Passwords and Passphrases
This training was created by the UW Office of the Chief Information Security Officer (CISO) to provide guidelines and best practices for password usage.

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 as additional resources on this web page in the navigation bar. They are listed in the order referenced in the training. A glossary of terms is 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.

Course Objectives
This training is intended to teach:

1. Why passwords are important for safeguarding personal and institutional information,
2. Ways passwords may be stolen by cyber criminals to access or steal valuable data,
3. Risks and threats to data that may impact you and ways to mitigate them with strong passwords,
4. Guidelines for protecting passwords and best practices for creating them,
5. Where to find resources for more information,

Passwords are Important
It is our shared responsibility to safeguard the University of Washington's data and information assets. You can do your part by using strong passwords and good password practices on all the accounts, devices, and systems that you use to access and store student, employee, research, and patient data.

Cybercriminals target universities to infiltrate systems and networks to access and steal valuable data. Two of the major ways they do this is by exploiting password practices that put information and data at risk or by cracking weak passwords. This training specifically discusses your UW NetID password at times, but it is intended to address all passwords—on mobile devices, desktop computers, personal and administrative accounts, servers, and systems of all kinds.

Consequences of Stolen Passwords
If a cybercriminal steals or guesses one of your passwords, he or she could gain access to your department's confidential information. If they succeed, this could potentially cost the university in several ways, including the cost of forensic investigation, the cost of notification to those affected by the breach, possible federal and state levied fines, and in the form of reputational harm.

Risks for You

Besides potential risks for the University, cracked or stolen passwords could have consequences for you. A cyberthief may use data they discover on your accounts and devices for identity theft. They may impersonate you online to access your email, financial or social networking accounts. They may steal credit card and Social Security numbers and other personal information you may have stored on devices, in spreadsheets, text documents, or in email. They may use this information to open up new accounts, or they might sell it to other cybercriminals. If you use social media, any information that is open to the public might be used to guess answers to security questions associated with bank and other financial and credit reports and accounts.

Guidelines for Password Practices

It's well known that weak passwords are easy to guess or discover using password-cracking software. But even the most complex ones can be stolen by motivated cybercriminals. They use tactics that might work in one of two ways: they either exploit weaknesses in commonly-used technologies or they prey upon vulnerabilities in the ways people habitually use technology. Let's consider some of these weaknesses and vulnerabilities and ways to avoid or mitigate them.

Falling for Phishing

A common way that passwords are compromised is through phishing. Phishing emails are designed to trick users into surrendering their University login credentials on phony web pages. Those credentials are then harvested to be sold on underground web sites or re-used to infiltrate University systems. Think before you click on any link in any email, even if you recognize the sender. Click the phishing link in the navigation bar for information about this threat.

Reusing Passwords Across Accounts

If you use the same password for different purposes, a cyberthief can learn the password from a less secure site or application and then use it to exploit other accounts. So never reuse your UW NetID password on any other account, and avoid re-using passwords across accounts in general.

Using Public Kiosks

Public computers and kiosks, such as those at a hotel, may be infected with malware that captures your keystrokes to steal your passwords. Avoid using such computers, such as those at a library, to log into your school, work or financial accounts.

Using Unsecured WiFi

Wireless networks in public places are subject to eavesdropping, and cybercriminals can easily trap passwords and other information without the user's knowledge. So use caution on shared wireless networks, such as those in airports, libraries, hotels or coffee shops. When you are on the UW campuses, you can use eduroam, a free encrypted wifi service, to access the wireless network. We'll talk more about eduroam later in the "Tools" section of this training.

Storing Passwords in Your Browser
When you are using a browser and it detects that you have entered a password for the first time, you're offered the possibility of saving it for later use. While it's convenient to be able to access secure pages you can access secure pages without the extra step of typing in your passwords, storing them in the browser is not recommended for several reasons.

Passwords saved in the browser may be stored in "clear text," which makes them easy to discover by those who know where to look. And even passwords that are encrypted may be vulnerable, as they can be accessed by certain types of malware or discovered by a thief---or by another user with administrative rights. For these and other reasons, choose security over convenience, and say no to storing passwords in the browser.

Storing Passwords in Plain Sight
Incidents and breaches still occur because passwords are stored on sticky notes next to computers. Don't write passwords down near your computer or on your desk in plain sight. Most of us have multiple accounts, and if you are choosing strong passwords and phrases, it may be necessary to write them down in order to remember them. If you do, keep them in a safe place, such as a wallet, a locked file cabinet, or both - or in some other safe, secure place away from your computer. Password managers can help you create strong passwords and keep track of them. We'll talk more about password managers in the tools section of this training.

Not Changing Default Passwords
Malicious hackers sometimes use tools that search networks for devices and applications that are still using the default username and passwords set by the vendor. Some forms of malware are configured to automatically propagate and search for those default credentials as well. Some tools allow them to find such devices within minutes after they are connected to the Internet. Additionally, default passwords for many devices are published online. Be sure to immediately change the default password on any account, device, or system you are responsible for, including wireless routers in your home.

Five Most Common Passwords
All of the vulnerabilities discussed so far apply whether passwords are weak or strong, and they cover the most common ways that University data is maliciously accessed or stolen. But in some instances, cybercriminals specifically prey upon the use of weak passwords, which are easier to guess and easier for password-cracking software to crack.

