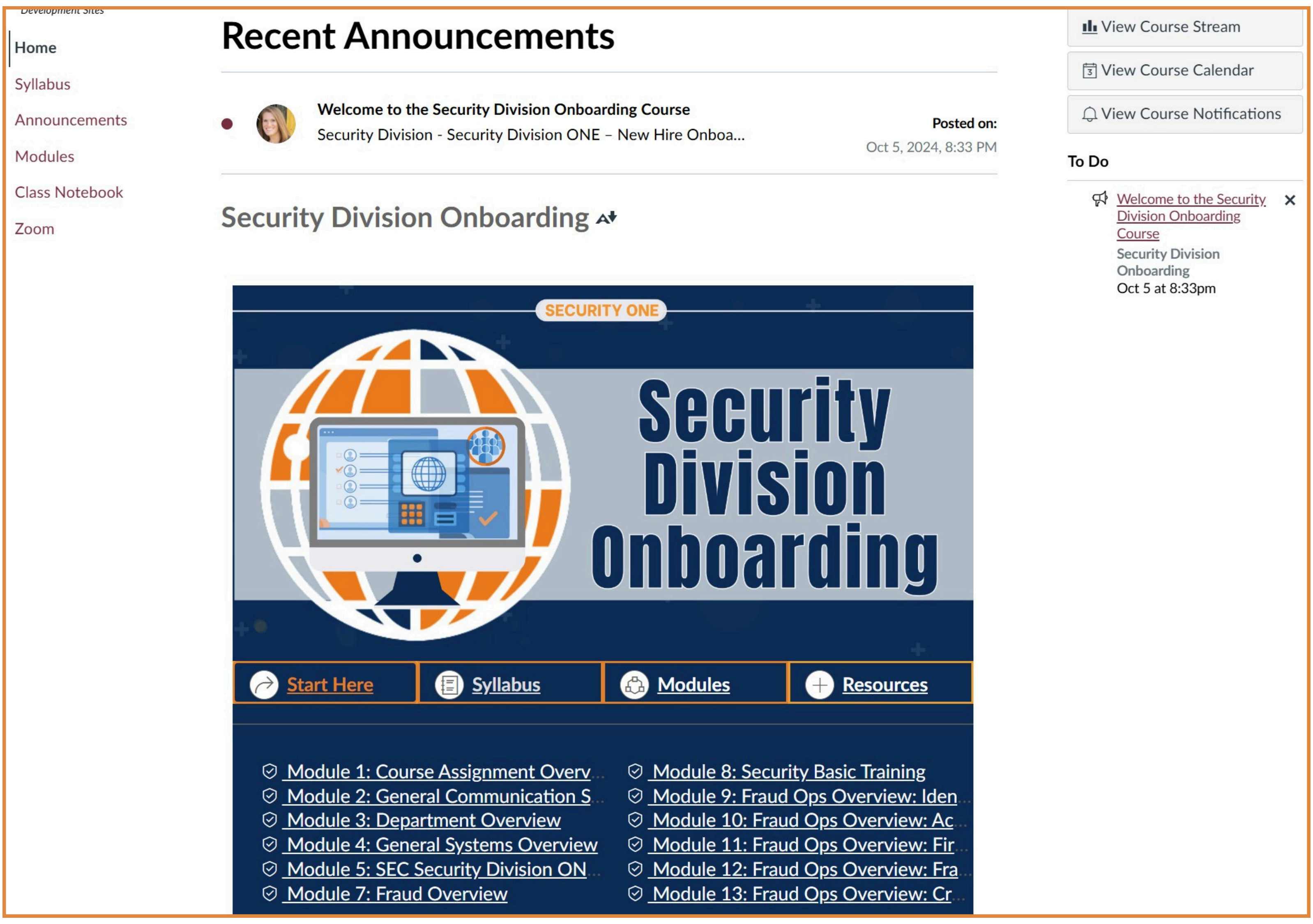


Development Sites

- Home
- Syllabus
- Announcements
- Modules
- Class Notebook
- Zoom

Recent Announcements

● **Welcome to the Security Division Onboarding Course**
Security Division - Security Division ONE – New Hire Onboa...
Posted on: Oct 5, 2024, 8:33 PM

Security Division Onboarding

Start Here | Syllabus | Modules | Resources

- Module 1: Course Assignment Overv...
- Module 2: General Communication S...
- Module 3: Department Overview
- Module 4: General Systems Overview
- Module 5: SEC Security Division ON...
- Module 7: Fraud Overview
- Module 8: Security Basic Training
- Module 9: Fraud Ops Overview: Iden...
- Module 10: Fraud Ops Overview: Ac...
- Module 11: Fraud Ops Overview: Fir...
- Module 12: Fraud Ops Overview: Fra...
- Module 13: Fraud Ops Overview: Cr...

View Course Stream
View Course Calendar
View Course Notifications

To Do

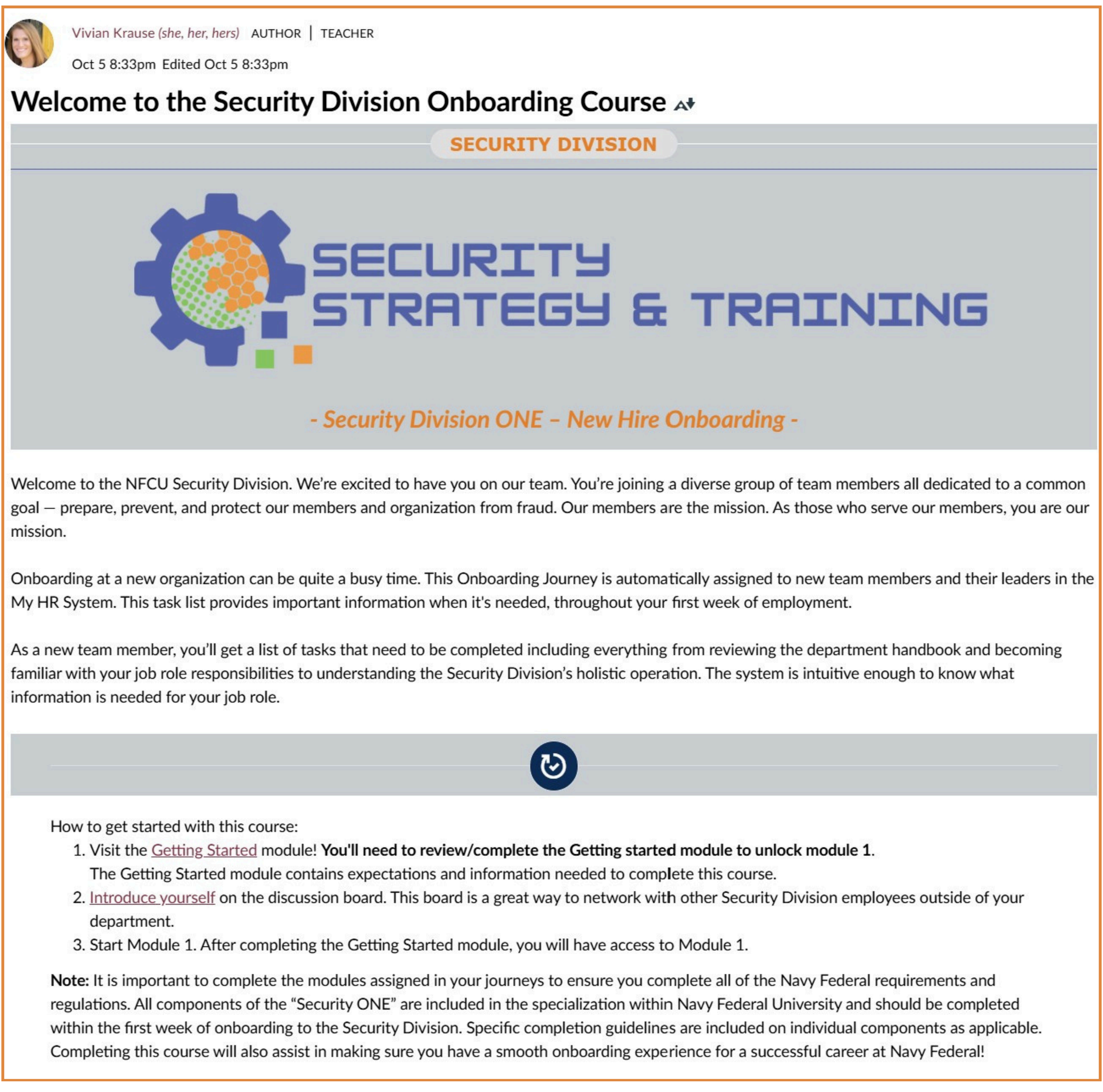
Welcome to the Security Division Onboarding Course
Security Division Onboarding
Oct 5 at 8:33pm

SECURITY ONE

Security Division Onboarding

Start Here | Syllabus | Modules | Resources

- Module 1: Course Assignment Overv...
- Module 2: General Communication S...
- Module 3: Department Overview
- Module 4: General Systems Overview
- Module 5: SEC Security Division ON...
- Module 7: Fraud Overview
- Module 8: Security Basic Training
- Module 9: Fraud Ops Overview: Iden...
- Module 10: Fraud Ops Overview: Ac...
- Module 11: Fraud Ops Overview: Fir...
- Module 12: Fraud Ops Overview: Fra...
- Module 13: Fraud Ops Overview: Cr...



Vivian Krause *(she, her, hers)* AUTHOR | TEACHER
Oct 5 8:33pm Edited Oct 5 8:33pm

Welcome to the Security Division Onboarding Course

- Security Division ONE – New Hire Onboarding -

Welcome to the NFCU Security Division. We're excited to have you on our team. You're joining a diverse group of team members all dedicated to a common goal — prepare, prevent, and protect our members and organization from fraud. Our members are the mission. As those who serve our members, you are our mission.

