NC State Data Security Module Transcript

Table of Contents:

DATA SECURITY

Slide 1 Disclaimer:

The purpose of this module is to increase awareness of security best practices for your employment at NC State and your personal online safety.

This information is not comprehensive and should not be considered legal advice. It is your responsibility to comply with existing state and federal laws as well as NC State University Data Security regulations and any grant-specific regulations that apply to your university role. See NC State Policies, Regulations & Rules.

Slide 2 Data Breaches:

A few years ago at the University of Maryland, a secure records database was compromised. This database had information dating back to 1998, including names, birthdays, university ID numbers, and even social security numbers. Over 300,000 people were affected as a result of this one data breach! This breach cost the University millions of dollars in responding and recovering from the incident.

Another recent example happened in the Maricopa County Community College District. In this much bigger example, the names, social security numbers, and financial information of more than 2.4 million former and current students, employees, and vendors were exposed on the internet. The data released went back as far as 30 years. This led to lawsuits, resignations, firings, and costs totaling over 26 million dollars.

These two security breaches were not isolated incidents; since 2005, educational institutions have suffered more than 700 reported incidents of security breach.

NC State systems are also being targeted on a daily basis. Including sophisticated phishing attacks designed to steal information and data from our users.

We talk about data security because we don't want your information to be compromised. We also don't want your research data hacked or your research subjects exposed. In a system as large as ours, one small data breach can have major financial, reputational, health and safety, and operational consequences.

Text On Screen: After narrator says, NC State Policy:

Breach at University of Maryland
- Data released: names, social security numbers, dates of birth, and university identification numbers.
- Over 300,000 people affected

Breach at the Maricopa County Community College District.
- Data released: names, social security numbers, and financial information
- Over 2.4 million people affected

Security breaches can and do happen when individuals do not follow proper procedures.

Slide 3 Introduction to Data Security:

After completion of this training you will be able to identify ways that you can be more secure. Remember, you are our first line of defense! We need you to help shield yourself and the university from cyber attacks. And you can, by putting together all of the pieces of your shield which include;

- using strong passphrases,
- guarding against phishing,
- applying security updates,
- securing mobile devices,
- securing your connection,
- and asking for help.

You will also be able to identify tools and services that NC State provides to help increase your security.

At the end of each section, click "next" to continue.

Slide 4 Introduction to Data Security cont.:

Let's take a moment to talk about why it's important to protect both the university's data and your personal data. There are a number of potentially harmful outcomes that could take place if your NC State account is compromised:

- Someone can use your account to send compromising or embarrassing emails.
- Your identity can be stolen, allowing someone to open payday loans using information stored in the MyPack Portal, like your W-2.
- Someone can access your Google or network drive which could lead to a data breach, costing the university thousands of dollars in money and human resources.
- Or, your account could be disabled, denying you access to campus resources and systems.

Each of these unfortunate incidents have already happened to NC State employees and students. **And, they could happen to you**.

But don't worry; the purpose of this module is to get you *comfortable* with data security *and* available campus resources, so you can protect your most important assets and those of the university.

You are our first line of defense! NC State has put in place a number of security measures to protect **our** campus, but we need you to help *shield* yourself and the university from cyber attacks. And you can—with just a few simple steps.

Slide 5 Strong Passphrases:

Protecting your NC State credentials — your Unity ID and password — is a simple but crucial step to keep your information secure.

In this module, we will refer to "passwords" as "passphrases." A passphrase is an expression or group of words that is easy for **you** to remember, but difficult for hackers to guess or break. Passphrases are generally longer than most passwords, making them more difficult to decode. Examples include a song lyric or a poem with a variety of letters, numbers and special characters.

This is a specific example of a passphrase. The passphrase expression is "wash the dishes now" but different letters have been replaced with symbols or numbers. It's over 12 characters long, includes a variety of characters, and is easy to remember but hard for others to guess. **Just don't use this one and make sure to come up with a passphrase of your own!**

The easiest way to secure your account is to —

- create a strong passphrase
- manage it securely
- set-up two-factor authentication; and
- never share your credentials. **No matter how great your passphrase, if you share it, it's no longer secure!** Sharing your passphrase is also a computer use policy violation. If you have already shared your current credentials, this is a great time to pause the module and change your password or passphrase by visiting go.ncsu.edu/password

Click the icons to learn more important passphrase tips.

