UNIVERSITY OF RICHMOND

SpiderSecure Training Program (Fall 2024 – Spring 2025)

Table of Contents

Back to the top

INTRODUCTION

The goal of the SpiderSecure Training Program is to provide cybersecurity awareness and education to the UR faculty/staff. In today's advancing technology landscape, it is even more important to understand the risks and ways to secure your devices and online accounts. Whether accessing the UR network from home, on campus, or abroad it is important the UR community knows what they can do to be able to get the best technology experience while staying SpiderSecure.

- **Course Description**
  - Cybersecurity topics will provide a range of security recommendations, tips, and tools to help you know how to better secure your devices and online accounts. Each semester there will be new concepts shared across the UR community. This will allow you to have sufficient time to work through and complete the lessons for each cybersecurity topic. Lessons will include but not limited to watching videos, self-guided web page reading, and completing surveys.
- **Objectives**
  - To familiarize UR faculty/staff of the cybersecurity basics to best secure devices and online accounts.
  - To familiarize UR faculty/staff of the security tools provided by UR to help best secure devices and online accounts.
  - To familiarize UR faculty/staff of the compliance and regulation of data security and privacy at UR.
- **Learning Outcomes**
  - UR faculty/staff understands and practices the cybersecurity basics to best secure devices and online accounts.
  - UR faculty/staff understands and utilizes the security tools provided by UR to help best secure devices and online accounts.

- UR faculty/staff understands the compliance and regulation of data security and privacy at UR.