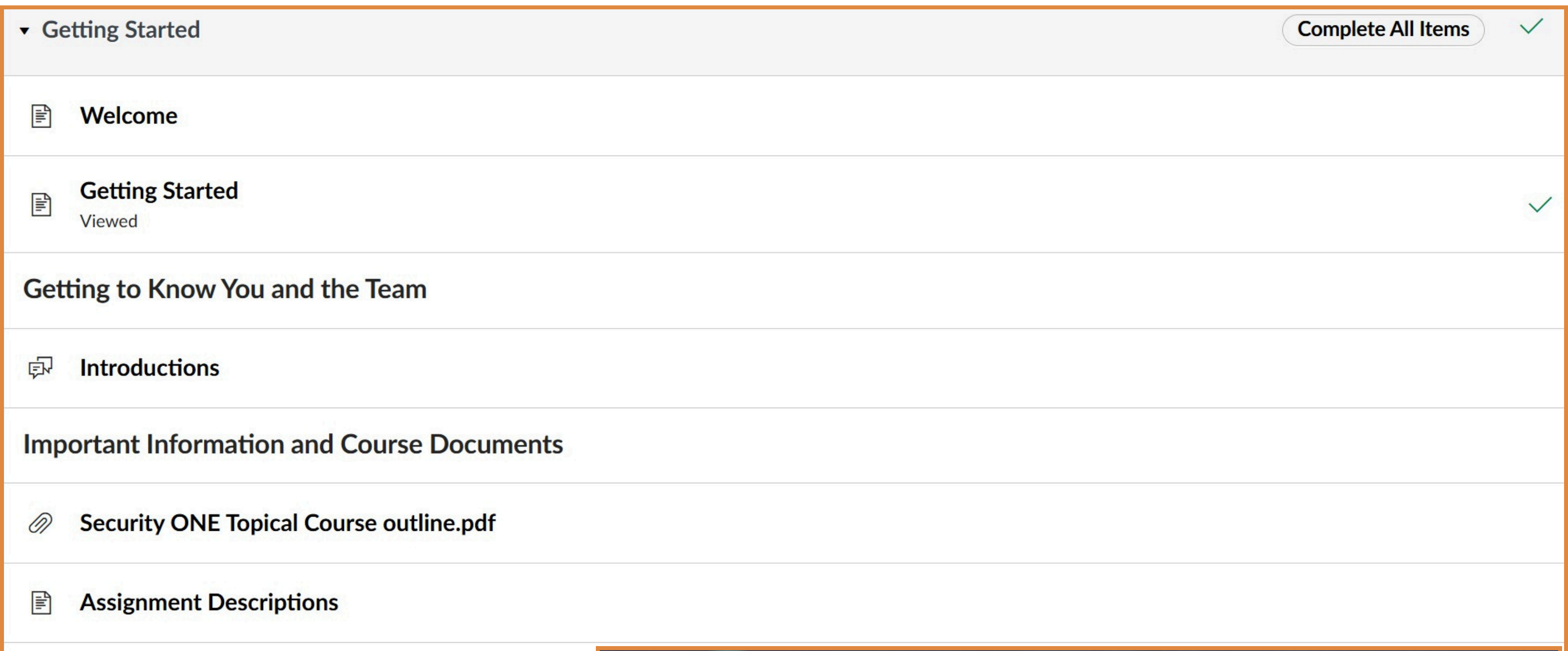
Onboarding at a new organization can be quite a busy time. This Onboarding Journey is automatically assigned to new team members and their leaders in the My HR System. This task list provides important information when it's needed, throughout your first week of employment.

As a new team member, you'll get a list of tasks that need to be completed including everything from reviewing the department handbook and becoming familiar with your job role responsibilities to understanding the Security Division's holistic operation. The system is intuitive enough to know what information is needed for your job role.

How to get started with this course:

1. Visit the Getting Started module! **You'll need to review/complete the Getting started module to unlock module 1.** The Getting Started module contains expectations and information needed to complete this course.
2. Introduce yourself on the discussion board. This board is a great way to network with other Security Division employees outside of your department.
3. Start Module 1. After completing the Getting Started module, you will have access to Module 1.

Note: It is important to complete the modules assigned in your journeys to ensure you complete all of the Navy Federal requirements and regulations. All components of the "Security ONE" are included in the specialization within Navy Federal University and should be completed within the first week of onboarding to the Security Division. Specific completion guidelines are included on individual components as applicable. Completing this course will also assist in making sure you have a smooth onboarding experience for a successful career at Navy Federal!



▾ Getting Started

Complete All Items ✓

Welcome

Getting Started
Viewed ✓

Getting to Know You and the Team

Introductions

Important Information and Course Documents

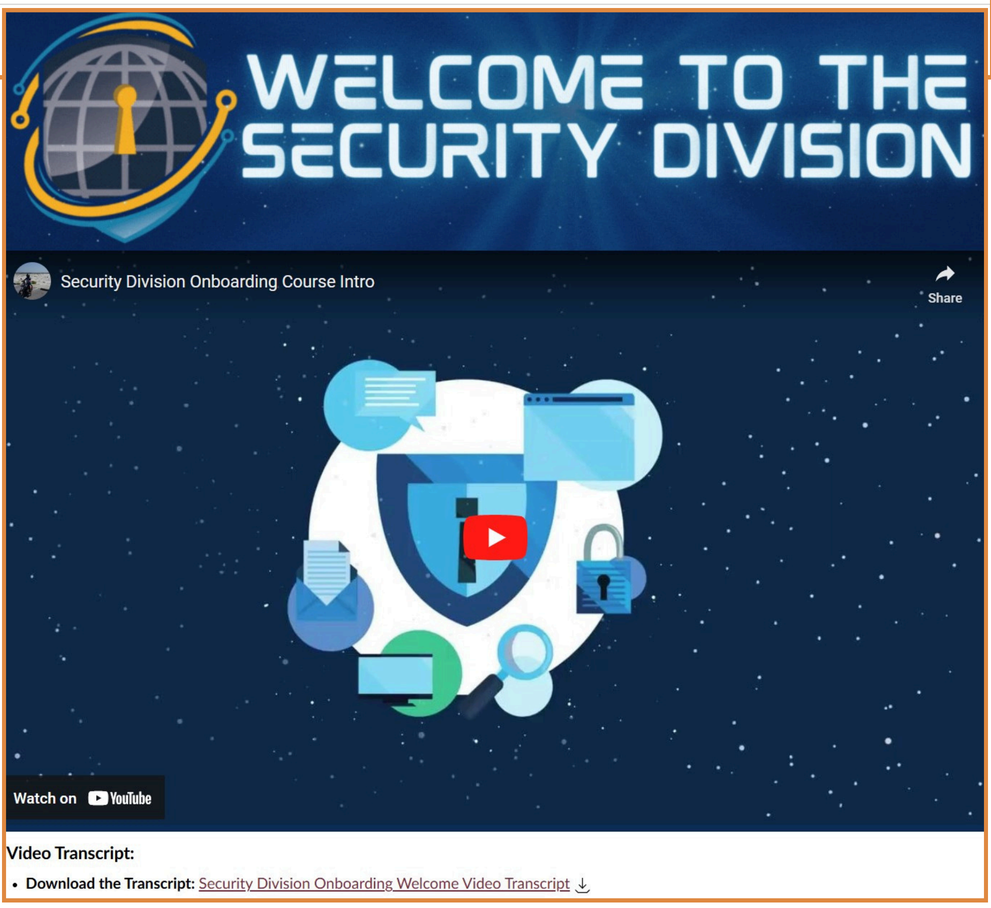
Security ONE Topical Course outline.pdf

Assignment Descriptions

Security ONE Course Overview and Policies.pdf

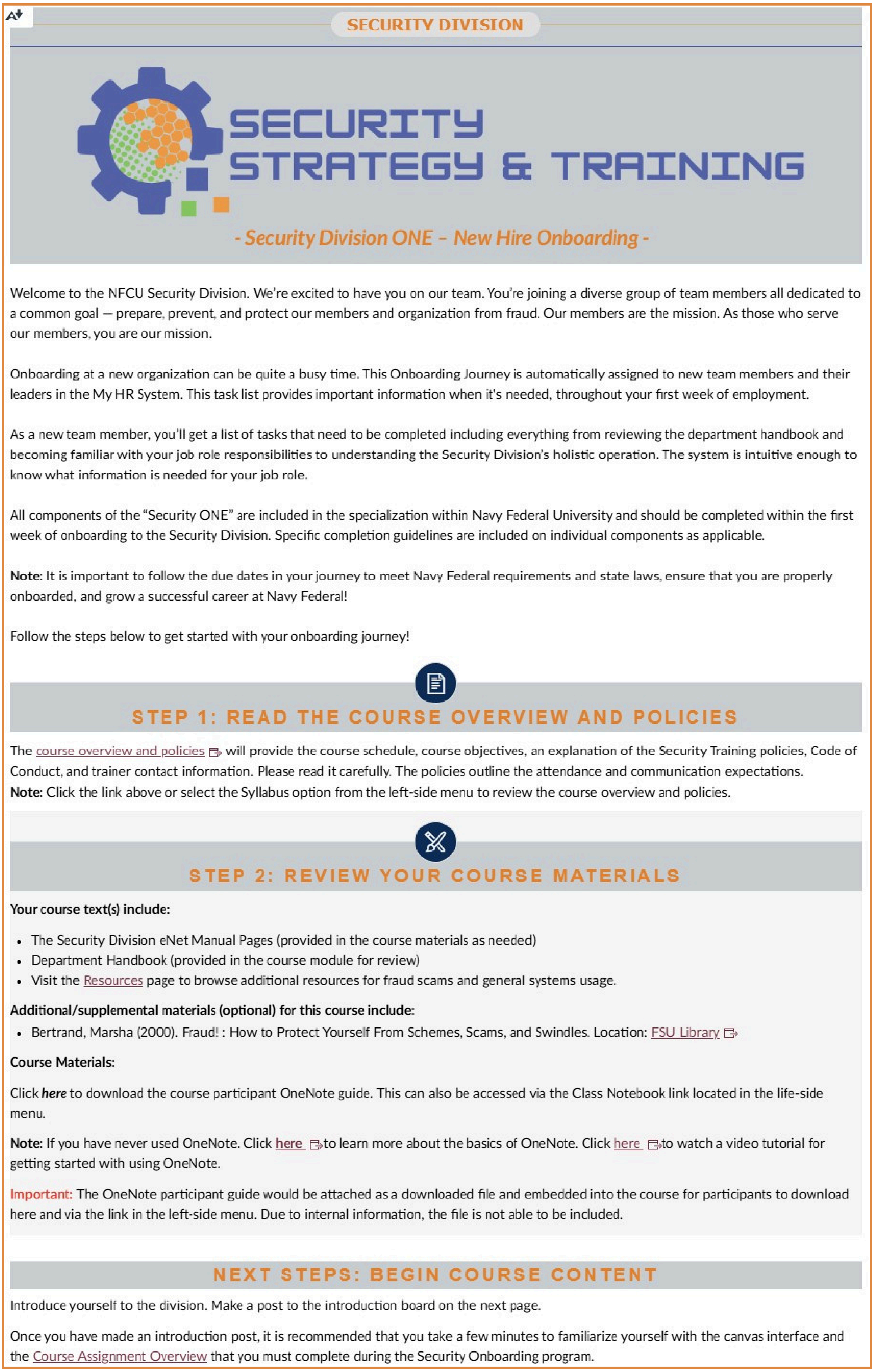
Click the link: Welcome Video to watch the course introduction video.