Text on Screen:

- Defend your Unity ID and Passphrase!
- ***Never*** share your passphrase. Remember that NC State IT staff will never ever ask for your passphrase, either by email or phone!
- If a colleague or manager needs to access your email or calendar, consider email delegation or calendar sharing. Do not share your passphrase.
- Learn how to create a strong passphrase at go.ncsu.edu/password
- We recommend that you do not write down your passphrases. If you choose to do so, keep them in a secure place like a locked drawer or saved on your phone behind a lock screen. Never write down a username and passphrase together.
- Consider a password manager, which can save your passphrases and automatically generate very strong ones. NC State does not officially recommend a password manager, but popular options on campus are KeePass and LastPass.
- **Always use different passphrases for different services.** This way, if your social media account is compromised it will not affect your online access to your bank information, medical records or work systems.

Slide 6 Beware of Phishing Attacks:

One of the biggest cybersecurity threats to the university and to you is phishing. At NC State, about half of our daily email traffic is either spam or phishing attempts. That's about half a million to a million bad messages every day! Most of these are stopped before they get to your inbox, but not all of them.

Phishing is an attempt to trick you into providing your personal information, like passphrases, credit card numbers, social security numbers, or other data that can be used to steal your identity or gain access to your online accounts.

These attacks are typically an email that appears to come from a trusted source, such as a friend, your bank, credit card company, social media site, your supervisor, or even the NC State Help Desk.

A well-crafted phishing attack tricks more than 40 percent of its recipients, which means you need to know how to spot a phishy email.

Look out for messages that ask you to, for example:

- Immediately confirm your ID, upgrade your account, or change your passphrase so your account isn't deactivated or deleted.
- ...or to...Click on an unrecognizable or suspicious link, like "Click Here."
- ...or to... Open a suspicious or unexpected attachment.

So, how else can you tell it's a phishing email? Here are a few more signs to watch out for:

- Check the sender's email address and see if it matches the sender's name. If it doesn't, that's a telltale sign it's phishing.

- Even if the sender's email address matches the sender's name and looks like it's from someone legitimate, it still may be a phishing attack. When people fall for phishing scams, hackers use their email accounts to send out even more phishing attacks. Recipients of these emails are 36 times more likely to be phished, just because they know and trust the email sender.

Slide 7 Beware of Phishing Attacks (cont):

So, how can you avoid getting phished?

- Don't click on suspicious links. To see where a link is taking you, hover your mouse over the link text. If the URL doesn't match the expected website, do not click it, and delete the message. You can also contact the Help Desk or the company's Customer Service department to determine if the email is official.
- Open a new window or tab and manually enter the official company or service URL to check for alerts on your account.
- Don't open or download unexpected or suspicious attachments.
- Still unsure? Forward the email to OIT's Help Desk at help@ncsu.edu or call 919-515-HELP for assistance.

Text On screen:

What you can do:

- Don't click suspicious links. To check where a link is taking you, hover your mouse over the link text.
- If you receive a suspicious-looking email from someone you know, it's okay to be skeptical. Check with the sender, through a method other than email, to verify.
- Open a new window or tab and manually enter the company or service's official URL to check for alerts on your account.
- Don't open or download unexpected or suspicious attachments.
- Still unsure? Forward the email with full headers to the Help Desk at help@ncsu.edu or call 919-515-HELP for assistance.

Slide 8 Apply Security Patches and Updates

The second biggest cybersecurity threat to campus, next to phishing, is unpatched software. Applying software updates does more than just provide you with the latest feature or bug fix. It also closes security holes that hackers, viruses and malware use to get in.

If you receive notifications or pop-up messages regarding software updates, please verify on the vendor's website before updating. You should periodically check vendor information to ensure you are running the latest version of the software. If you have questions about a software update notification, contact your local IT staff or OIT.

Some users on campus are supported by OIT's Managed Desktop service or by college IT staff. This means that university IT will apply all available updates and patches to your work computer. Remember that you are responsible for updating software on personal computers and devices that access NC State networks and for NC State-owned computers that are not managed by OIT's Managed Desktop or other college or division IT staff.

Text on Screen:

- Install software updates and patches when they are available. If you are a Mac user, check iTunes for updates. If you are a Windows user, check the Microsoft Action Center for updates.
- If you are supported by OIT's Managed Desktop or college/division IT support, patches to your work computer are automatically installed.
- Not sure if your computer is managed by OIT Managed Desktop or college/division IT staff? Ask your supervisor or find out more at LanTechs for Campus Units.
- You are responsible for updating personal devices, and non-managed NC State-owned devices that connect to NC State networks.

