Welcome to the New Employee Orientation for **Cybersecurity Basics**. Florida State University has an ongoing commitment to secure FSU’s technology environment and to safeguard the data that we are entrusted to protect.

**Navigation:**

- This training course should only take 10 to 15 minutes of your time.
- A panel will appear on the left-hand side once you begin the course.
- Use the menu to move through each of the sections.
- Click on all interactive media to fully engage with the information.
- Select the **Start Course** button at the top of the page to begin.

**CYBERSECURITY FUNDAMENTALS**

**Getting Started**

**AVOIDING CYBERTHREATS**

**What are Cyberthreats?**

**Protecting your Data**

**How to Spot a Phish**
Safe Use of Social Media

RESOURCES & POLICIES

Promote Cybersecurity at FSU

Wrap-up & Resources
First things first

Let’s start with **what you will learn** and **how it applies to your job**. Flip each card to reveal the knowledge and skills you will gain by completing this Cyber Security e-course.

This training is intended to provide a basic overview of cybersecurity for FSU students, staff, and faculty.
You'll learn about various cyber threats and the damage that they can do.

You'll learn how you can keep yourself safe from cyber threats both at work and at home.

Locking the Door
What do you do to keep your home safe? Most people lock the doors when they leave, at the bare minimum. Some have security cameras installed. Others have home alarm systems to protect against intruders.

But intuitive safeguards aren't just for our physical spaces. We store highly sensitive data online, and exposure can mean something far worse, with longer-lasting consequences than losing valuable possessions to a thief.

Watch this video to learn why it’s important to take cybersecurity precautions, as well as tips for keeping your information safe.

**What Is Cybersecurity?**

Cybersecurity involves safeguarding the networks and devices you use to protect your data from online criminals. At the most basic level, this can be locking your phone with facial recognition or using a strong password for your private Wi-Fi connection.
So, why should you care about cybersecurity? Whether you access sensitive data daily through Florida State University networks or simply use your phone to surf the web, any online activity can provide a vulnerability for criminals to exploit—that is, a loophole they can enter through to access personal information.

Now, let’s explore the main types of cyberthreats and how you may encounter them at work or home.
Hackers and criminals carry out cybercrime to exploit others and steal valuable data. Flip the flashcards below to learn more about common types of attacks that could affect you:

**Phishing**

Phishing attacks are carried out through fake emails, text messages, and even phone calls that may seem legitimate—for example, an email from a bank—to get
### What's the Harm?

Failure to put safety locks on your data can result in many harmful scenarios at Florida State University, and beyond. Now that we know what threats exist, let’s find out what damage cyber-threats can cause.

<table>
<thead>
<tr>
<th>Malware</th>
<th>Once malware—delivered through unsecured websites, links, and file attachments—is installed on your computer, an attacker can use the malicious</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Attacks</td>
<td>Denial-of-service attacks (DoS) flood a company’s server with traffic. A distributed denial of service attack (DDoS) uses multiple devices to target a company or even a</td>
</tr>
</tbody>
</table>

---
Keep you from doing your job by denying you access to work networks or files.

Result in the loss or theft of data resulting in violations of data confidentiality.

Compromise work data associated with the University operations and research. This can lead to lawsuits by affected parties, a loss of public trust in your work unit, a loss of grant opportunities, or criminal prosecution in some cases.

Check Your Understanding...

Questions 1 of 3

Cyberthreats can be encountered at one’s work as well as one’s private life.

- True
- False

Submit
Question 2 of 3
Match each type of cyberthreat to its description.

- **Identity thieves**: Parties that attempt to steal your personal information such as social security number.

- **Hackers**: Parties who attempt to gain access to a computer system to steal info or cause damage.

- **Malware**: Computer programs designed to harm your device and steal information.

- **Phishing**: Tricking a user into giving up log-in information or downloading malicious software.
Question 3 of 3
Which of the following is not a likely consequence of being exposed to a cyberthreat?

- Denial of access to work materials
- Bodily injury
- Violation of confidentiality
- Employment consequences

Given the severity of consequences, it's up to you to be the first line of defense against cyberthreats. Up next, we'll show you how to defend and protect your data.
So, what can you do to ensure safety from hackers, intruders, and attackers? These basic tips will help keep your work and personal data safe.

“64% of Americans have had their personal information exposed in a data breach. Protecting yourself against such a breach involves understanding how these threats operate and what you can do to prevent yourself from becoming a victim.