Click here to read the video transcript.


WELCOME TO THE SECURITY DIVISION
Security Division Onboarding Course Intro
Share
Watch on YouTube

Video Transcript:

- Download the Transcript: Security Division Onboarding Welcome Video Transcript



- Security Division ONE – New Hire Onboarding -

Welcome to the NFCU Security Division. We're excited to have you on our team. You're joining a diverse group of team members all dedicated to a common goal — prepare, prevent, and protect our members and organization from fraud. Our members are the mission. As those who serve our members, you are our mission.

Onboarding at a new organization can be quite a busy time. This Onboarding Journey is automatically assigned to new team members and their leaders in the My HR System. This task list provides important information when it's needed, throughout your first week of employment.

As a new team member, you'll get a list of tasks that need to be completed including everything from reviewing the department handbook and becoming familiar with your job role responsibilities to understanding the Security Division's holistic operation. The system is intuitive enough to know what information is needed for your job role.

All components of the "Security ONE" are included in the specialization within Navy Federal University and should be completed within the first week of onboarding to the Security Division. Specific completion guidelines are included on individual components as applicable.

Note: It is important to follow the due dates in your journey to meet Navy Federal requirements and state laws, ensure that you are properly onboarded, and grow a successful career at Navy Federal!

Follow the steps below to get started with your onboarding journey!

STEP 1: READ THE COURSE OVERVIEW AND POLICIES

The course overview and policies will provide the course schedule, course objectives, an explanation of the Security Training policies, Code of Conduct, and trainer contact information. Please read it carefully. The policies outline the attendance and communication expectations.

Note: Click the link above or select the Syllabus option from the left-side menu to review the course overview and policies.

STEP 2: REVIEW YOUR COURSE MATERIALS

Your course text(s) include:

- The Security Division eNet Manual Pages (provided in the course materials as needed)
- Department Handbook (provided in the course module for review)
- Visit the Resources page to browse additional resources for fraud scams and general systems usage.

Additional/supplemental materials (optional) for this course include:

- Bertrand, Marsha (2000). Fraud! : How to Protect Yourself From Schemes, Scams, and Swindles. Location: FSU Library

Course Materials:

Click ***here*** to download the course participant OneNote guide. This can also be accessed via the Class Notebook link located in the life-side menu.

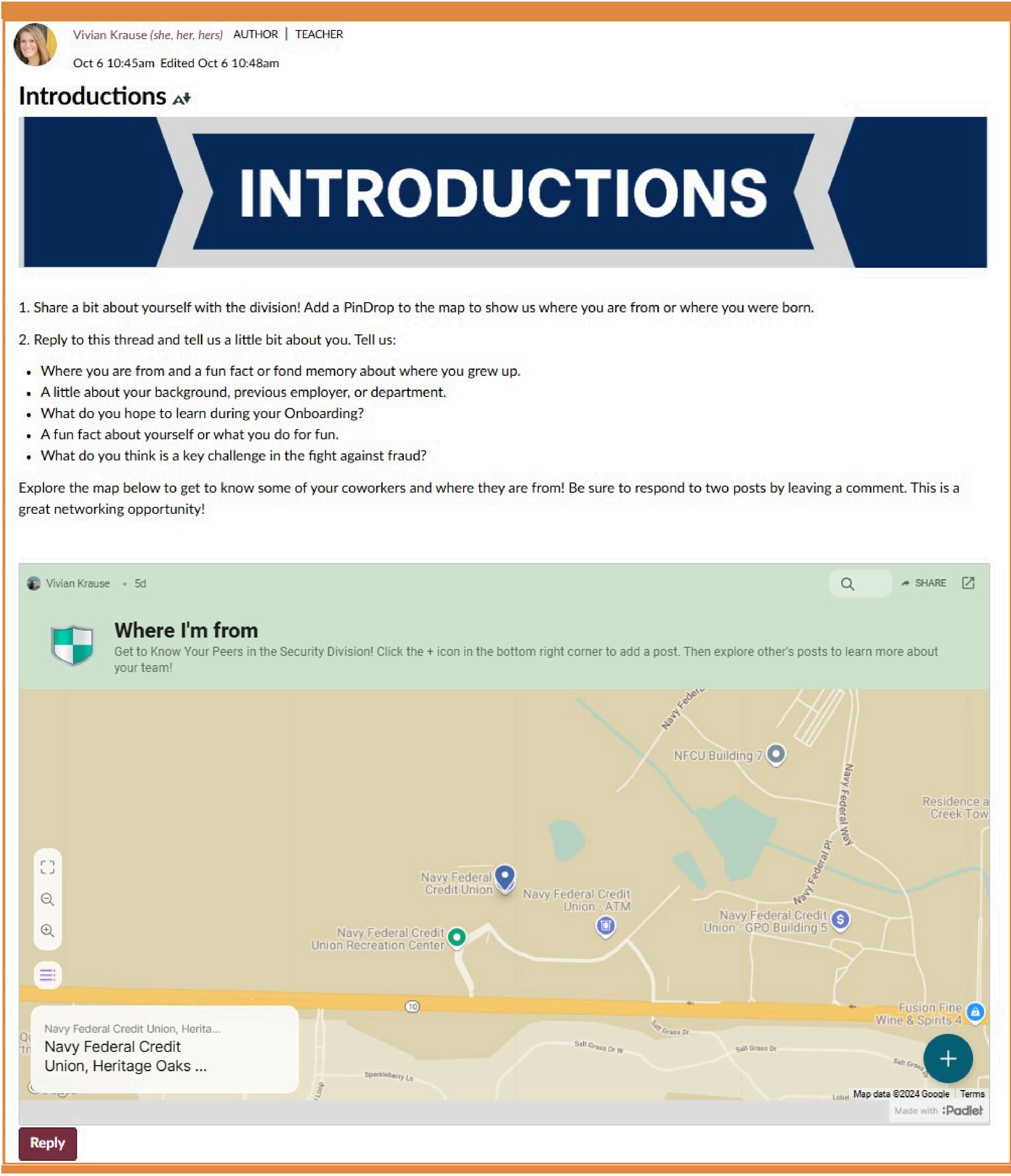
Note: If you have never used OneNote. Click **here** to learn more about the basics of OneNote. Click here to watch a video tutorial for getting started with using OneNote.

Important: The OneNote participant guide would be attached as a downloaded file and embedded into the course for participants to download here and via the link in the left-side menu. Due to internal information, the file is not able to be included.

NEXT STEPS: BEGIN COURSE CONTENT

Introduce yourself to the division. Make a post to the introduction board on the next page.

Once you have made an introduction post, it is recommended that you take a few minutes to familiarize yourself with the canvas interface and the Course Assignment Overview that you must complete during the Security Onboarding program.



Vivian Krause (she, her, hers) AUTHOR | TEACHER

Oct 6 10:45am Edited Oct 6 10:48am

Introductions

INTRODUCTIONS

1. Share a bit about yourself with the division! Add a PinDrop to the map to show us where you are from or where you were born.

2. Reply to this thread and tell us a little bit about you. Tell us:

- Where you are from and a fun fact or fond memory about where you grew up.
- A little about your background, previous employer, or department.
- What do you hope to learn during your Onboarding?
- A fun fact about yourself or what you do for fun.
- What do you think is a key challenge in the fight against fraud?

Explore the map below to get to know some of your coworkers and where they are from! Be sure to respond to two posts by leaving a comment. This is a great networking opportunity!

Vivian Krause • 5d

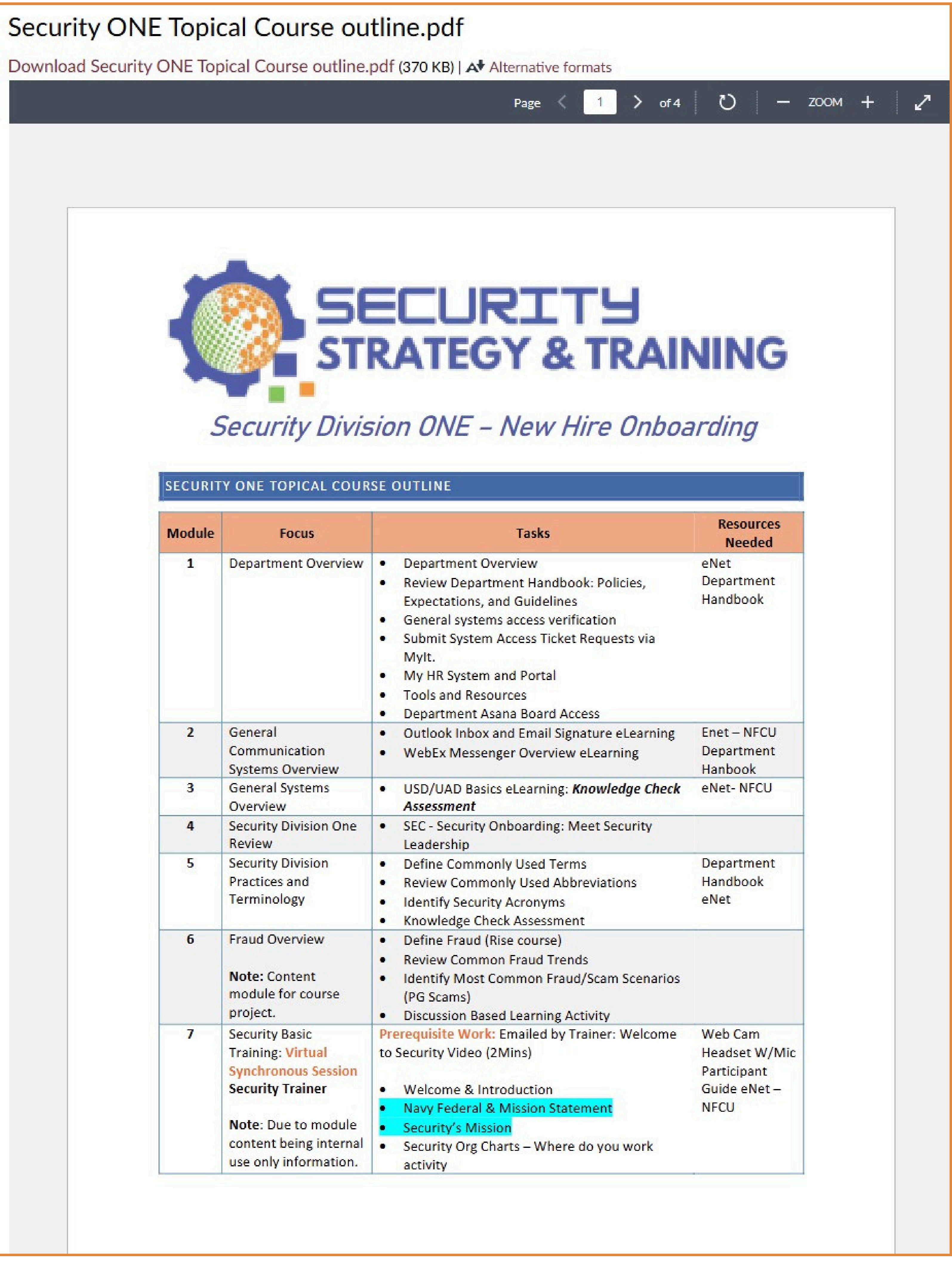
Where I'm from

Get to Know Your Peers in the Security Division! Click the + icon in the bottom right corner to add a post. Then explore other's posts to learn more about your team!