Back to the top

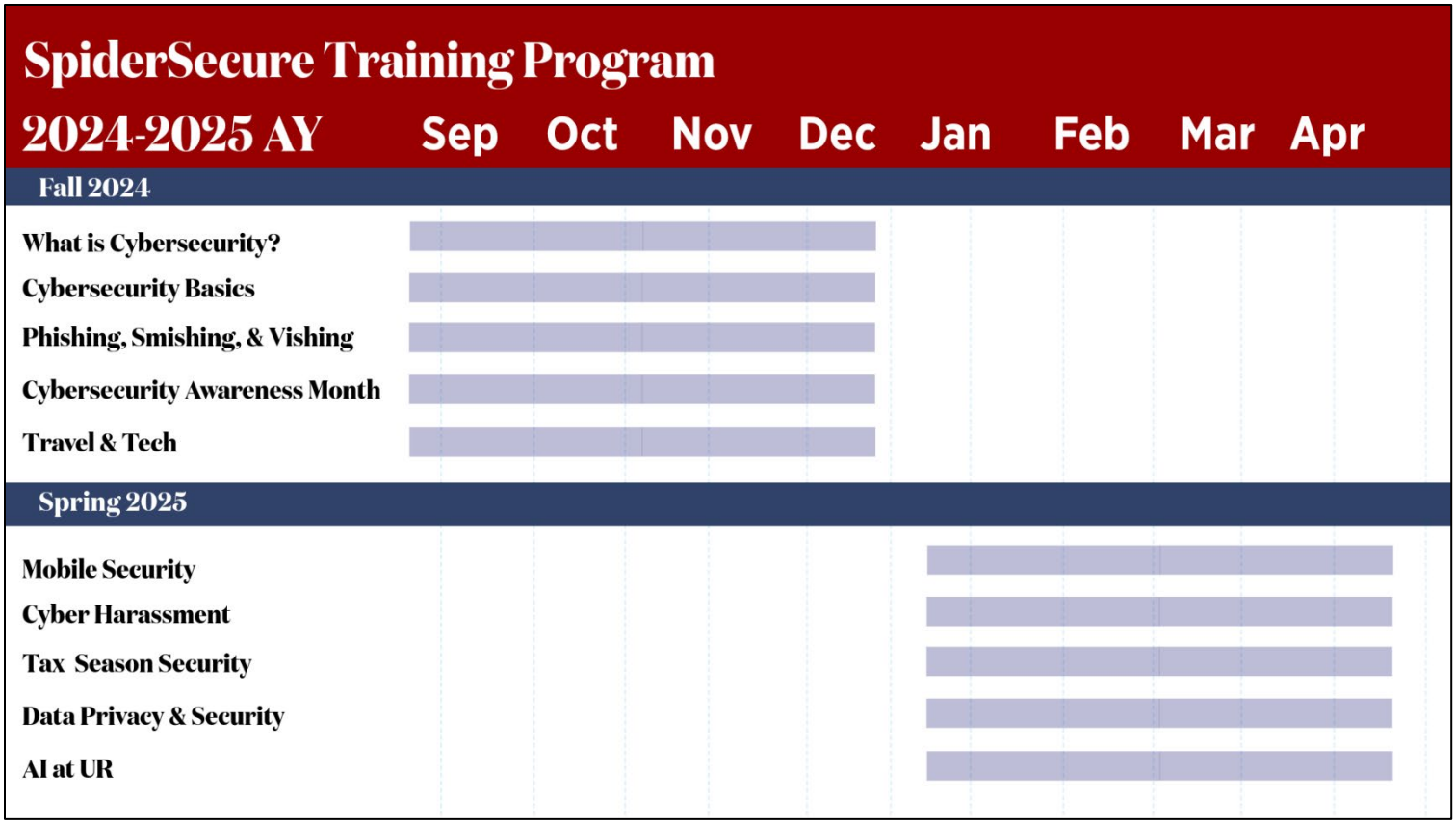
TRAINING COURSE COORDINATION

The Information Services Security team has developed the SpiderSecure Training Program; it will be reviewed and updated as needed. The training program will commence at the beginning of the fall academic year and topics will be covered across the fall and spring semesters. For additional support, questions, or concerns email the IS security team at **infosec@richmond.edu**.

- **Evaluation & Grading**
  - Assignments will be marked complete or incomplete.
    - No grades will be given.
  - Assignments will be conducted and completed on LinkedIn Learning which will be assigned by HR through Workday.
    - At the end of Spring 2025, a SpiderSecure Survey will be available for completion.
  - At the end of Spring 2025, a SpiderSecure Survey link will be sent out through SpiderBytes and a QR code link will be published on digital Signs. The SpiderSecure Survey is a feedback form to help improve future versions of the SpiderSecure Training Program.
  - Faculty/staff members who have completed some or all of the SpiderSecure Training Program will be eligible for the 2024-2025 SpiderSecure Incentive Program.
- **Training Course Schedule**
  - The following topics below will be covered.
    - Fall 2024 (Sep 2024 to Dec 2024)
      - What is Cybersecurity?
      - Cybersecurity Basics
      - Phishing, Smishing, and Vishing
      - Cybersecurity Awareness Month
      - Travel and Tech
    - Spring 2025 (Jan 2025 to Apr 2025)

- Mobile Security
- Cyber Harassment
- Tax Season Security
- Data Privacy & Security
- AI at UR

  - Timeline is from September 2024 to April 2025.
  - See below for an overview of the SpiderSecure Training Program.



[Back to the top](#)

FALL 2024 (SEP 2024 TO DEC 2024)

From September 2024 to December 2024, the following cybersecurity topics will be covered. Continue to learn more about the Fall 24 SpiderSecure cybersecurity topics.

- **What is cybersecurity awareness and education?**

- It is the practice and application of sharing, educating, and empowering a cybersecurity-conscious culture when accessing technology using any device from any place. UR's Information Services Security team is responsible for providing and managing a cybersecurity awareness and education to help support the UR community in securely using UR devices and accessing UR networks while still getting the best experience.

- **Cybersecurity Basics**
  - The 5 Basics
    - Use up-to-date software.
    - Use multi-factor authentication (MFA).
    - Use a VPN.
    - Use a high-quality antivirus software.
    - Use secure passwords (and a password manager).
  - **Computers (i.e. desktops, laptops)**
    - You should be able to know and feel you are secure when using your computer/laptop for work, school, or personal.
    - Maintaining a secure computer/laptop means knowing where to get the latest software updates, having a trustworthy antivirus software, and being able to securely store and use secure passwords when accessing online accounts.
  - **Mobile Devices (i.e. phones, tablets)**
    - Mobile devices can be susceptible to different cybersecurity risks such as outdated apps, end of support for devices after a certain period of time, and targeted mobile device attacks.
  - **AI Security**
    - ChatGPT and other Generative AI technologies are increasingly becoming integrated in the classrooms and across the UR community spaces.
    - It will be even more important to be aware of the security concerns especially related to data and privacy regulatory standards.
- **Phishing, Vishing, Smishing**
  - **Phishing** is an email-based cyber-attack that targets individuals through well-crafted emails.
    - The goal of the attack is to trick users into opening up the email and clicking on any attachments or links.