These are the 5 worst passwords from the Top 25 Worst Passwords list of 2018:
1 - 123456
2 - password
3 - 123456789
4 - 12345678
5 - 12345

This list is based upon files containing millions of passwords that were stolen and posted online by hackers last year. These easy-to-guess passwords are also thought to be the most commonly used.

The simple passwords on this list indicate that many people either don't know or don't focus on the importance of having a strong password. Perhaps they believe that a determined cybercriminal can ultimately crack any password, no matter what it is. That's like saying you shouldn't lock the door of your house when you leave because thieves can break the windows! And while it may be true that locking your doors won't stop a determined thief, it will cause most of them to move on to an easier target.

To read the entire list, click the "Worst Passwords" link.
(Link:
https://www.securitymagazine.com/articles/88626-the-worst-passwords-of-2017-revealed)

Attacks on Weak Passwords
Let's consider some of the ways that cyber thieves can crack weak passwords. Three types of attacks are: brute force, dictionary, and password spray attacks.

A brute force attack is one that employs a procedure to try different combinations of characters repetitively until all possible combinations have been exhausted. Because this type of attack might use many possible key combinations--sometimes millions or more--brute force attacks are effective when the password length is short, and it's less effective as the password length gets longer.

A dictionary attack is a type of brute force attack that cuts the number of possible combination---either by using words from the dictionary or lists of names and other key information about users. These attacks are more effective on passwords that are commonly used.

A password spray attack takes advantage of the fact that many people use weak passwords, such as those listed on the previous slide. These types of attacks take a list of commonly-used passwords and tests them on multiple users at an organization. By testing passwords on many accounts at the same time, this method can be used without triggering account lockout protections that may be in place to guard against brute force attacks. So even if a thief isn't targeting you specifically, they may find you and gain access to your account if you are using a password that is easy to crack.

Best Practices for a Stronger Password
Keeping in mind that a short and simple password makes your data more vulnerable to cyber thieves for certain types of attacks, consider the following best practices for password creation.

Use a Combination
Use a combination of numbers, lower-case and upper-case letters, and symbols. This makes it more difficult to for passwords to be discovered in a brute-force attack.

Password Length
While it is often recommended and it is important to use a combination of characters, the length of your password is even more important than mixing upper and lower-case letters with symbols. Each character added to a password makes it exponentially more difficult to crack.

Use a Passphrase
If it's hard to remember a long password, consider using a passphrase or a combination of words instead. Because most organizations more than one character set, you can use spaces or special characters to make your password random and long, yet memorable to you. Here is an example:

Buddy likes 2 b&rk @squirrelz. *(But don't use this particular password, by the way)*

When creating memorable passphrases, keep in mind that it's important to use phrases that are unique and meaningful only to you. Don't use well-known phrases, such as movie titles or quotes from Shakespeare texts.

Don't Use Personal Information
Cyber thieves use social media accounts, the Internet, or underground forums to discover personal information about you, so this type of data is not a good choice for a password. Never use publicly-available or personal information such as your date of birth, Social Security Number, or credit card number, or even a portion of those numbers in creating a password.

Tools
Besides the *best* practices and guidelines for creating and securing your passwords, the following slides discuss tools you can use to enhance security.

Password Manager
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 (such as LastPass, DashLane, or 1 Password) can be used to create, store, and access complex passwords as you need them. They require you to remember only one master password in order to access the others you have stored in the service. So if you use this kind of service, either create a hint to help you remember your master password or write it down and store it in a safe place.

Multi-Factor Authentication
Multi-factor authentication (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 to the Duo service, click the "Duo" link in the navigation bar.

Eduroam
At the UW, you can use eduroam to provide additional security on wireless networks. Eduroam is a free encrypted WiFi service, and it's the preferred WiFi method for all faculty, staff, and students at the UW. In addition to providing an extra layer of security on campus, eduroam allows users from the UW to securely access the Internet from any eduroam-enabled institution. Once configured, eduroam gives seamless connectivity at over 30,000 participating locations around the world. To learn more, click the eduroam link.

Husky OnNet
If you are working from a remote location or from home and want to connect to University resources and applications, you can use Husky OnNet, a Virtual Private Network (VPN) service. Husky OnNet provides an encrypted connection to the UW from remote locations, such as from home, a 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.

If You Suspect a Compromise or Incident
If you suspect your UW NetID password has been compromised, or if you have forgotten it, you can reset it online, or you may either call or visit the UW-IT Technology Service center to reset it. Contact information can be accessed via the "Contact" link on this web page.

If you suspect an information security 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. See the infographic on the page linked in the "Report and Incident" link to determine 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.

Key Tips
There are many ways for cybercriminals to access information, systems, and accounts, and while there is no one perfect guideline or best practice that will definitely deter them, employing a combination of strategies may be the best solution for safeguarding personal and institutional information.

Remember these key tips for creating strong passwords and keeping them safe:

- Avoid clicking on links in email
- Don’t reuse passwords across accounts
- Use caution or completely avoid unsecure wireless networks and public computers
- Use unique passwords and passphrases that are at least 16 characters and spaces
- Use services such as eduroam and Husky OnNet or another VPN service for a secure connection

I hope I've convinced you that good passwords are important. Let's all do our part to safeguard the personal and institutional information of students, patients, faculty, researchers, and staff.

Contact & Credits

If you have questions, contact ciso@uw.edu or check out our website at ciso.uw.edu\