Welcome to the Information Security Training for Users with Elevated Privileges to University Systems. This is required for users assigned roles or permissions that, if misused or compromised, could allow a person to exploit the university systems for their own gain or illicit purpose. This training is intended to ensure that individuals in these roles have a clear understanding of their responsibility for protecting their accounts from misuse or compromise. Additionally, we will cover what the possible consequences could be if their accounts are misused or compromised due to the lack of due care in protecting them and then having them subsequently be used to exploit university systems.
To expand a bit more, the need for training such as this directly relates to the facts. Statistics show that many breaches are caused by insiders. When talking about “insiders”, breaches fall into one of two categories. They can be intentional acts of misuse, as would be the case of an inquisitive or disgruntled employee, contractor, etc. However, many breaches occur due to unintentional compromise or misuse that results from an insider’s action or inaction.

The rest of this training will focus on how to protect yourself from becoming one of the statistics.
The first topic to be covered is NetID password security.

Let's start with this question......Is there a scenario that you can think of when it's okay to share your NetID password?

• Perhaps with a new employee that has not yet gained access?

• OR what about student workers that don't have access, but you need their help with data entry during a crunch period?

• How about your supervisor?

• Or what would you do if you're out on medical leave and a co-worker calls and asks you for your username and password, because he or she needs to access something that is part of your normal duties? What should you do?
Please watch the following video which contains a hypothetical situation. We’ll discuss the details afterward.

http://security.arizona.edu/sites/default/files/UA_Password_Video_Final_1.flv
As you can see in the preceding video, the professional actors in this hypothetical situation learned the hard way that it is NEVER okay to share your NetID password with anyone.

Why?

Passwords authenticate that you are who you claim to be. If someone authenticates as you with your NetID password, that person has access to ANYTHING to which your account is authorized to do. Yes, this person may only do what you “asked” him to do or “think” he would do, but whatever your privileges allow, you have just granted that person access if he chooses to do so! This can include accessing your own personal information, available via UACCESS for self-service purposes.

As the owner of the account, YOU are responsible for all activity (legitimate or illegitimate) associated with that account, at least until and unless an investigation provides evidence to the contrary.
The hypothetical situation in the video you saw is a good illustration of how sharing a NetID password may seem harmless to an employee at the time. While it depicted a specific example of an employee sharing her password with a student worker, the employee could have shared her password with a co-worker, temp employee, vendor, consultant, etc. or any one with whom she worked.

Remember that sharing your password can provide an opportunity for someone to do the wrong thing in your name.

I know many of you are thinking....my department staff, student workers, vendors that I work with just wouldn’t do anything like what the student in the video did. And, if there ever was someone I didn’t feel I could trust, then I would definitely know not to share. More often than not, you’re right; most people wouldn’t use someone else’s account access for anything other than the intended use. And many would say “I don’t want your password!” But are you really sure about this? The person may start out as being curious, and it could lead to that person taking the opportunity to access something he or she would not usually be able to access to resolve an issue.

Let’s explore the “why” a little further.
When you share your password, consider that the following could happen. What may start as curiosity could lead to more. The example in the video highlights that sometimes we see one thing on the surface and have no indication or reason to be concerned. What causes a person to decide to misuse another's access once shared is purely based on that individual. There can be many factors that play into this decision: financial and personal stresses, varying opinions of what's right and wrong and the individual's ability to justify his or her actions based on the circumstances. The list of why someone misuses or takes advantage of an opportunity like this is long. But keep in mind that you can control the situation by not sharing your NetID password. It belongs to you and no one else should use it.
Now consider what you may be giving this person the opportunity to do with your NetID and password.

If you have access to student records, and depending on the roles assigned, you could have given this person access such as the following:

- Change grades
- Admit or deny admittance for someone
- Enter a degree exception requirement
- Change Enrollment Deposit Status
- Update Lawful Presence Status

Confidentiality and Integrity – View or update

- Social Security Numbers
- Direct deposit information
- Tax information
- Benefits information

Alternatively, your credentials could be used to access employee records. Depending on the role assigned, a person using your log-in information could view or update employee SSN information, direct deposit information, employee tax information, or employee benefits information.