- **Smishing** is a text-message based cyber-attack that targets individuals through SMS (Short Message Service) or text messages. The term is a combination of "SMS" and "phishing."
  - Just like email-based phishing attacks, these deceptive messages often appear to be from trusted sources, and they use social engineering tactics to create a sense of urgency, curiosity, or fear to manipulate the recipient into taking an undesired action.
- **Vishing** is a phone-based cyber-attack that targets individuals through phone calls or voicemail. The term is a combination of "voice" and "phishing."
  - This attack may be calls from attackers claiming to be government agencies such as the IRS, software vendors like Microsoft, or services offering to help with benefits or credit card rates. Attackers will often appear to be calling from a local number close to yours. As with smishing, flaws in how caller ID and phone number verification work make this a dangerous attack vector.

- **Cybersecurity Awareness Month**
  - October is Cybersecurity Awareness Month (CAM). This is a collaborative effort between the U.S. Department of Homeland Security (DHS), and its public and private partners, including the National Cyber Security Alliance (NCSA), to raise awareness about the importance of cybersecurity and exercising good cybersecurity hygiene. The University of Richmond joins other institutions of higher education in raising awareness of the vital role cybersecurity plays in a protecting the UR community. We have partnered with DHS and NCSA to bring this year's event to campus.
  - This year's theme for the 2024 Cybersecurity Awareness Month is TBD and the topics of focus will be the following below.
    - TBD.
- **Travel and Tech**
  - Due to enhanced security measures in most countries, travelers with tech should be prepared for possible disruptions or additional wait times during the screening process. Here are some of the few steps you can take to help secure your devices and your privacy.
    - Take only needed technology.
      - This may mean leaving some of your devices at home, using temporary devices, removing personal data from your devices, or shifting your data to a secure cloud service. Authorities or criminals cannot search (or take) what you do not have.
    - Back-up and encrypt

        - Protect the information your devices bring. Make sure to fully encrypt your device and make a full backup of your data that you leave back at home.
    - Use a VPN, Say no to unsecured public Wi-Fi
        - However, using an unsecured public Wi-Fi hotspot can allow others to view the contents of your electronic activity. Never access your sensitive financial accounts from an unsecured network.
    - Pause before posting on social media
        - It can be fun to share vacation pictures in the moment, but online postings on social networks (e.g., Tik Tok, Facebook, Instagram, Snapchat, etc.) can let other people know that you are not at home and that your home may be empty. Posting vacation pictures on social media once you are safely home helps protect your physical belongings.

- **Fall 2024 Assignments**
    - **LinkedIn Learning (Fall 24 SpiderSecure Training)**
        - Updating software (From the course: Cybersecurity at Work)
            - Video Length: 2m 27s
        - Phishing (From the course: Cybersecurity Awareness: Web3, Crypto, and NFTs)
            - Video Length: 2m 50s
        - SMS phishing: A text-based attack (From the course: Cybersecurity Awareness: Phishing Attacks)
            - Video Length: 3m 30s
        - Vishing (From the course: Cybersecurity Awareness: Social Engineering)
            - Video Length: 1m 59s
        - Secure your home and office (From the course: Traveling for Business)
            - Video Length: 3m 21s
        - Understanding public Wi-Fi and hotspots (From the course: Cybersecurity Awareness: Cloud Security)
            - Video Length: 4m 19s
    - **Visit IS Security website and review the webpages below.**
        - Cybersecurity Basics
            - Reading Length: 3 - 5 minutes

- Phishing, Smishing, Vishing
  - Reading Length: 3 – 5 minutes
- Cybersecurity Awareness Month
  - Reading Length: 3 - 5 minutes
- Travel & Tech
  - Reading Length: 3 – 5 minutes

Back to the top

SPRING 2025 (JAN 2025 TO APRIL 2025)

From January 2025 to April 2025, the following cybersecurity topics will be covered. Continue to learn more about the Spring 25 SpiderSecure cybersecurity topics.

- **Mobile Security**
  - Multi-Factor Authentication
    - Multi-Factor Authentication, or MFA, is one of the most effective methods of protecting yourself against credential compromise. Many organizations are making MFA a requirement to access accounts and information portals that contain confidential or sensitive data pertaining to their users or services. In a study conducted by Microsoft it was concluded that 99.9% of account compromise incidents examined during the period of their study would have been prevented had the organizations utilized MFA.[1]
    - The University of Richmond utilizes Duo MFA and encourages all students, faculty, and staff to enable MFA wherever possible to protect their sensitive data. This simple and effective control could prevent you from becoming the victim of account compromise or identity theft.
      - For instructions in "How to Enroll in Duo", please refer to the SpiderTechNet article.
- **Cyber Harassment**