Pew Research Center

Keep Passwords Secure
Predictable words and sequences make weak passwords because hackers can easily run countless word and number combinations to crack your account. The best way to protect yourself from cyber threats is to ensure your passwords are as secure as possible.

Password Tips

- Make sure your passwords are difficult to guess by avoiding dictionary words or common passwords, such as the word password!
- Use long passwords that contain letters, numbers, and symbols.
- Use a secure program like LastPass or KeePass to store your passwords.
- Never share your password with anyone.
- Don’t ever write your password down and keep it near your physical workstation.
Never Share Personal Information

Preventing identity theft is another way to keep cyber threats from ruining your day.

Identity Theft Tips

- Don’t ever volunteer your social security number, driver’s license, credit card, or other personal or financial information unless you’re confident you know who’s receiving it.

- Never send this information through email or instant messaging and remember to protect other people’s personal information similarly.
It’s also a good idea to request a copy of your credit score from major credit bureaus to safeguard against unauthorized activity.

**FSU will never ask you** for your FSUID, username, or password in an email or phone call. We’ll cover *phishing* in the next lesson.

### Always Back Up Your Files

When malware erases files from your device or network, those files are often unrecoverable. So, keep your most important files backed up on an external drive and store them in the cloud.

- **Tip #1:** regularly back up your data onto
- **Tip #2:** be sure to test your backup files occasionally
Keep Software Up to Date

Does your computer notify you when you need a software update? As cumbersome as they may seem, updates protect against potential security breaches by addressing vulnerabilities. Select each marker to explore some common reasons to stay updated.
Upgrading Windows
System Improvements

Updates may add new features to your software and improve functionality.
Enable MFA

Multifactor authentication (MFA) allows you to protect your data through various layers. Instead of merely protecting your account with a password, you also obtain verification through phone or email. So, even if someone obtains your password, they still won't be able to access the account without also having access to your phone or email.
Automatic Updates

Most software and operating systems update automatically. This is usually true with work computers, but it’s a good idea to check with your IT manager to make sure updates are set to occur regularly.

Avoid Malware Threats

Malware is another cyberthreat to guard against. Malware takes many forms, but there are three main types that you should know about. Flip each card below to learn more.
Ransomware attempts to limit access to a system or files until the user pays a ransom.

Spyware records your actions in an attempt to steal valuable data such as your passwords and bank count information.

Adware slows down your computer and tracks your internet usage.
Tips to Avoid Malware Threats

1. **Beware of unknown senders.** Never open or download email file attachments sent by someone you don’t know. Sometimes, the email will seem like it’s from an acquaintance—a method known as *spear-phishing*. So, before opening a file, always double-check the sender’s email address.

2. **Check URLs.** One of the easiest ways to know if you’re entering a safe website is to check the URL. Today, secure websites all use a URL that starts with `https`. If you see that a website URL starts with `http`, it’s not a secure place to conduct sensitive activity.

3. **Use antivirus software.** Be sure to keep your antivirus software (i.e., Norton, McAfee, or Windows Defender) up to date for maximum effectiveness.

Check Your Understanding

Drop and drag the cards below into either the 'True' or 'False' categories. If you are correct, the card will stick. If you are incorrect, you will need to try again.
So to protect against possible vulnerabilities. Information can be used by hackers to make unauthorized purchases.

Cyberthreats can be encountered both at one's work and one's private life.

Installing antivirus software protects your device against all malware.

Hackers can steal your data but not change the data.

It's easy to tell if an email is from someone you know or an unknown sender.
Question 1 of 3
You should never be afraid to say 'no' to suspicious callers if they ask for your personal information.

- True
- False

Question 2 of 3
Match the type of malware to its description.
Question 3 of 3

Which of these strategies is **not** an effective one for protecting your passwords?

- Using different cases, letters, numbers, and symbols
- Using different passwords for different sites
- Writing it down and stick it in your desk drawer
- Never sharing your password with anyone
In a world where most business happens online, protecting your data is as essential as safeguarding your physical space from external threats. The most common types of cybercrime include phishing, malware, and DoS and DDoS attacks. They can result in credit card fraud, loss of company data, and identity theft.