Of highest criticality are Social Security Numbers. If a security breach involves names and SSNs, Arizona's Breach Notification Statute (44-7501) requirements can have substantial financial and reputational impact as a result.

Remember that you're the expert in what you do; that is why you have been assigned these privileges. With that privilege comes the responsibility to ensure the protection of the integrity and confidentiality of the data you are authorized to access.
Here are a few additional reminders for keeping your NetID password safe from compromise.

Do not use your NetID password on any other account. Doing so will increase your points of exposure. In fact, we strongly recommend that you use different passwords for different types of accounts. This will minimize the number of accounts that a hacker could gain access to with the same password if compromised.

Don’t store passwords online, unless you do so in encrypted files. Users who prefer to store this information electronically should use a Password Manager Program, such as Password Safe, KeePass and Password Gorilla. These programs allow users to safely and easily create a secure encrypted username/password list. Then the user only has to create and remember a single "Master Password". Because this password unlocks and grants access to the owner’s entire username/password list, it’s important to create a strong master password. Once stored, passwords can be copied by double-clicking on them and pasting them directly into the application.

Don’t write your passwords down UNLESS you then place them in a locked, secured location such as a locked filing cabinet or drawer accessible only to you. File them in a place that you will remember, but not in an obvious location like under “P” for passwords.
Remember at the beginning of this presentation that I said an unintentional insider threat can come from a person’s action or inaction. An example of inaction would be not locking your computer when you walk away from your desk.

Think of how many times in the course of your day you may walk away from your desk for a variety of reasons. You may intend to only be gone for a minute, but then may be called upon to do something else. Before you know it, 10 minutes or more may have passed. During that time, you may be logged into an application that contains sensitive data, such as student or human resource records. While the application and workstations have a session time-out policy as part of the security, it only takes a moment for someone to do something using your credentials without your permission before that application time-out policy is activated.

An even more serious situation could occur in that time. You may provide someone with the opportunity to install malware on your computer, such as a keylogger. A keylogger is a program that records the keystrokes on a computer. The log will be saved in a file and may then be sent to another machine over a network or the Internet. By examining the keylog data, it may be possible to find private information such as a username and password combination and harvest key pieces of information that would either be valuable to use or sell for personal gain.

While you have security software installed on your computer that is helpful in detecting malware such as this, one of the best ways to protect yourself from keyloggers is to make sure that you don’t provide an opportunity for one to be installed by not allowing unauthorized access to your computer for someone to walk up and install the malware.

Locking your computer is very simple. On a Windows machine, you can hit the “Windows” button and “L” at the same time, or hit control-alt-delete and select “lock this computer.” On a Mac, hit Shift + Command + Q.
To summarize, keeping computers and data secure takes vastly less time than recovering from a security problem, which can be an expensive activity in more ways than one. If your account is misused or compromised, there can be serious and far-reaching consequences.

- The University may suffer a financial or reputational loss as a result of the compromise.
- You may be held accountable for any negligent action, or inaction, that led to the compromise if there is evidence that you did not use due care in protecting those elements for which you control. Disciplinary action could be taken up to and including termination.
- And as previously mentioned, as required by Arizona’s Breach Notification Statute (44-7501) if the compromise involves SSNs there could be a significant financial and reputational impact to the department as well as the university.

**CONSEQUENCES**

- Financial and/or reputational loss
- Employee may be held responsible for any action or inaction that led to the incident
  - Disciplinary action up to and including termination
- Arizona’s Breach Notification Statute (44-7501) = if the compromise involves SSNs
  - Could have significant financial and reputational impact
You have reached the end of the awareness module. You may now go to https://request.uaccess.arizona.edu/privilegeduseragreement/ to sign the attestation of compliance.