Slide 9 Secure Your Mobile Devices:

Using mobile devices, like smartphones and tablets, has become a common practice in the business world, and knowing how to keep your information secure can be a challenge.

There are steps you can take to secure your information on mobile devices to prevent data loss and theft.

First: Enable a Screen lock
Set up a passcode, PIN, or pattern lock on your device and make it longer than the minimum length required. Simply locking your device can prevent others from accessing and potentially stealing sensitive data.

Screen locks are especially important for mobile devices, but locking all workstations, including desktops and laptops, when they are not in use is essential for data security as well.

Second: Install anti-malware
Mobile devices can be infected with malicious programs just as easily as desktop machines. Installing anti-malware software on your mobile phones and tablets helps ensure that they will be protected from the latest attacks. Make sure to enable the auto-update option!

Third: Apply software updates
Updating and patching your mobile devices is just as important as updating and patching your computer. Updates secure your devices against vulnerabilities and make it harder for hackers to get in.

Fourth: Secure your Wi-Fi

Using unsafe Wi-Fi connections is like leaving the front door open for hackers. Even with password protection, public Wi-Fi can leave your data exposed to others using the network. It's best to avoid accessing sensitive accounts or documents while on public Wi-Fi, even if it's "secured" with a password. Choose "ask to join" in your Wi-Fi settings to prevent automatically connecting to networks that might be unsafe.

Fifth: Backup your data
Having a backup plan for all devices is essential because your phone may hold your most precious data. Some phones have automatic backup options available, but there are multiple methods available for backing up and transferring your data from your phone to your PC or the cloud. Whatever method you choose, make sure to backup your device regularly.

Sixth: Know your apps and permissions
Only download apps from reputable sources and make sure to check permissions before downloading. App permissions control what the app can do with your device and your data – everything from recording your conversations to sending text messages without your consent. So, make sure you understand what the app can do before you install it.

Please see the Mobile Device Security website for more options to secure your device such as enabling encryption.

Text on Screen:
1: Enable a Screen lock
2: Install anti-malware
3: Apply software updates
4: Secure your Wi-Fi
5: Backup your data
6: Know your apps and permissions

See Mobile Device Security Website for more security options

If you have questions about how to secure your mobile device, contact the Help Desk at help@ncsu.edu or 919-515-HELP (4357)

Slide 10 Secure Your Connection WiFi:

We can't talk about data security without mentioning Wi-Fi.

NC State provides extensive Wi-Fi coverage. Register your mobile devices to connect to NC State's Wi-Fi networks automatically wherever you are on campus.

eduroam is an encrypted network that provides our most secure Wi-Fi and is recommended for students, faculty and staff. It also has the additional benefit of automatically connecting you to Wi-Fi when visiting other eduroam institutions.

Nomad is another Wi-Fi option on campus. You may also hear it referred to as the NCSU wireless network. After you register your device with Nomad, you'll connect automatically, without having to enter your username and passphrase, whenever you're on campus. This network is a good choice for devices that are not compatible with eduroam.

Text On screen:

NC State Wi-Fi Networks

- eduroam: Most secure Wi-Fi network
  - Encrypted
  - Automatically connect when visiting other eduroam institutions
  - eduroam registration directions
  - List of participating eduroam members.
- Nomad: "NCSU Network"
  - automatically connect on campus
  - alternative to eduroam
  - Nomad device registration instructions

Slide 11 Secure Your Connection VPN:

Sometimes, you may need to access NC State resources from off-campus locations. Let's talk about how you can be secure even when you're not physically here at NC State.

To access University restricted services when you're not on campus, use a virtual private network, or VPN. A VPN provides a secure connection that can't be intercepted by potential eavesdroppers.

NC State uses the AnyConnect VPN client. When you start the VPN, you will be asked to enter your Unity username and password. Once you're verified, the program creates an encrypted network connection between your remote device and the NC State network. This allows you to access restricted services and sensitive data safely.

You can find additional resources at the NC State VPN Access page. Or, if you would like help to set up a VPN, you can contact the OIT help desk at help.ncsu.edu

Text On screen:

VPN: "Virtual Private Network"

- Secure off-campus access
- Connect to mapped drives and other resources on campus
- Visit NC State Virtual Private Network Access

Need assistance? Visit https://help.ncsu.edu

Slide 12 Ask For Help:

Data security is complex. It changes rapidly, and its application varies from project to project. Because of this, it's especially important to be aware of common situations where you might need help.

