Video 2: Account Security

Topics in this Module

Welcome to NAU's Information Security Essentials training. This module includes the following topics:

- Your NAU Account
- Account Responsibilities
- Password Sharing – hint: never do it!
- Scenarios Involving Faculty, Staff, and Student
- Strong Passwords
- Two-Factor Authentication
- What to do if you suspect fraudulent activity on your account

To learn more about these topics, click "continue. To jump straight to the tutorial quiz, click "jump to quiz".

Your NAU Account

As a member of the NAU community, you are provided with a unique username and password that grants you access to sensitive information. We all have access to sensitive information, whether we are aware of it or not. This includes your own personal information that can be accessed through your PeopleSoft LOUIE account, such as your paycheck, direct deposit, addresses, and social security number. You also have access to tools for your workplace that contain sensitive information such as your NAU email, shared files, and a variety of online tools such as the PeopleSoft Financial and HR systems. Some NAU employees have access to information protected under privacy laws such as the Family Educational Rights and Privacy Act, FERPA, Health Information Portability and Accountability Act, HIPAA, and the Purchasing Card Industry Data Security Standards, PCI DSS. Thanks to NAU's Central Authentication System, or CAS, single sign on, you only need to log in once to gain access to many of NAU's resources. While this makes things more convenient for us as employees, it makes account security that much more important. If an unauthorized user gains access to your account credentials, they are able to access and perform actions on your behalf for *all* of these tools and services.

You are Responsible for your Account

You are completely responsible for anything that happens on your NAU account and your username and password are the keys to that account. You should NEVER share your NAU username and password with anyone! Your NAU password should also be unique. You should never reuse your NAU password to login to other accounts such as online banking services or social media accounts such as Facebook.

Never Share your NAU Password!

I'd like to introduce you to three people who found themselves in a difficult situation in regards to their NAU account. David, a student employee at NAU, Lisa, a member of our staff, and Kevin, one of our faculty members. Please click on them to hear their story.

Student Employee Scenario

David is a student employee at NAU. His parents are helping him pay for his college education. His tuition and other NAU expenses are paid through his LOUIE account, which his parents would need his NAU username and password to access. David knows that he should not share his NAU username or password with anyone, but he trusts his parents to only access his account to make payments. Should David give his parents his username and password?

Absolutely not. By giving his parents his NAU username and password, David is also giving them access to other NAU services, such as his courses in Blackboard Learn, his email account, his grades, and any accounts he has access to for his job responsibilities. Even though David trusts his parents, he is still liable for anything they do on his account and just the act of sharing his NAU username and password with his parents could cost David his job. We realize this is a common situation that many students run into, and we have a solution. All students have the ability to add an authorized user to their "TouchNet" fee payment account. This account provides the ability to view a student's account and make payments without sharing access to other information on a student's account. If you have any questions about how to set up a TouchNet account, please contact the Student Technology Center at 928-523-9294.

Staff Scenario

Lisa and her coworker are working on a project together. The project is currently on hold until Lisa finishes a report. Unfortunately, Lisa is out sick. Her coworker offers to work on her report while she is out sick but the report is only saved on Lisa's work computer. Is it ok for Lisa to give her coworker her NAU username and password so they can login to her computer to retrieve this report?

Lisa should not give out her NAU username and password to her coworker. By giving her coworker her NAU username and password, Lisa is also giving access to other NAU services, such as her paycheck and direct deposit information in PeopleSoft and her email account. If you have a business need for sharing information, contact the Solution Center and they can help you establish a solution. For example, in this scenario, the Solution Center can set up an account for Lisa's coworker on Lisa's computer and assist her in accessing the document she needs to work on. To avoid future dilemmas, the Solution Center can assist Lisa and her coworker in utilizing "NAU Shares" or other file storage locations including employees' "H Drives" where permissions can be set so that specified people can access files as needed, or a Sharepoint site for team collaboration.

Faculty Scenario

Kevin is an instructor at NAU and has a TA that helps him with his classes. It is the end of the semester and Kevin has tasked his TA with final grades. The TA has the final grades for all Kevin's classes' completed and is ready to enter them into LOUIE. Should Kevin give his TA his NAU username and password so that his TA may enter these grades into LOUIE?

Kevin should not give his TA his NAU username and password. By giving his TA his NAU username and password, Kevin is also giving access to other NAU services, such as his paycheck and direct deposit information in PeopleSoft, his email account, and if that TA is in one of Kevin's classes, they also have access to make changes to their own grade. TAs and GAs are granted access to class grade books on their own NAU account so that they can submit grades for you to review. If you have any other business need for sharing sensitive information, contact the Solution Center and they can help you establish a solution.

Your NAU Account

As an employee of NAU, you have been granted access to sensitive information such as research data, FERPA, HIPAA, and PCI restricted information, or financial data. Others such as your spouse, children, student employee, TA, friend, or your parents have not. Even if you trust them, you should never give them your username and password. If they access your account, you are liable for any data they obtain and anything they do with this data. One unauthorized person accessing information threatens the integrity of NAU's information, violates the NAU Acceptable Use Policy, and could violate privacy laws and standards, such as FERPA, HIPAA, and PCI.

Your NAU Account

In addition, anyone who gains access to your account will also have access to your personal data. This person now has the ability to add or drop classes, accrue charges, send emails, or change the direct deposit account of your paycheck, all on your behalf. You are responsible for all of these actions, some of which will not be reversible.

Strong Password

Along with keeping your password a secret, you want to ensure that you have a strong password that others will not be able to guess. NAU's password requirements are in place to help you create a strong and secure password. Your password must be between 7 and 128 characters in length, it must contain at least one character that is an uppercase letter, a lowercase letter, and a digit or special character. We require you to change your password every 90 days to help keep it more secure and you should never reuse your NAU password for other services such as Facebook, Twitter, or banking services.

For example, capital I, <[less than sign]3 L o u 1 e is a strong password and fulfills NAU requirements. Of course, because I just used it as an example in this training it is no longer unique so you should never use this password. On the other hand, smellycat is a really weak password and does not fit NAU's password requirements.

Two-Factor Authentication

Some NAU account holders are required to use two-factor authentication because they have greater access to sensitive data. If you are one of those people you will have an additional authentication step after entering your NAU username and password in order to gain access to your NAU account. For example, after logging in to your computer with your NAU credentials, you may then be asked to verify that login from your mobile phone.

Many online services such as banks offer you the option to set up two-factor authentication for logins. It is a good idea to consider this as an additional layer of security for your personal accounts. Remember, do not reuse your NAU password for non-NAU online services!

What if I Suspect Fraudulent Activity on My Account?

What if someone does gain access to your account? You may notice this because of strange activity on your account. For example, if you are suddenly not able to log in to your account, things change that you did not change, or you are receiving failed delivery notifications on emails that you did not send. If you suspect there is fraudulent activity on your account, change your password right away using the NAU password change tool, and contact the Solution Center. The sooner NAU has been made aware of fraudulent activity on your account, the sooner we can take steps to protect the information on your account and safeguard other accounts. Remember if See Something – Say Something! It helps everyone out if you do.