Navy Federal Credit Union, Herita...

Navy Federal Credit Union, Heritage Oaks ...

SHARE
Navy Federal
NFCU Building 7
Navy Federal Way
Residence a Creek Tow
Navy Federal Pl
Navy Federal Credit Union
Navy Federal Credit Union - ATM
Navy Federal Credit Union - GPO Building 5
Navy Federal Credit Union Recreation Center
10
Fusion Fine Wine & Spirits 4
Salt Grass Dr
Sparkleberry Ln
Map data ©2024 Google
Terms
Made with Padlet
Reply



Security ONE Topical Course outline.pdf

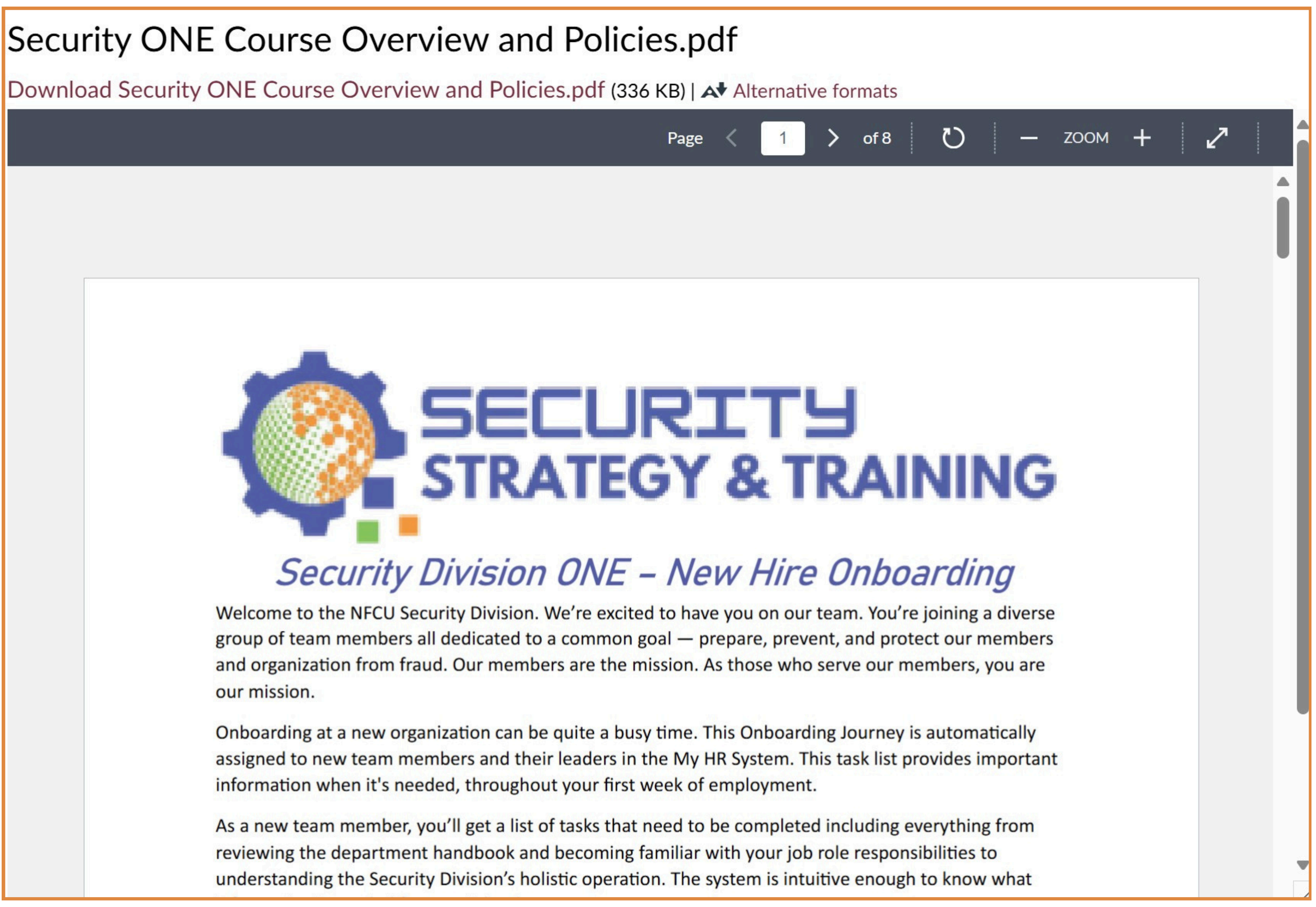
Download Security ONE Topical Course outline.pdf (370 KB) | Alternative formats

SECURITY STRATEGY & TRAINING

Security Division ONE – New Hire Onboarding

SECURITY ONE TOPICAL COURSE OUTLINE

Module	Focus	Tasks	Resources Needed
1	Department Overview	• Department Overview • Review Department Handbook: Policies, Expectations, and Guidelines • General systems access verification • Submit System Access Ticket Requests via MyIt. • My HR System and Portal • Tools and Resources • Department Asana Board Access	eNet Department Handbook
2	General Communication Systems Overview	• Outlook Inbox and Email Signature eLearning • WebEx Messenger Overview eLearning	Enet – NFCU Department Hanbook
3	General Systems Overview	• USD/UAD Basics eLearning: ***Knowledge Check Assessment***	eNet- NFCU
4	Security Division One Review	• SEC - Security Onboarding: Meet Security Leadership	
5	Security Division Practices and Terminology	• Define Commonly Used Terms • Review Commonly Used Abbreviations • Identify Security Acronyms • Knowledge Check Assessment	Department Handbook eNet
6	Fraud Overview **Note:** Content module for course project.	• Define Fraud (Rise course) • Review Common Fraud Trends • Identify Most Common Fraud/Scam Scenarios (PG Scams) • Discussion Based Learning Activity	
7	Security Basic Training: Virtual Synchronous Session **Security Trainer** **Note**: Due to module content being internal use only information.	Prerequisite Work: Emailed by Trainer: Welcome to Security Video (2Mins) • Welcome & Introduction • Navy Federal & Mission Statement • Security's Mission • Security Org Charts – Where do you work activity	Web Cam Headset W/Mic Participant Guide eNet – NFCU



Security ONE Course Overview and Policies.pdf

Download Security ONE Course Overview and Policies.pdf (336 KB) | Alternative formats

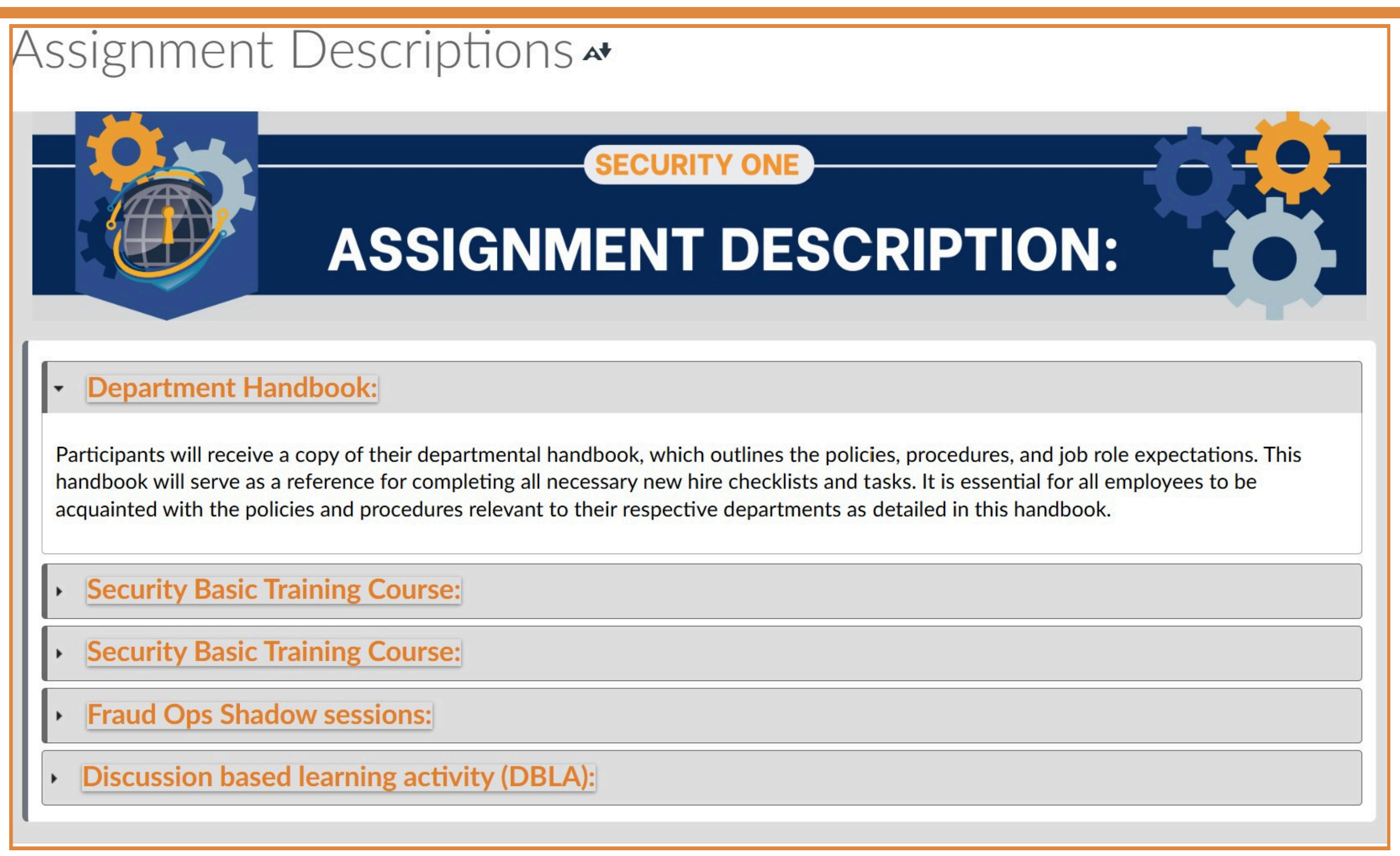
SECURITY STRATEGY & TRAINING

Security Division ONE – New Hire Onboarding

Welcome to the NFCU Security Division. We're excited to have you on our team. You're joining a diverse group of team members all dedicated to a common goal — prepare, prevent, and protect our members and organization from fraud. Our members are the mission. As those who serve our members, you are our mission.