To prevent security breaches, remember these key tips:

1. Keep passwords secure
2. Never share personal information
3. Always back up your files
4. Keep software up to date
5. Avoid malware threats

By taking these proactive measures, you can significantly reduce your chances of exposure to malicious hackers—and protect your privacy from prying eyes.
Small steps can make a world of difference. It may seem daunting to address hacking and security breaches, but these small steps can often save you from big trouble down the road. In most cases, thieves will target a house with a single, easy-to-break lock rather than a home with multiple levels of security.
Imagine This

- A message from your bank requests that you verify your account information.
- A note from an old friend begs you to wire money for an emergency.
- An urgent plea from your streaming service warns that your recent payment was declined and asks you to reenter payment details.
- A student receives an email from an employer promising a high-paying part-time job and they ask for money or personal identification information in exchange.
What do these emails all have in common? They are all examples of **phishing scams**. Learn how to **spot the red flags** of fraudulent emails.

**What Is Phishing?**

**Phishing** is a term for online scams in which attackers impersonate a person or entity the victim trusts to gain access to sensitive information, financial accounts, and more. Phishers
pose as a legitimate company or friend and manipulate targets into performing specific actions. For example, they might trick you into:

- Clicking on a malicious link or downloading an attachment embedded with malware
- Divulging your username, password, or account information
- Wiring money to an account trolled by the scammer

**Common Phishing Examples**

Most computer users know not to click random links in sketchy emails. But as users have become more sophisticated in their use of email and the internet, scammers have gotten trickier, too. Phishing emails come in various forms, but there are some common ruses that cybercriminals use. Let’s take a look at some common phishing scenarios:

**The Contest Winner**

Beware of any email telling you that you’ve won something, especially if you don’t recall entering a contest. No matter the prize offered, you likely won’t receive more than a headache.

**A Message From the Government**

The FBI, CIA, IRS, or any other government entity won’t reach out via email if they need to get in touch. Emails supposedly from the IRS increase around tax time. Be cautious of an email from a government agency. If you think it might be legitimate, look up the phone number on the government website and call to inquire.
Anatomy of a Phishing Email

Millions of phishing scams happen each day. It's impossible to create an exhaustive list of phishing scams because fraudsters create new ones all the time. But phishing emails often

There’s a Problem With Your Account

These phishing emails ask you to log in to verify your account, change your password, or validate account ownership, but the goal is the same—to get your login information. If you’re concerned about your account, independently look up the customer service number or official company email address and ask for more information.

A Friend in Need

Be wary of an email from a friend or relative asking you to send money—especially if the message communicates urgency. Their account was likely hacked—and the request is from a scammer trying to bilk their contacts out of cash. If you receive an email like this, give your loved one a call to make sure they’re OK and let them know they’ve been hacked.

Tech Support

Emails claiming to be from tech support entities informing you that you have a virus or need to download something are a common phishing ruse. Never click on links or downloads, even if they appear to be from a trusted organization like Microsoft or Apple. Instead, purchase and install an antivirus program from a trusted business and routinely run scans and updates.
feature characteristic red flags, and knowing what to look for is the first step in keeping yourself—and your information—safe. Review the following sample phishing email and click on each marker to explore some common warning signs.
Sense of Urgency

Cybercriminals often imbue phishing emails with a sense of urgency because they want to motivate you with panic and fear. Be suspicious of emails with language like, “Act now,” or an all-caps plea like this one: “URGENT!” If you detect a sense of urgency in an email, take time to investigate before clicking.
Typos and Mistakes

Misspellings, grammatical errors, and incorrect or strange phrasing are hallmarks of phishing emails. Scammers don’t proofread as a corporation might, and they may not be sending emails in their native language. If you notice typos in a supposedly professional email, especially in conjunction with other warning signs, it may be a phishing attempt.
Threats

Threatening language is common in phishing emails. Warnings of account closures or missed or failed payments are meant to make you act fast without considering the consequences. If an email features a threat like this, especially if it’s your first time hearing about the issue, it’s likely a phishing attempt.
Threats

Threatening language is common in phishing emails. Warnings of account closures or missed or failed payments are meant to make you act fast without considering the consequences. If an email features a threat like this, especially if it's your first time hearing about the issue, it's likely a phishing attempt.
Request for Personal Information

Many phishing emails include a request to input your account information, verify your password, or solicit other personal credentials or data. If you’re concerned about your account safety and want to log in, open a new window and navigate to the site after independently confirming the correct URL rather than clicking a link embedded in an email.
Deceptive Links

Phishing emails commonly request that the recipient click a link. Fraudsters try to trick people into clicking by creating links that resemble the actual address. For example, they might use a “1” to replace the “i” in a company’s name. Sometimes, they’ll even create spoof websites that look identical to the real thing. It’s critical to inspect links closely before clicking.
Generic Greeting

Phishing emails often begin with generic greetings like “Dear Customer” or “Dear Subscriber.” Most scammers either won’t take time to personalize phishing emails or don’t know your name, so they resort to vague greetings. A legitimate company with whom you do business will typically use your name.
Unfamiliar Recipients

Phishing emails often include other unknown recipients. Check the “To:” and “Cc:” fields of suspicious emails to see if the message was sent to multiple people. If so, the email is probably a phish.

