Video 1: What is Information Security?

Topics in this Module

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

- An Overview of Information Security
- Sensitive Data Types and Responsibilities
- Access to Information and Data
- Security Breaches and Unauthorized Account Use
- Consequences of a Breach or Unauthorized Account Use
- How You Can Help

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

What is Information Security?

Welcome to NAU's Information Security Essentials training. Information security is very important to NAU and we require you as an NAU employee to successfully complete this course so you will be better prepared to protect both NAU data and your own personal data.

Welcome!

This training consists of four modules, each with a short quiz at the end. You must pass all four quizzes to successfully complete the training. Make sure you click the Continue button on the quiz results page to ensure your score is recorded.

What is Information Security?

Let's get started with an overview of information security.

As a university, we protect a lot of sensitive information and data, such as social security numbers, bank account information, and student grades. Information security protects this information and ensures the confidentiality, integrity, and availability of information. This means that our information is only accessible by those who are authorized to access it, our information is up-to-date, accurate, and reliable, and you have access to the information you need, when you need it. NAU is committed to preserving the availability, confidentiality, and integrity of its information resources while also preserving and nurturing the open, information-sharing requirements of its academic culture

We Need Your Help!

NAU has safeguards in place to ensure the security of our information resources and to maximize the integrity of information. We make every effort to ensure that you, as an NAU employee, have access to the information resources you need to quickly and effectively complete your job. However, we all play an important role in information security and we need your help. Many security breaches are the result of human mistakes, not system weaknesses. You are our first line of defense against data

security breaches and identity theft at NAU. Your awareness and use of sound security practices is our best defense. If you See Something – Say Something!

You are Responsible for Sensitive Information
As employees of NAU, we all have access to sensitive information that needs to be protected. At the very least, we have access to our own personal information, such as direct deposit accounts, paycheck information, and our social security number. Some of us may have access to substantially more sensitive information such as student data. Sensitive student data includes grades, and dates of birth and addresses may be considered sensitive if requested. Sensitive information also includes research data, such as participant information, survey results, and phone numbers, and HR and financial data, such as timesheets, budgets, and travel accounts. All of this information should be treated as sensitive and you should never share it.

If you are ever unsure of which information is sensitive, or the appropriate way to handle that information, contact the Solution Center at 523-1511.

Access to Information
The type of information you have access to is determined by the duties and responsibilities of your position. For example, an instructor needs to be able to enter student grades, therefore they have access to this information. A staff member may never need access to student grade information to complete their job duties, so they do not have access to this information. Because your duties and responsibilities determine what information you have access to, you should NEVER use another person's account, including their NAU username and password, as they may have access to information that you do not. Likewise, you should never share your NAU username or password with anyone, or let them use your account.

Security Breaches and Unauthorized Account Use
For the purposes of this training, a security breach is defined as the unauthorized acquisition, access, use, or disclosure of sensitive information through technical means, which compromises the privacy or security of such information. Unauthorized account use is similar to a breach in that an unauthorized entity gains access to sensitive information. However, rather than gaining access through weaknesses in technical safeguards, this access is possible because an individual has gained access to a specific account or accounts. Examples of this include purposefully sharing account credentials and successful "social engineering" attacks such as email "phishing" which trick people into giving away account information. Both breaches and unauthorized account use threaten the confidentiality and integrity of NAU information.

Consequences of a Breach or Unauthorized Account Use
A breach or unauthorized access of personal information can cause harm to any individual whose information is accessed. It can also cause harm and embarrassment to NAU, and, if you are responsible for the breach or unauthorized access, you could face disciplinary action or termination from NAU.

What to Do if You Suspect a Breach or Unauthorized Account Use?

If you suspect an information security breach or unauthorized account access has occurred, act quickly! Call the Solution Center immediately at 523-1511 and provide them with any information you can on the incident. If you believe your account has been compromised, you should also change your password and security questions immediately!