Onboarding at a new organization can be quite a busy time. This Onboarding Journey is automatically assigned to new team members and their leaders in the My HR System. This task list provides important information when it's needed, throughout your first week of employment.

As a new team member, you'll get a list of tasks that need to be completed including everything from reviewing the department handbook and becoming familiar with your job role responsibilities to understanding the Security Division's holistic operation. The system is intuitive enough to know what



Assignment Descriptions

SECURITY ONE

ASSIGNMENT DESCRIPTION:

▾ Department Handbook:

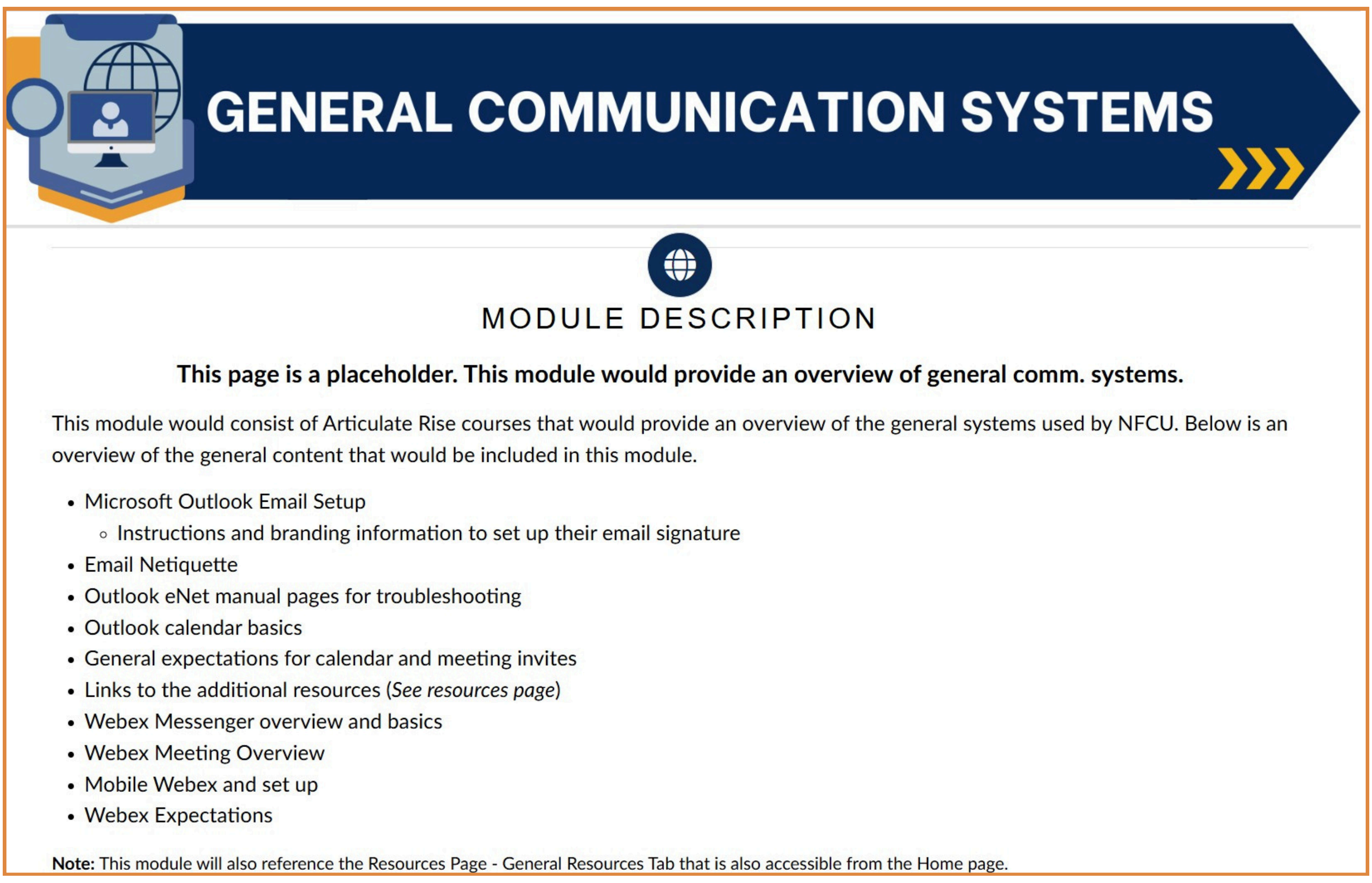
Participants will receive a copy of their departmental handbook, which outlines the policies, procedures, and job role expectations. This handbook will serve as a reference for completing all necessary new hire checklists and tasks. It is essential for all employees to be acquainted with the policies and procedures relevant to their respective departments as detailed in this handbook.

▸ Security Basic Training Course:

▸ Security Basic Training Course:

▸ Fraud Ops Shadow sessions:

▸ Discussion based learning activity (DBLA):



GENERAL COMMUNICATION SYSTEMS

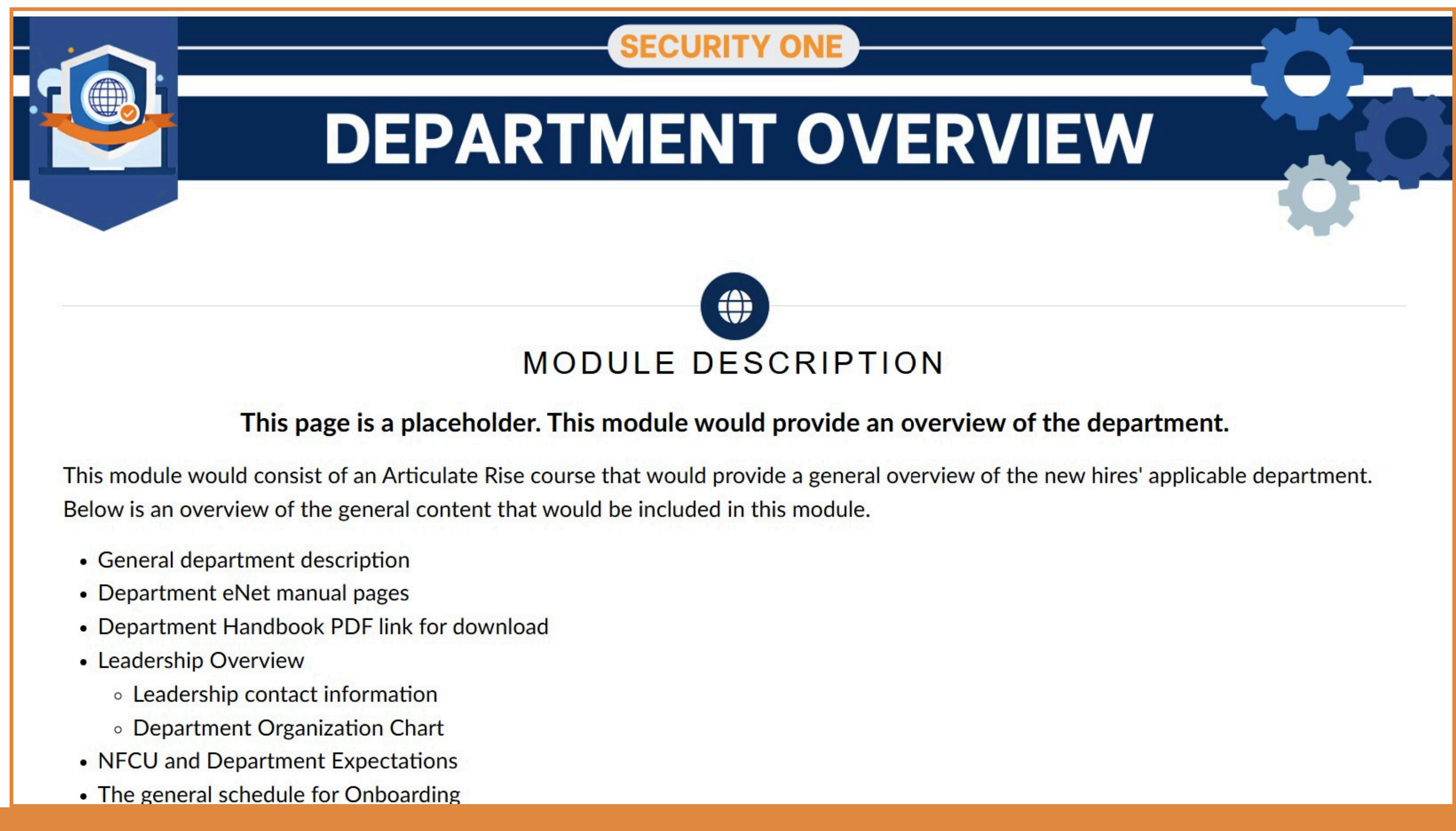
MODULE DESCRIPTION

This page is a placeholder. This module would provide an overview of general comm. systems.

This module would consist of Articulate Rise courses that would provide an overview of the general systems used by NFCU. Below is an overview of the general content that would be included in this module.

- Microsoft Outlook Email Setup
  - Instructions and branding information to set up their email signature
- Email Netiquette
- Outlook eNet manual pages for troubleshooting
- Outlook calendar basics
- General expectations for calendar and meeting invites
- Links to the additional resources (*See resources page*)
- Webex Messenger overview and basics
- Webex Meeting Overview
- Mobile Webex and set up
- Webex Expectations

Note: This module will also reference the Resources Page - General Resources Tab that is also accessible from the Home page.