These situations include, but are not limited to:

- travel
- human and animal subject studies
- use of student personally identifiable information
- off-campus data storage, such as the Cloud,

- contract negotiations
- grant closeout
- suspicion of data breach
- regulation changes and
- significant developments during research, such as new discoveries or advances

Know who to contact if you are unsure how data security guidelines apply to your project, if you have identified a potential data security situation, if you have a technology question, or if you suspect a data breach.

OIT serves the entire campus community, however your unit may have its own IT staff. If you have questions, need help, or would like to request consultation, start with your unit's IT staff. They may be able to help with your specific project, or they may refer you to OIT for more general issues. If you don't have local IT staff or they are not available, you can contact OIT directly at help.ncsu.edu.

Text on Screen:

Start with your local IT staff. Check with your supervisor if you need help identifying your local IT contacts. If your local IT support is unavailable or you do not have local IT support, contact the OIT Help Desk.

OIT Help Desk: help.ncsu.edu
919-515-HELP
help@ncsu.edu

MENU OF TOOLS

Congratulations! You have completed your data security shield and are armed with basic security knowledge. Now let's talk about the tools and resources provided by NC State to help you keep all of your data safe.

Slide 1 Two Factor Authentication:

We're using two-factor authentication, or 2FA, at NC State because it can prevent up to 98% of account compromises due to phishing and other scams. 2FA is an extra layer of protection for your account because it confirms your identity through *two sources* - something you *know*, like a passphrase, and something you *have*, like a phone or other device. This means that in order for a hacker to access your account, they would need to have both your passphrase and your second factor.

To learn more about 2FA at NC State, visit go.ncsu.edu/2fa.

Two-factor authentication is also available for services outside of NC State to help keep your personal accounts safe. Check with your bank, credit card company, social media sites, and other companies you do business with, like Amazon, to find out what types of 2FA they offer.

Text on Screen:

Two-factor authentication (2FA) adds an additional level of security for your accounts.

2FA requires you to log in with:
- something you know (passphrase)
  AND
- something you have (code, mobile device, or U2F key)

Learn more: go.ncsu.edu/2fa

Slide 2 User Identification and Authentication:

Sometimes we get locked out of our accounts and need help getting back in. NC State has a system for that!

User Identification and Authentication, or UIA, is a set of security questions and answers that only you will know. If you have forgotten your passphrase or cannot two-factor into your accounts, UIA will help you regain access by verifying your identity with the self-service passphrase reset tool or when calling the OIT Help Desk.

When creating UIA questions, consider ones with answers that:

- Cannot be easily guessed by others or found on the Internet.
- Are easily remembered and aren't likely to change.

Text on page:

Your UIA Questions help you:

- Use the self-service passphrase reset system at go.ncsu.edu/password
- Reset your passphrase over the phone with the OIT Help Desk

- **Create UIA questions with answers that:**
  - Cannot be easily guessed by others or found on the Internet.
  - Are easily remembered and don't change frequently.

Slide 3 Antivirus and Anti-malware:

In addition to protecting your usernames and passphrases, it is important to consider how to protect the various physical devices you use to access and store information.

In this section, we'll refer to all malicious programs, including viruses, spyware, trojans, and adware as *malware*.

PCs, cell phones, laptops and tablets are all targeted by hackers. One popular hacking method is to use infected email attachments that, when opened, immediately install malware. These bad programs can cause all kinds of problems—from crashing and locking your device to stealing and sharing your data. Some even use your device to infect others on the network!

Worse yet is a kind of malicious software called "ransomware." Ransomware infects your computer– or the entire network– and holds your computer and data hostage until a "ransom," ranging from hundreds to tens of thousands of dollars, is paid to the hackers.

Protecting your devices from malware helps to protect all devices on the NC State network. In fact, every device that connects to the NC State network is *required* to have anti-malware software. Devices you receive from campus should already have anti-malware software installed, but devices that you own—any computers, tablets or mobile phones that you've purchased for yourself—may not. So if you connect to the university network from a personal device, you are responsible for making sure it's protected with anti-malware software.

To learn more, check out NC State Antivirus Resources and ensure all your devices have important anti-malware protection.