[1] https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

- The common factor is the use of technology to establish power and control by causing fear and/or intimidation. It is intentional and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. This may include the criminal tracking down someone's personal and private information and using it to make them afraid. Examples of cyber harassment include but is not limited to:
  - Cyber bullying – Creating harmful posts, sharing personal or false information, inciting others to harass a target on-line. This may mean leaving some of your devices at home, using temporary devices, removing personal data from your devices, or shifting your data to a secure cloud service. Authorities or criminals cannot search (or take) what you do not have.
  - Cyberstalking – Cyberstalking is a crime in which someone harasses or stalks a victim using electronic or digital means.
  - Doxing – Sourcing and collecting someone's personal/private information and then publicly releasing it online.
  - Trolling – The act of posting damaging or harassing comments on social media to purposefully insult or humiliate the recipient.
  - Hate Speech – offensive discourse targeting a group, or an individual based on inherent characteristics (such as race, religion or gender) and that may threaten social peace.

- **Tax Season Security**
  - It is that time of the year again, "Tax Season". It is not just a busy time for taxpayers but also for cybercriminals. Thousands of people have lost millions of dollars and their personal information to tax scams. Tax-related identity scams occurs when someone uses your stolen personal information, including your Social Security number, to file a tax return claiming a fraudulent refund.
- **Data Privacy & Security**
  - How does UR classify its data?
  - What are UR's data security and privacy regulatory standards?
- **AI at UR**
  - How does ChatGPT use your content data aka data input?
  - What are some examples of inappropriate use of ChatGPT at UR?
- **<u>Spring 25 Assignments</u>**

- **LinkedIn Learning (Spring 25 SpiderSecure Training)**
  - Multifactor authentication (From the course: Cybersecurity at Work)
    - Video Length: 1m 42s
  - Treat Others Respectfully Online (From the course: Working and Collaborating Online)
    - Video Length: 1m 55s
  - Recognize Phone Scams (From the course: Security Tips)
    - Video Length: 6m 42s
  - Personal Data Security (From the course: Cybersecurity Awareness: Social Engineering)
    - Video Length: 1m 31s
  - What is AI? (From the course: Introducing AI to Your Organization)
    - Video Length: 2m 23s
  - Generative AI and where each of us fits in (From the course: Get Ready for Generative AI)
    - Video Length: 5m 20s
- **Visit IS Security website and review the webpages below.**
  - Mobile Security
    - Reading Length: 3 – 5 minutes
  - Cyber Harassment
    - Reading Length: 3 - 5 minutes
  - Tax Season Security
    - Reading Length: 3 – 5 minutes
  - AI at UR
    - Reading Length: 3 - 5 minutes
  - Data Classification Standard
    - Reading Length: 3 – 5 minutes
  - Data Security Standard
    - Reading Length: 3 – 5 minutes

Back to the top

SPIDERSECURE INCENTIVE PROGRAM

SpiderSecure Training Program (Fall 2024 – Spring 2025)

UR faculty/staff members who complete some or all of the SpiderSecure Training Program (Fall 2024 – Spring 2025) will be recognized. It is important to recognize individual efforts to improve one's cybersecurity awareness to be able to best support the UR community in being SpiderSecure.

- UR faculty/staff who complete **SOME** training will receive the following listed.
  - A Certificate of Completion.
- UR faculty/staff who complete **ALL** training will receive the following listed.
  - A Certificate of Completion.
  - A custom 2024-2025 SpiderSecure Champion Sticker.

  - Eligibility to receive swag as a SpiderSecure Incentive Program participant.
- The SpiderSecure Incentive Program encourages UR faculty/staff members to continue being SpiderSecure and earn more rewards for completing the annual SpiderSecure Training Program. The chart below shows the prizes one can earn based on the number of stickers achieved.

1 SpiderSecure Sticker	1 x Raffle entry for a Mug
3 SpiderSecure Stickers	1 x T-Shirt
5 SpiderSecure Stickers	1 x Hoodie

[Back to the top](#)

SUMMARY

Cybersecurity is a shared responsibility. The Information Security staff is responsible for helping the University of Richmond community protect information resources by building security awareness and having the appropriate security controls in place. Whether accessing the UR network from home, on campus, or abroad it is important the UR community knows what they can do to be able to get the best technology experience while staying SpiderSecure.

- **References & Resource Links**
  - IS Security Website
  - IS Policy Information
  - IS Services

Back to the top