SECURITY ONE

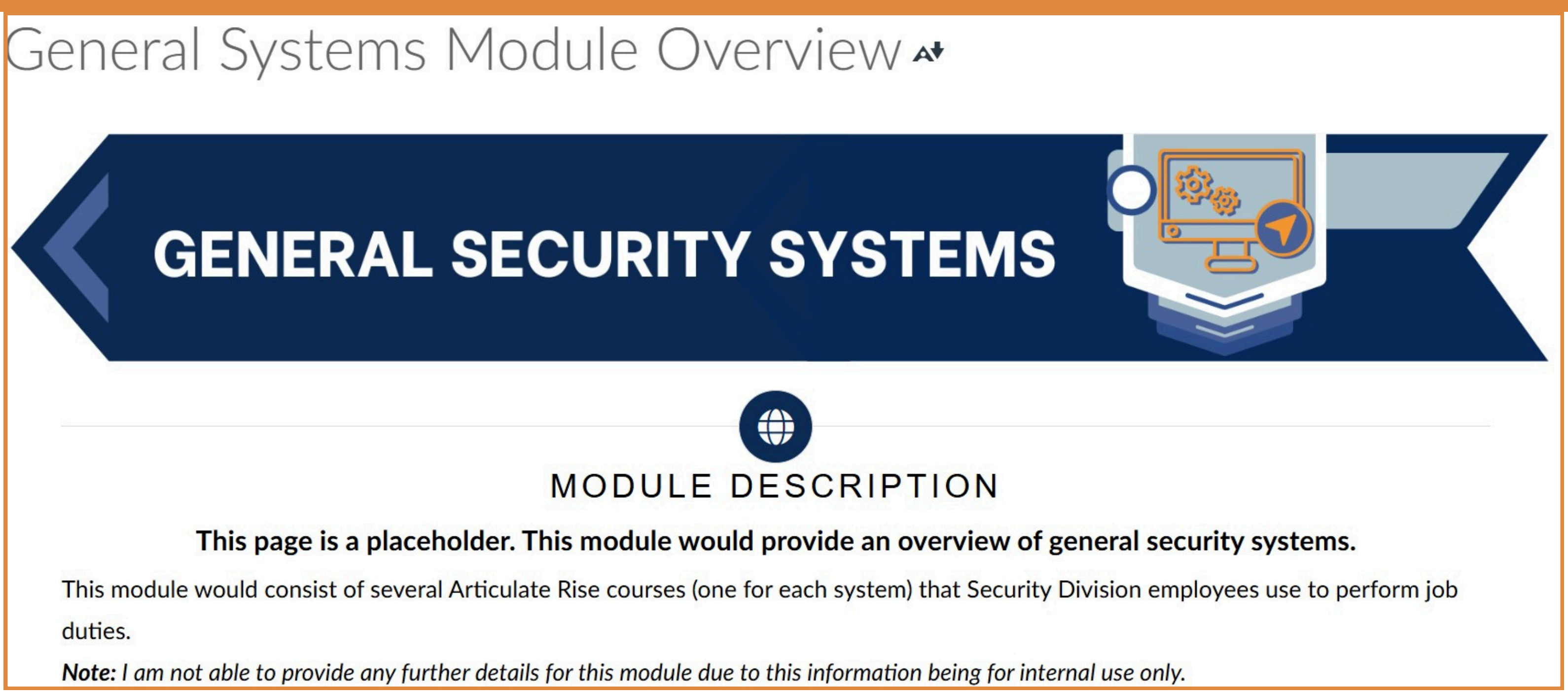
DEPARTMENT OVERVIEW

MODULE DESCRIPTION

This page is a placeholder. This module would provide an overview of the department.

This module would consist of an Articulate Rise course that would provide a general overview of the new hires' applicable department. Below is an overview of the general content that would be included in this module.

- General department description
- Department eNet manual pages
- Department Handbook PDF link for download
- Leadership Overview
  - Leadership contact information
  - Department Organization Chart
- NFCU and Department Expectations
- The general schedule for Onboarding



General Systems Module Overview

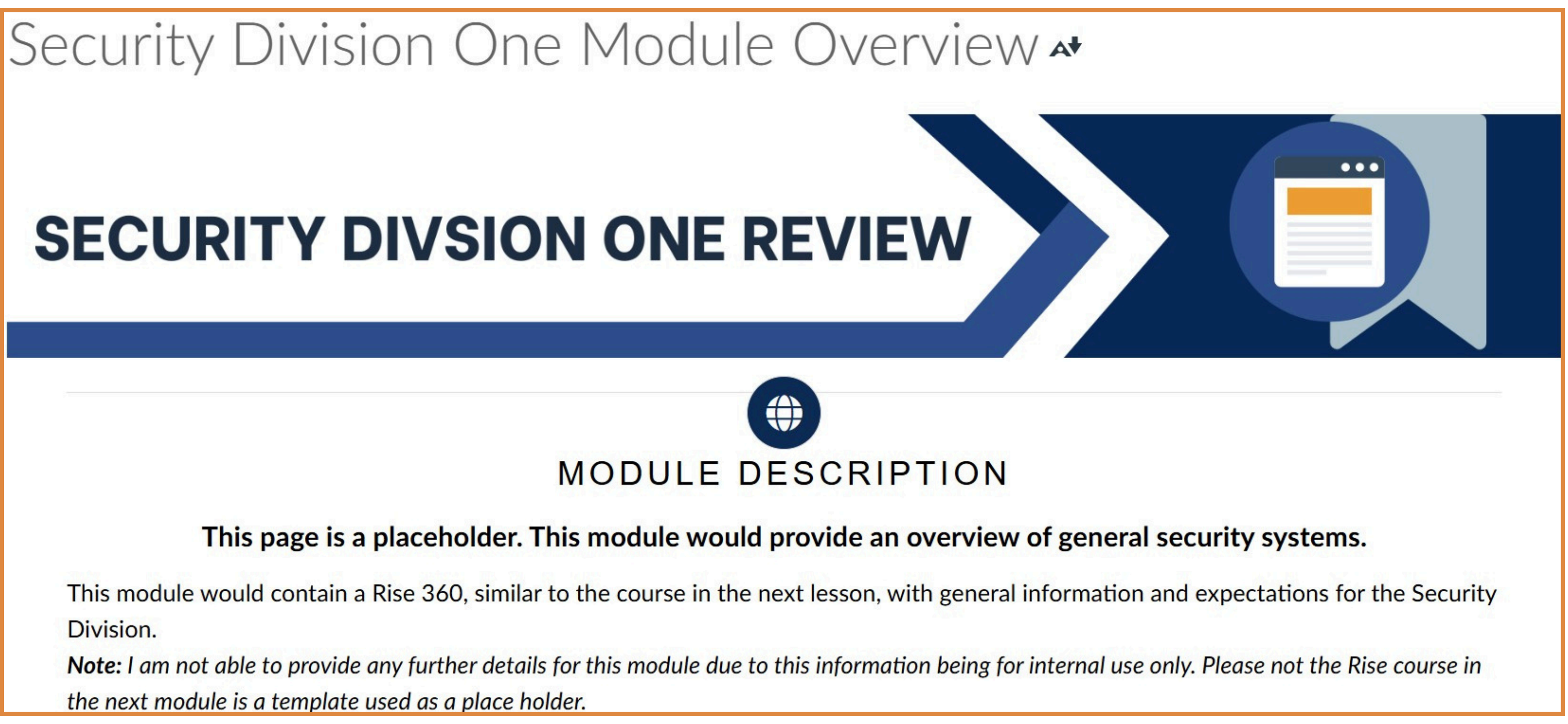
GENERAL SECURITY SYSTEMS

MODULE DESCRIPTION

This page is a placeholder. This module would provide an overview of general security systems.

This module would consist of several Articulate Rise courses (one for each system) that Security Division employees use to perform job duties.

Note: *I am not able to provide any further details for this module due to this information being for internal use only.*



Security Division One Module Overview

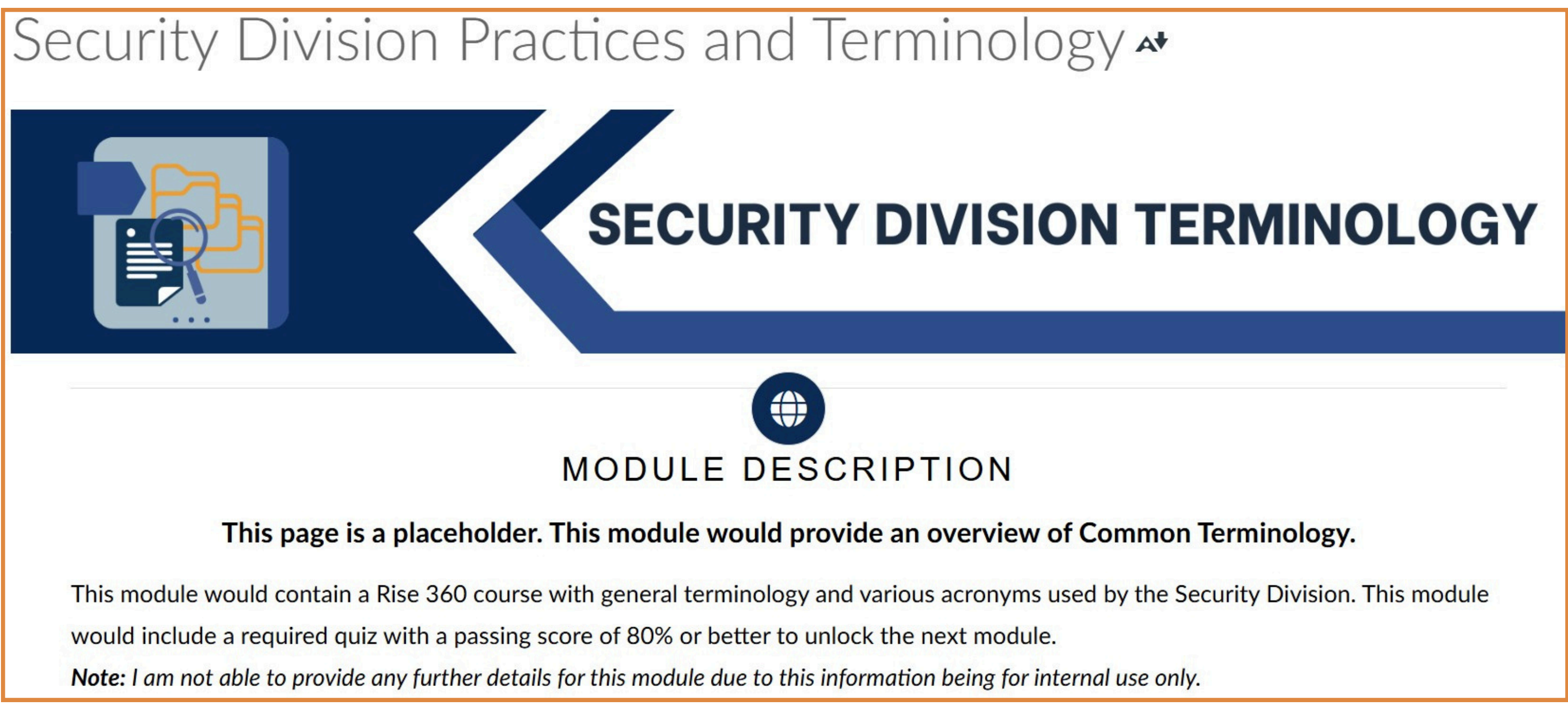
SECURITY DIVSION ONE REVIEW

MODULE DESCRIPTION

This page is a placeholder. This module would provide an overview of general security systems.