Not all phishing emails will include every red flag. There may just be one or two, so familiarize yourself with all the warning signs.

Other common features of phishing emails to watch for include:

- Unfamiliar or strange sender email addresses
- Odd timestamps (businesses typically won’t send an email at 3 a.m.)
- Attachments that you didn’t request
- Unsolicited messages or other communication not initiated by you
The goal of phishing is to solicit personal information like account credentials, Social Security numbers, passwords, or other sensitive data. Be wary of any email that asks for personal information.

**Question 1 of 2**

You receive an email from Amazon that says your account is about to expire and instructs you to click a link and log in to confirm the account is active. What do you do?

- [ ] Click the link and log in; I don’t want my Amazon account to expire.
Question 2 of 2
You just received an email with an urgent plea from an old friend. They need you to send money ASAP to help them out of a jam. What do you do?

- Find out where to send the money. You should always help a friend in need.
- Call your friend to verify it’s a real request, and then decide what to do.
Reply to the email to ask follow-up questions.
Safe Use of Social Media

Being careful about how you **communicate online** can help keep you safe from cyberthreats.

**Benefits and Risks**

Social media platforms like Facebook, Twitter, Instagram, and LinkedIn have become an important part of our personal and professional lives. We use them to share updates with distant friends and family, find like-minded people, network, expand our influence, or grow and support our customer base. However, just because these platforms are popular doesn’t mean they don’t carry risks. Be mindful of what you put on social media account.

Consider the following stories:
A Video Message

Sonia’s friend sends her a video on Instagram with the message, “OMG! Is this you?!?” Curious, Sonia clicks on the link, which never takes her to the video. Instead, Sonia inadvertently downloads malware (malicious software)—and now, hackers can use her account to send the same malicious link to all of her friends.

A Friend Request

Spencer receives a friend request from a woman he doesn’t recognize. After clicking on her profile, he sees that she went to his high school and has two mutual friends. Feeling guilty for not remembering her, Spencer accepts the request.

**What Spencer doesn’t know:** The account is fake. It’s actually a hacker who wants to gather personal details about Spencer and his network. They will then use this information to launch more deceptive phishing attacks.

A Status Update

Excited about her first vacation abroad, Janine checks in from the airport and broadcasts that she’ll be traveling throughout Europe for the next two weeks. She shares several photos and status updates during her trip.

When she returns home, however, Janine finds a broken window. Someone burglarized her house while it was empty—stealing her jewelry, electronics, and other valuables.
6 Tips for Safe Social Networking

Avoid these dangers by increasing your cybersecurity awareness and following safe social networking practices. Click through the following cards to learn six tips to protect your social media accounts from online predators and prying eyes.
Use Strong Passwords

Account passwords serve as the first line of defense against fraud. Don’t hand the keys to hackers by using easy-to-guess passwords—or the same password for multiple accounts. Instead, follow these guidelines:

- Create a unique password for every account.
- Use a combination of upper and lowercase letters, numbers, and symbols.
- Choose long passwords, ideally eight characters or more.
- Don’t use generic phrases or personal information as your password (such as your last name, birthday, street address, or “abc12345”).
- Enable multifactor authentication (MFA) whenever possible. MFA requires another form of identification beyond your password, such as entering a one-time login code sent to your phone.
Manage Your Privacy Settings

Most social media platforms offer privacy settings that allow you to control who can view your online profile and individual posts. Audit your privacy settings regularly. While businesses and public figures may keep their profiles public to gain followers, the rest of us are safer restricting access to friends and known contacts.

You might also be able to control whether tagged posts, videos, or photos from friends appear on your profile or timeline.

*Tip:* Want to know what strangers can see? Search your name on Google to review what appears publicly.
Reject Friend Requests From Strangers

However, no privacy setting will block strangers that you willingly accept into your network. Examine your friend requests carefully. Do you know them—and how well? Only accept friend requests from people you know and trust, and review your friend list regularly to rid your account of unwelcome guests. You may not want your ex, for example, hanging around.