Text on Screen:
Tips to stay safe:

- Do not open unexpected or suspicious attachments.
- Mobile devices are as vulnerable to malware as traditional computers.
- Every device that connects to NC State's network is required to have anti-malware software. Remember that **you** are responsible for keeping your devices secure! NC State Antivirus Resources

Slide 4 Google Drive Security:

NC State is a Google campus, which means we use Google tools like Drive for communication, collaboration, and productivity. Even when you use trusted tools like Google to collaborate, you still need to think about security.

A key security feature you need to be aware of is *permissions*. You can control the permissions setting for each file and folder that you own in your Google Drive. Using these settings, you can specify who can view, comment on, edit, download, and print your information. You can also set expiration dates for viewers and commenters.

It is your responsibility to use Google Drive and other G Suite tools securely and in accordance with any security guidelines.

Text On screen:

Sharing data via Google Drive:
Consider who has access to your Google Drive files.

Key Security Features:

- Limit settings/permissions for editors.
- Limit ability of viewers and commenters to download, copy or print documents.
- Set expiration dates for how long a viewer or commenter can access documents. This setting may be helpful to use for contractors or part-time employees temporarily assisting with a project.

Slide 5 Data Sensitivity Framework:

Not all data are created equal at NC State. Some data is highly sensitive and should be handled with extra caution, while some data is not sensitive at all. A great tool you can use to understand data security for your project is the Data Sensitivity Framework. This tool was designed to help NC State employees answer the questions:

- How sensitive is the data I work with?
- Where am I allowed to store my data?
- What protection controls are required by the university?

In the Data Sensitivity Framework, there are five levels of data classification:

- Ultra-sensitive (Purple)
- Highly sensitive (Red)
- Moderately sensitive (Yellow)
- Normal, not sensitive (Green)
- Unclassified (White)

For example, maybe you're working with critical US infrastructure information, personnel data, or financial aid information. Each of these data types have different data classification levels!

Some of the most sensitive data elements at NC State that fall into the Purple and Red categories are social security numbers, credit card numbers, bank account passwords and PINs, student health records, and many types of personally identifiable information (PII). To learn what classification – or color – your data falls into, review the Data Sensitivity Framework.

Once you know the sensitivity level of your data, you can also find out how to protect your data and comply with regulations. The Data Sensitivity Framework helps NC State prevent security breaches and data loss.

Remember—it is your responsibility to ensure that Data Sensitivity Framework guidelines are being followed when you store or share sensitive data.

Text On Screen:

Questions You May Have:
- How sensitive is the data I work with?
- Where am I allowed to store my data?
- What protection controls are required by the university?

Data Sensitivity Levels

The Data Sensitivity Framework includes the following levels:

- Ultra-sensitive – Purple
- Highly sensitive – Red
- Moderately sensitive – Yellow
- Normal, not sensitive – Green
- Unclassified– White

Visit Determining Sensitivity Levels for Shared Data, to identify your data's classification.

Visit Storage Locations for University Data to determine where you can safely store sensitive data.

Slide 6 Policies:

In your role as an NC State employee, you may access various types of sensitive data, including medical, student or financial information. You need to be familiar with specific policies that pertain to these datasets.

> Policies and regulations can be issued as a result of federal or state government mandates, NC State or UNC General Administration requirements, or individual industry contractual agreements.

Text on Screen:
Federal and State Laws:

- HIPAA - Medical Records
- GLBA - Banking (Financial Aid) Information
- FERPA - Student Privacy
- NC Identity Theft Act - PII

NC State Policies & Regulations Examples
POL 08.00.01 - Computer Use Policy
REG 08.00.02 - Computer Use Regulation
REG 08.00.03 - Data Management Procedures
RUL 08.00.16 – NC State University Security Standards for Sensitive Data and Systems
REG 01.25.09 - Privacy/Confidentiality, Release and Security of Protected Health Information

UNC GA Requirements (ISO 27002)

Contractual Agreements:

- PCI DSS - Credit Cards
- Federal Research Agreements with CUI (NIST 800-171)
- Nondisclosure agreements

Slide 7 Reminders and Related Links:

Thank you for completing this course on Data Security. Remember, you are the shield and can defend yourself and the university from cyber attacks. Don't hesitate to seek help when it comes to data security! If you're interested in additional information, you can find all the resources we've talked about in the "resources" tab.

Remember, you are the shield and can defend yourself and the university from cyber attacks!