This module would contain a Rise 360, similar to the course in the next lesson, with general information and expectations for the Security Division.

Note: *I am not able to provide any further details for this module due to this information being for internal use only. Please not the Rise course in the next module is a template used as a place holder.*



Security Division Practices and Terminology

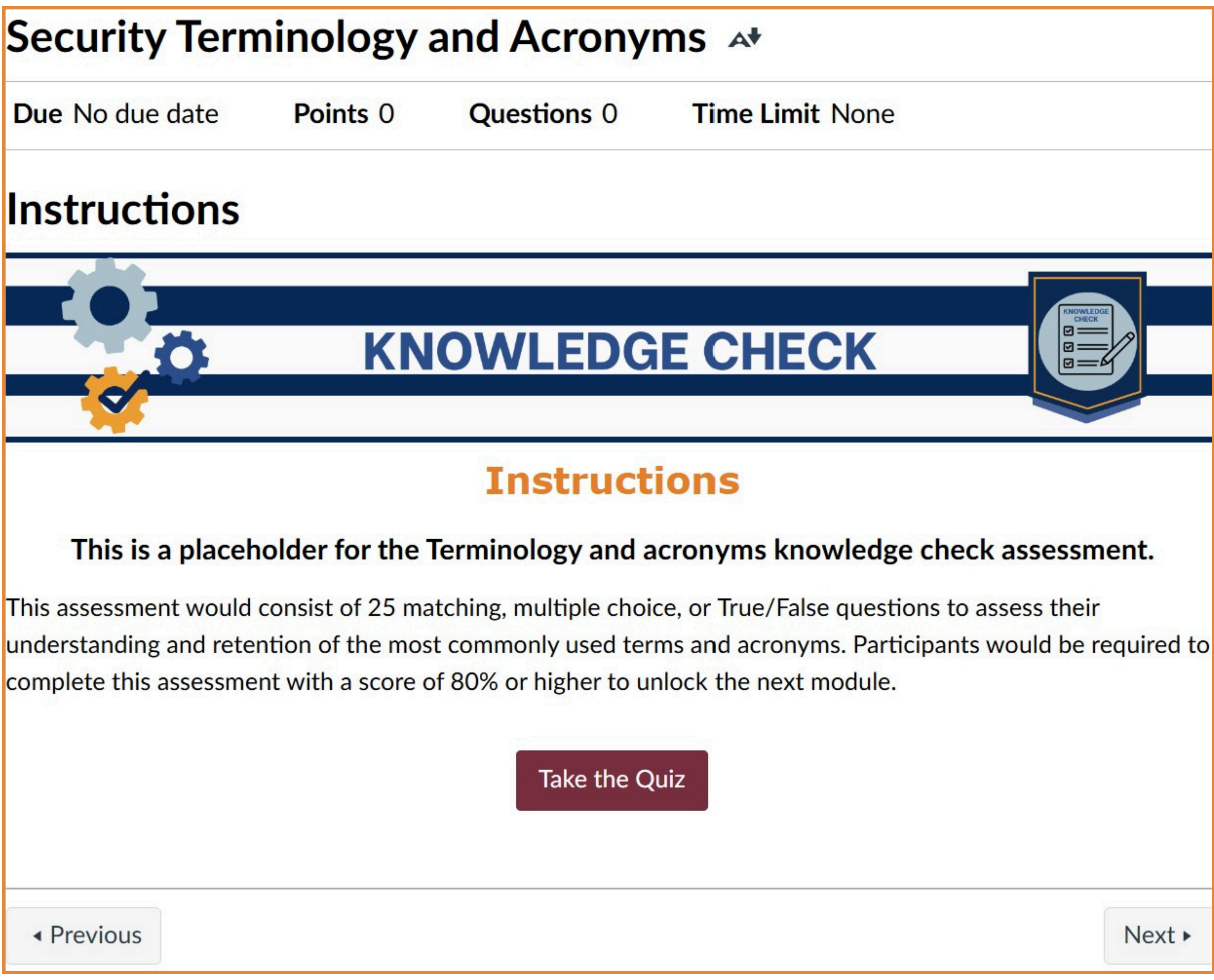
SECURITY DIVISION TERMINOLOGY

MODULE DESCRIPTION

This page is a placeholder. This module would provide an overview of Common Terminology.

This module would contain a Rise 360 course with general terminology and various acronyms used by the Security Division. This module would include a required quiz with a passing score of 80% or better to unlock the next module.

Note: *I am not able to provide any further details for this module due to this information being for internal use only.*