*Tip:* Online predators can impersonate someone you know by using public photos and information to create a fake or duplicate account. If in doubt, call or text your friend to ensure the account is theirs before accepting.
Share Selectively

Many people use social media to share updates and photos of their life with friends and family. However, even if your profile is private, never forget that you’re still posting personal information online, making it vulnerable to hackers or unintended audiences. Be selective with what you share, and avoid oversharing sensitive or personal information that could be used for fraud, identity theft, or other crimes. That includes your:

- Home address
- Phone number or email address
- Social Security, passport, or driver’s license numbers
- Bank, loan, or credit card information
- School, family, or work information
- Car information

**Additional considerations:** You might also think twice about sharing your location or travel plans. Thieves sometimes target homes or cars of people they know are out of town, and stalkers may follow online location “check-ins” to track down victims.
Don’t Click on Suspicious Links

Malicious links are one of the most common ways hackers manipulate victims into downloading malware. Always think before you click. Avoid clicking articles with shocking or sensationalized headings or ads promoting “free” gifts or other offers that seem too good to be true. Also, be wary of friends who send you a link with a vague or generic message, such as “Check this out!” Their account may be hacked.

*The bottom line:* Trust your gut. If a link seems “phishy,” don’t click.
Update Your Software Regularly

Finally, defend your device from cyberattacks by installing antivirus software and keeping your computer operating system, browser, and other programs current. Software updates often include critical security patches, so don’t procrastinate installing them.
Summary

Many of the tips covered here boil down to adopting a few simple habits: Practice good password and computer security, restrict public access to your accounts, avoid oversharessing, and be aware of common scams and take care to avoid them.

Watch your webcam. Many social platforms enable users to share live or pre-recorded videos—or they allow you to video chat with friends. Be careful when using these functions. Hackers can hijack webcams and turn them on remotely to spy on you. There’s also a risk of user error if you forget to turn your video off after using it—or you accidentally press “record.”
Promote Cybersecurity at FSU

Cybersecurity Tips for Work

Contact your IT manager at cybersecurity issues. Your IT manager can provide information about current cybersecurity measures in place in your work unit and help you identify policy violations or security weaknesses. You can ask them about implementing new cybersecurity measures. Remember, cybersecurity is everyone’s responsibility.
1. Check with your IT manager before you install new programs on your work device.

2. Avoid opening links and attachments in your emails if you cannot verify the source of the message.

3. Use a cross-cut shredder when you are destroying sensitive documents with non-directory student information, proprietary FSU information, or social security numbers.

4. Take a moment to read FSU’s information security and privacy policies.

Cybersecurity tips that you use at work are also good for your home! Scroll and flip each card below for more ways to promote cybersecurity.

Secure your Technology

Don’t leave your devices unsupervised or in plain view. Make sure to password protect your devices and set up a screen timeout.
Use a Firewall

Install a firewall on your home computer and run anti-malware scans regularly.

User Accounts

Set up separate user accounts with different family members.

Programs and Apps

Try to avoid installing unnecessary programs or apps on your devices.
Copyright Restrictions

Pay attention to copyright restrictions with downloading software, games, movies, or music.

Check Your Understanding...

Question 1 of 5
Allowing data to be exposed to cyberthreats can result in professional and legal consequences, both for myself and my work unit.
Question 2 of 5
Which of the following is true regarding patching your devices?
Select all that apply.

- Patches may improve your device or program functionality
- Many programs apply patches automatically
- It isn’t necessary to apply patches regularly
They can keep you safe from cyberthreats

True

False

Question 3 of 5
Florida State University will sometimes ask you for your username, FSUID, or password over the phone or email.
Question 4 of 5
What should you use to destroy physical copies of non-directory student information, proprietary FSU information, or social security numbers?

- [ ] Cross-cut paper shredder
- [ ] Recycle bin
- [ ] Your home trash can
- [ ] All of the above
Question 5 of 5

Sometimes it’s **not necessary** to check with my IT manager to install new programs on my work device.

- [ ] True
- [ ] False

**Great job!** You have completed the Cyber Security Basics training.
Questions?

If you have questions about cybersecurity and cyberthreats be sure to check out FSU’s cybersecurity resources at its.fsu.edu/ispo or follow FSU ITS on Twitter @floridastateITS.
We want your feedback!

Please take a brief survey to help improve upon future training for FSU employees.