Don’t leave confidential and restricted information on copiers, on other office machines or in common areas.
- When purging paper data, confidential/restricted records should be shredded using an office shredder or an approved contracted document disposal vendor.

Sharing and Transmitting Data
Data in transit or in motion carries some risks that are distinct from risks to data at rest. For instance, when you send an email, it typically takes a long and winding journey through various networks. Anyone with the right tools can intercept your message as it moves along this path. If you are using your smartphone in a cafe, eavesdropping tools might also be used to view your data and activities on the WiFi network.

But UW offers tools you can use to block these types of intrusions: Eduroam, a free encrypted wireless service, and Husky OnNet, a service that creates a virtual private network (VPN) by encrypting traffic from remote locations to the University. More information about these services can be found in the “Things to Do” section of this training.

[Eduroam]
[Husky OnNet]
[Encryption Risk Advisory]
Know the Policies
The UW Office of the CISO develops and facilitates University-wide information security policies to manage due-care and respond to changes in laws and regulations.

- Policies represent rules that are published in the UW policy directory.
- Guidelines are recommendations, advice, or procedures that help explain how University rules and policies are implemented.

The UW Administrative Policy Statements and UW Information Security Guideline are linked on this web page.

UW Policies

Things to Do
At the core, protecting information is being aware that the data you have stored in your devices and systems is valuable, to you and others and remembering that it should be kept secure. While best practices and checklists are not the perfect panacea, that doesn't mean they aren't useful and necessary. They are an important part of keeping track of many details associated with maintaining technology. Remember they are not the end points of awareness, only the beginning. Here's a list of fundamentals to get you started:

Update and Patch
Many data breaches occur because operating systems and other types of software are not fully updated and patched, making them vulnerable to malware infections and other types of malicious hacking. It is vital to keep all software on all machines and devices up to date, and to uninstall software that you are not using.

More information:
Update and Patch Risk Advisory

Use Antivirus Software
Anti-virus software can help protect computers and devices from various forms of infection, but it must be kept up to date. Members of the UW community can install a free version of Sophos anti-virus for home use and for unmanaged University-owned computers and devices. Click the “Sophos” link for more information.

Sophos anti-virus software (for the UW community)
Sophos for mobile devices

Limit Administrative Account Usage
When malware infects a computer or device, it often can only access files, folders, and applications available to the account that is in use at the time of infection.

For this reason, to minimize the potential scope of damage in case of a successful
attack, it is best to only use administrative accounts when it is absolutely necessary. Limiting administrative account use on machines to only what is essential is a way to implement the principle of least privilege.

**Employ Strong Passwords and Use Pins**

Locking devices with a password or pin, creating an appropriately complex password or passphrase for user accounts, and avoiding using the same password for multiple accounts are some of the simplest ways to safeguard valuable personal and University data.

It can be difficult to remember all of your passwords and passphrases, particularly if they are as strong as they need to be to secure data. Password managers can be used to create, store, and access complex passwords as you need them. Password managers require you to remember only one master password in order to access the others you have stored in the service. So if you use a password manager, create a hint to help you remember your master password. If you must write it down, be sure to store it in a safe place.

**Use Multifactor Authentication**

Multi-factor authentication or MFA adds an additional layer of protection in addition to your password. At the UW, Duo, an MFA service, has been added to secure applications that access institutional data. For more information about enrolling your device in the Duo service, click the "MFA" link.

**Encrypt Whenever Possible**

Remember to use encryption when and wherever possible. There are multiple ways to encrypt data at rest and in transit: individual files and folders may be encrypted, and so can hard drives, mobile devices, and email, network, Internet, and wireless communications. Click the “encryption” link for more information.

**Use Eduroam**

At UW campuses, you can use eduroam, a free encrypted service, to provide additional security on wireless networks. In addition to providing an extra layer of security on campus, this service allows users from the UW to securely access the internet from any eduroam-enabled institution throughout the world. To learn more, click the “eduroam” link.

**Use Husky OnNet**

If you are working remotely and want to connect to University resources and applications, you can use Husky OnNet, a virtual private network or VPN service. Husky OnNet provides an encrypted connection to the UW from remote locations. Such as from home, coffee shop or at the airport. An encrypted connection provides greater security when you use your UW NetID password and other passwords to access the UW network. For more information, click the “Husky OnNet” link.
**Be Selective**
Be selective about which computers you access data and use your passwords on. If possible, avoid using shared computers such as those in Internet cafés and public kiosks.

**Back It Up!**
Back up your machines, devices, databases, and systems on a regular basis in case they are lost, stolen, inappropriately accessed, or corrupted.

Ransomware locks data and devices until a sum of money is paid to attackers. If your computer is infected by ransomware, back ups may be the only way to recover lost data.

Back up all data that you are responsible for, using multiple methods or formats. Backup devices that are connected to computers may also become infected, so have at least one backup that is offline.

**Wipe Data from Devices**
Discarded desktop computers, laptops, and mobile devices may contain personal and UW information that could be discovered and fall into the wrong hands if the physical device is not wiped and disposed of in a secure fashion.

If data is not deleted in the proper way prior to disposal or sending it to surplus, then there is the potential for a data breach. UW's moving & surplus team will purge data from University computers, either with erasure software or by physically destroying the drive. However, all UW departments and end users should assist in this process by reviewing the data stored on any device and deleting confidential and restricted information.

Options for wiping machines and devices vary according to the system. Check operating system or manufacturer instructions for the appropriate procedures.

[Secure Disposal Risk Advisory](#)

**Report Suspected Incidents Promptly**
If you suspect an information security or privacy incident or breach, it is important to report it immediately. If it is determined that notification is required, state law requires that those affected be notified within 45-60 days.

Who you report the incident to depends on the type of data that is involved. Click the report and incident link for more information about determining the delegated authority for different types of data.
If you are unsure about what types of data are involved, contact the UW Office of the CISO at ciso@uw.edu or (206) 685-0116 for assistance.

Credits and Contact
For questions about this training, contact ciso@uw.edu or check out our website at ciso.uw.edu

Narration:
Jeff Blancato
Knowledge Management Specialist, UW Integrated Services Center

Content Developed by:
Melissa Albin
Information Security Analyst
UW Office of the Chief Information Security Officer
malbin@uw.edu

Designed by:
Tiffany Truong

Photos by:
UW Photo Database