CYBERSECURITY AND YOU

Welcome to Team ND!

This is an introduction to the official security training you will complete through the State PeopleSoft Enterprise Learning Management system.

When you have been given access to PeopleSoft, you will be assigned a mandatory security training course*. In the meantime, please review this information and follow the recommended safeguards to help protect you, our citizens and our state from cyber threats.

Your Role: The threat landscape, internet security, and you

Cybercrime is big business, and the bad guys have learned that the easiest way into your organization's network is to trick you into letting them in.

Cybercriminals are targeting organizations like ours, and they are targeting you! The information you have access to, including files and network access, holds high value to cyber criminals. You are a target.

The days of the clumsy, badly worded, easy-to-spot phishing emails are gone. Today's threats are sleek, sophisticated, and very slippery. They can slide right through your organization's antivirus software and spam filters and go straight to your inbox.

Let's take you on a tour of the threat landscape. We'll show you some of the common ways the bad guys try to trick you.

Example 1: Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you in order to get you to take some action that isn't in your own best interest or in the best interest of your organization, for example, plugging an infected USB device into your computer. The hacker might use the phone, email, post service, or direct contact to try to trick you. Phishing and spear phishing are forms of social engineering.

Example 2: Malware

Malware stands for "malicious software" - an umbrella term for all the software out there that is being used by cybercriminals to spy on you and steal your information.

Once your computer becomes infected, some malicious apps can log your keystrokes when you type your password. Some apps take over your computer and can even allow the hacker to turn on your webcam to spy on you or listen to your conversations.

One type of malware that's in the news a lot if called "ransomware." This malicious software can hold the files on your computer or your smartphone hostage until you pay a ransom!

*Enterprise Architecture Employee Security Awareness standard ST009-05.2

NORTH Dakota | Information Technology
Be Legendary.™

HELPFUL TIPS TO BE #CyberAware

Help Build a Culture of Cybersecurity Awareness

The easiest way for a cyber criminal to access your computer is social engineering. Remember to:

Secure Your Workstation

- When leaving your workstation, ALWAYS lock it; it is department policy to do so. To lock your workstation, hold down windows + L keys.

Be aware of Spam & Phishing Attempts

- State of ND email addresses are public, so cyber criminals have an easy method to contact state employees.
- Email is the number one method for cyber criminals to contact their victims.
- Be suspicious of emails being sent from an unfamiliar person or emails requesting action (click this link, you've won money, etc.).

Personal Email is strongly discouraged

Secure Your Passwords

- Passwords are keys; guard them like you guard your house key.
- Our network and software security and firewalls can be the best and yet, if someone obtains our password, all the security in the world will not protect our data.

Create Strong Passwords:

- Use something that is easy to remember.

Do not include:

- Names,
- Birthdates,
- Seasons,
- Favorite team names, etc.
- Hackers focus on the region of their potential victim, so they may try Fall2019, Vikings1, Packers1, Fargo2020, etc. as password attempts.

Visit our website for additional information, password and access control tips, and requirements.
https://www.nd.gov/itd/standards/access-control-standard

How long would it take for a high-powered server to guess these passwords?

Today123	36.99 minutes
Today1234!	19.24 years
Mi55ouriR!v3r	1.65 hundred thousand centuries

Remember:

- All portable data containing Personally Identifiable Information (PII) or Protected Health Information (PHI) MUST be encrypted.
- Shred or destroy confidential information when it is no longer needed.
- Wireless Security
  - Connect to trusted wireless networks only.
  - State of ND locations have two access points: StageNet-Guest (public) and StageNet-Member (private, encrypted)
  - If connecting to a guest or public network, do not access confidential information (work, banking info, etc.) unless you are using a VPN connection.
- Social Networking
  - Do not post confidential information on public websites, forums, blogs, or social media sites.
  - Posting personal information on these sites gives cyber criminals information to use against you.

Stay vigilant, remember these important precautions, and help protect yourself, our state and our citizens!