Security Terminology and Acronyms

Due No due date **Points** 0 **Questions** 0 **Time Limit** None

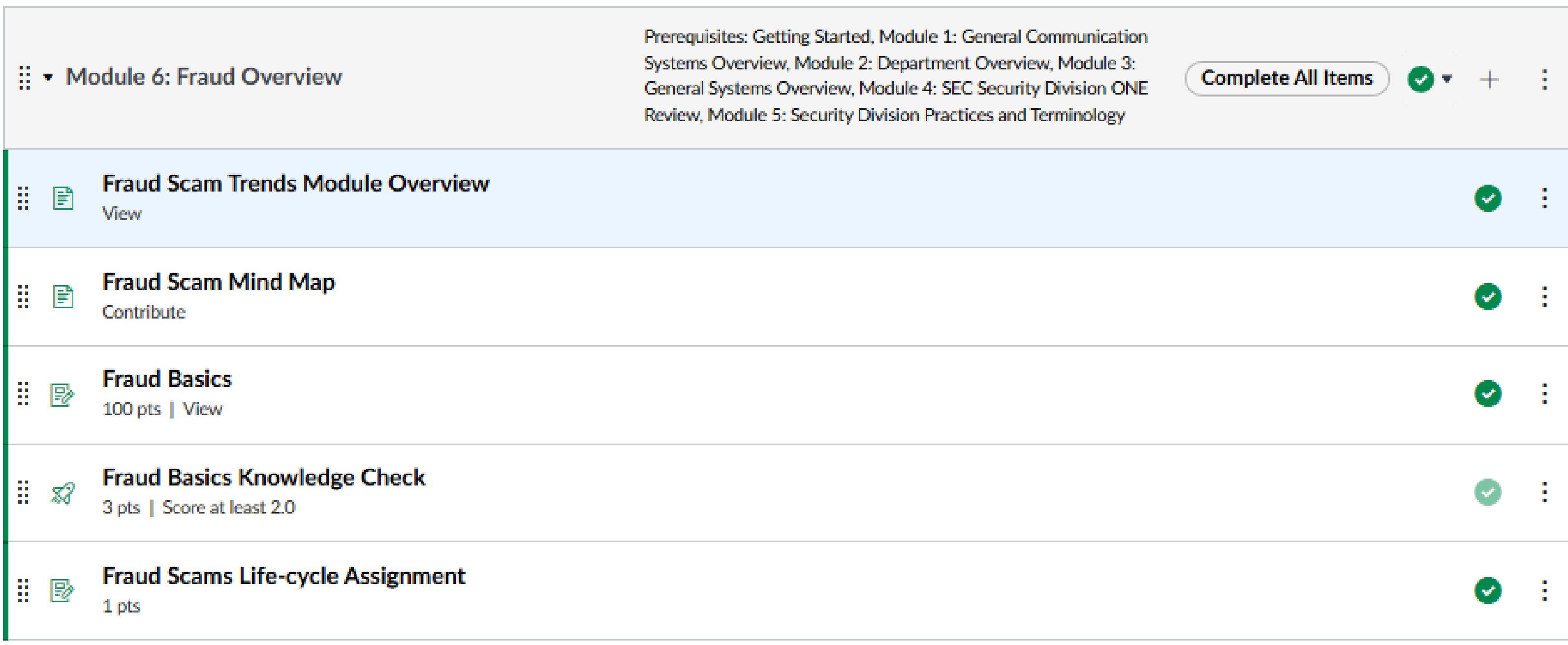
Instructions

KNOWLEDGE CHECK

Instructions

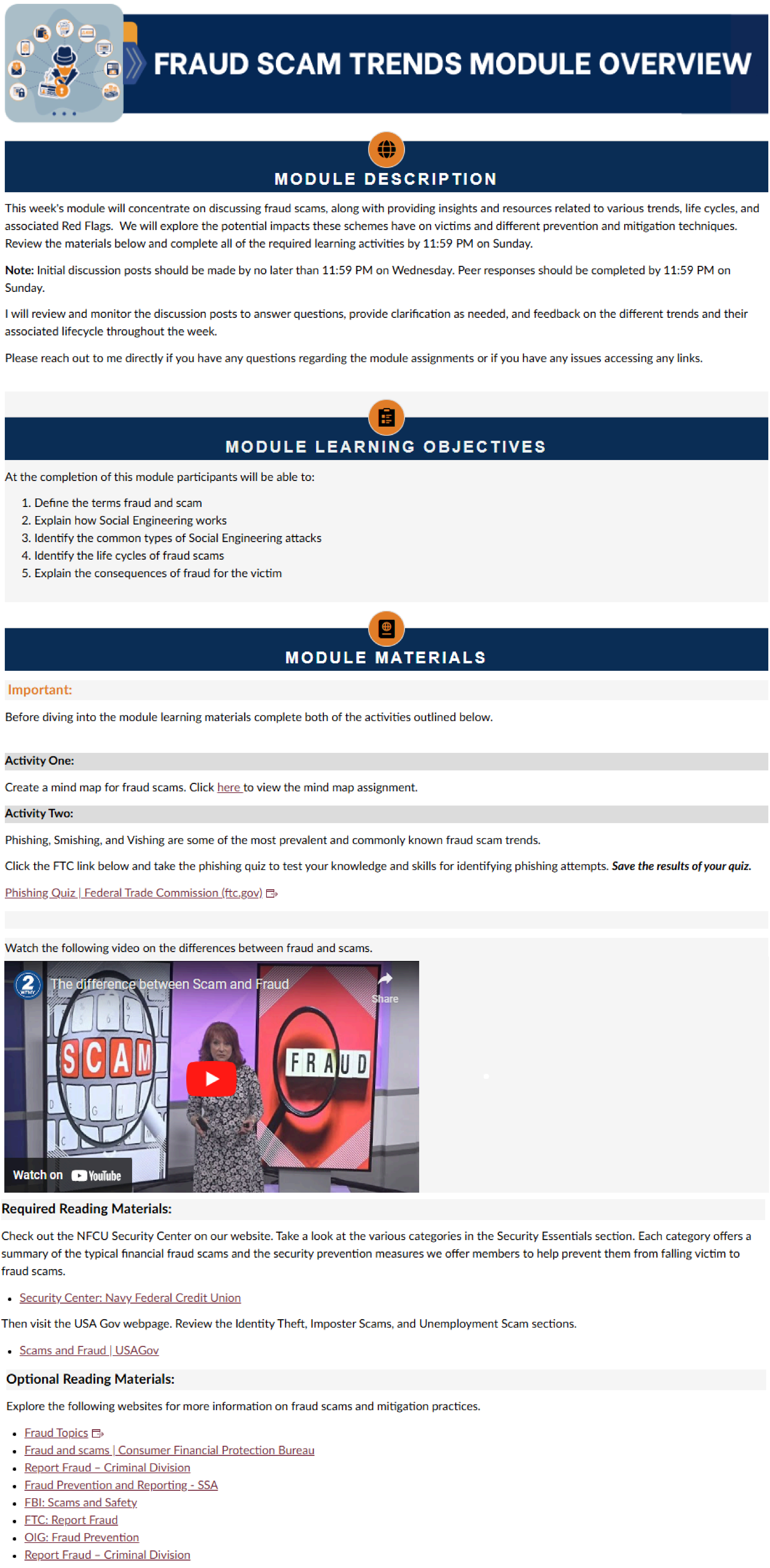
This is a placeholder for the Terminology and acronyms knowledge check assessment.

This assessment would consist of 25 matching, multiple choice, or True/False questions to assess their understanding and retention of the most commonly used terms and acronyms. Participants would be required to complete this assessment with a score of 80% or higher to unlock the next module.



Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology

Item	Details
Fraud Scam Trends Module Overview	View
Fraud Scam Mind Map	Contribute
Fraud Basics	100 pts | View
Fraud Basics Knowledge Check	3 pts | Score at least 2.0
Fraud Scams Life-cycle Assignment	1 pts



FRAUD SCAM TRENDS MODULE OVERVIEW

MODULE DESCRIPTION

This week's module will concentrate on discussing fraud scams, along with providing insights and resources related to various trends, life cycles, and associated Red Flags. We will explore the potential impacts these schemes have on victims and different prevention and mitigation techniques. Review the materials below and complete all of the required learning activities by 11:59 PM on Sunday.

Note: Initial discussion posts should be made by no later than 11:59 PM on Wednesday. Peer responses should be completed by 11:59 PM on Sunday.

I will review and monitor the discussion posts to answer questions, provide clarification as needed, and feedback on the different trends and their associated lifecycle throughout the week.

Please reach out to me directly if you have any questions regarding the module assignments or if you have any issues accessing any links.

MODULE LEARNING OBJECTIVES

At the completion of this module participants will be able to:

1. Define the terms fraud and scam
2. Explain how Social Engineering works
3. Identify the common types of Social Engineering attacks
4. Identify the life cycles of fraud scams
5. Explain the consequences of fraud for the victim

MODULE MATERIALS

Important:

Before diving into the module learning materials complete both of the activities outlined below.

Activity One:

Create a mind map for fraud scams. Click here to view the mind map assignment.

Activity Two:

Phishing, Smishing, and Vishing are some of the most prevalent and commonly known fraud scam trends.

Click the FTC link below and take the phishing quiz to test your knowledge and skills for identifying phishing attempts. ***Save the results of your quiz.***

Phishing Quiz | Federal Trade Commission (ftc.gov)

Watch the following video on the differences between fraud and scams.

Required Reading Materials:

Check out the NFCU Security Center on our website. Take a look at the various categories in the Security Essentials section. Each category offers a summary of the typical financial fraud scams and the security prevention measures we offer members to help prevent them from falling victim to fraud scams.

- Security Center: Navy Federal Credit Union

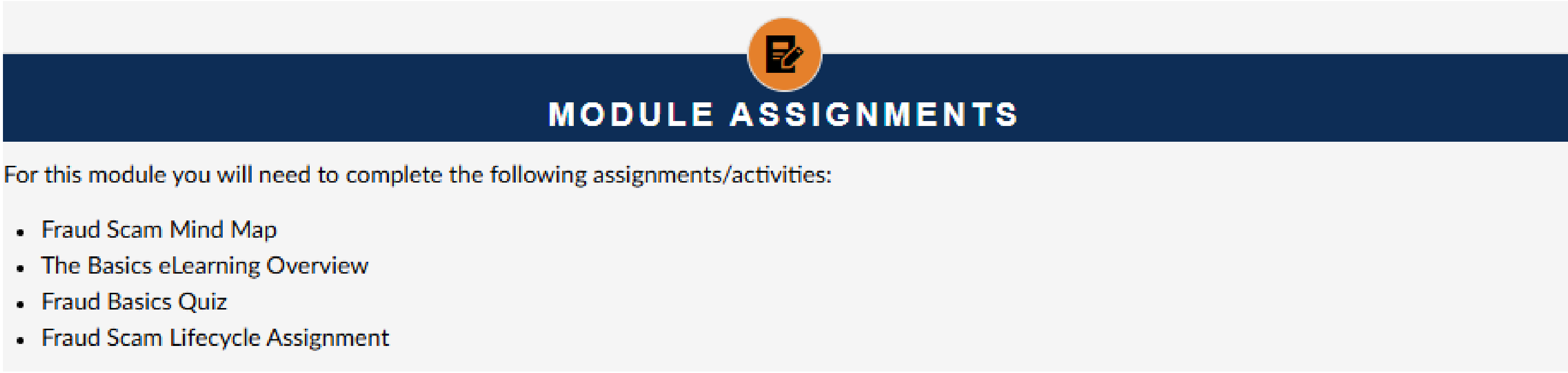
Then visit the USA Gov webpage. Review the Identity Theft, Imposter Scams, and Unemployment Scam sections.

- Scams and Fraud | USAGov

Optional Reading Materials:

Explore the following websites for more information on fraud scams and mitigation practices.

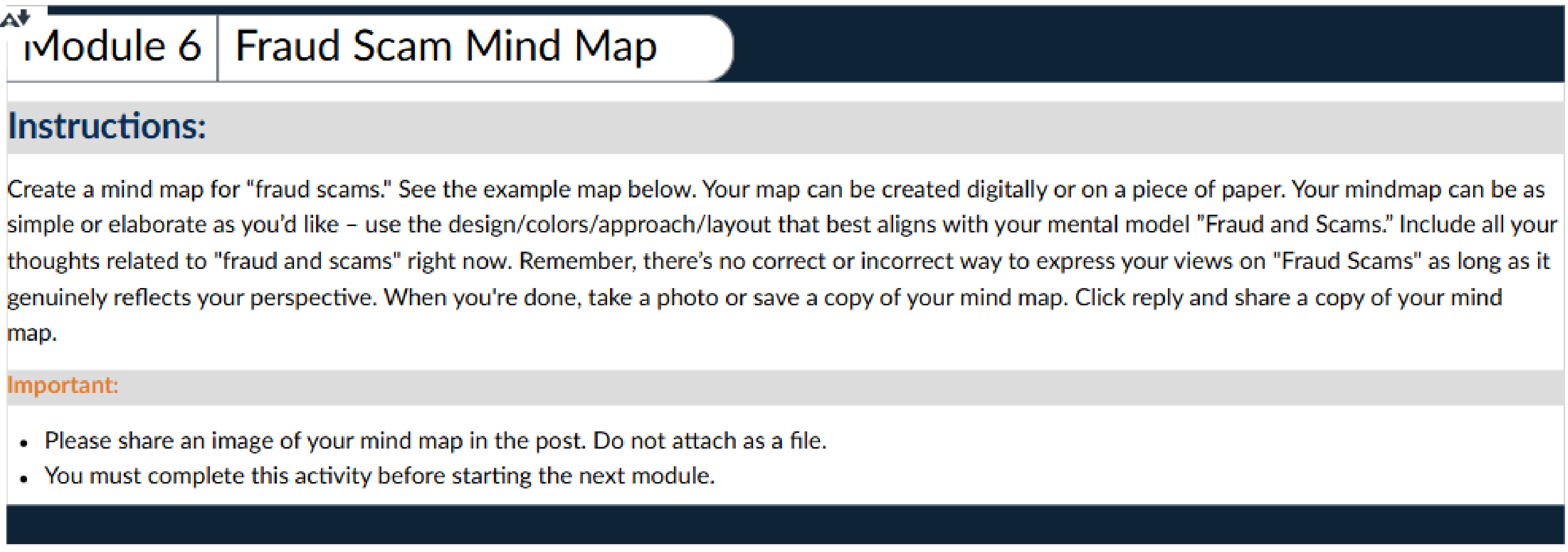
- Fraud Topics
- Fraud and scams | Consumer Financial Protection Bureau
- Report Fraud – Criminal Division
- Fraud Prevention and Reporting - SSA
- FBI: Scams and Safety
- FTC: Report Fraud
- OIG: Fraud Prevention
- Report Fraud – Criminal Division



MODULE ASSIGNMENTS

For this module you will need to complete the following assignments/activities:

- Fraud Scam Mind Map
- The Basics eLearning Overview
- Fraud Basics Quiz
- Fraud Scam Lifecycle Assignment



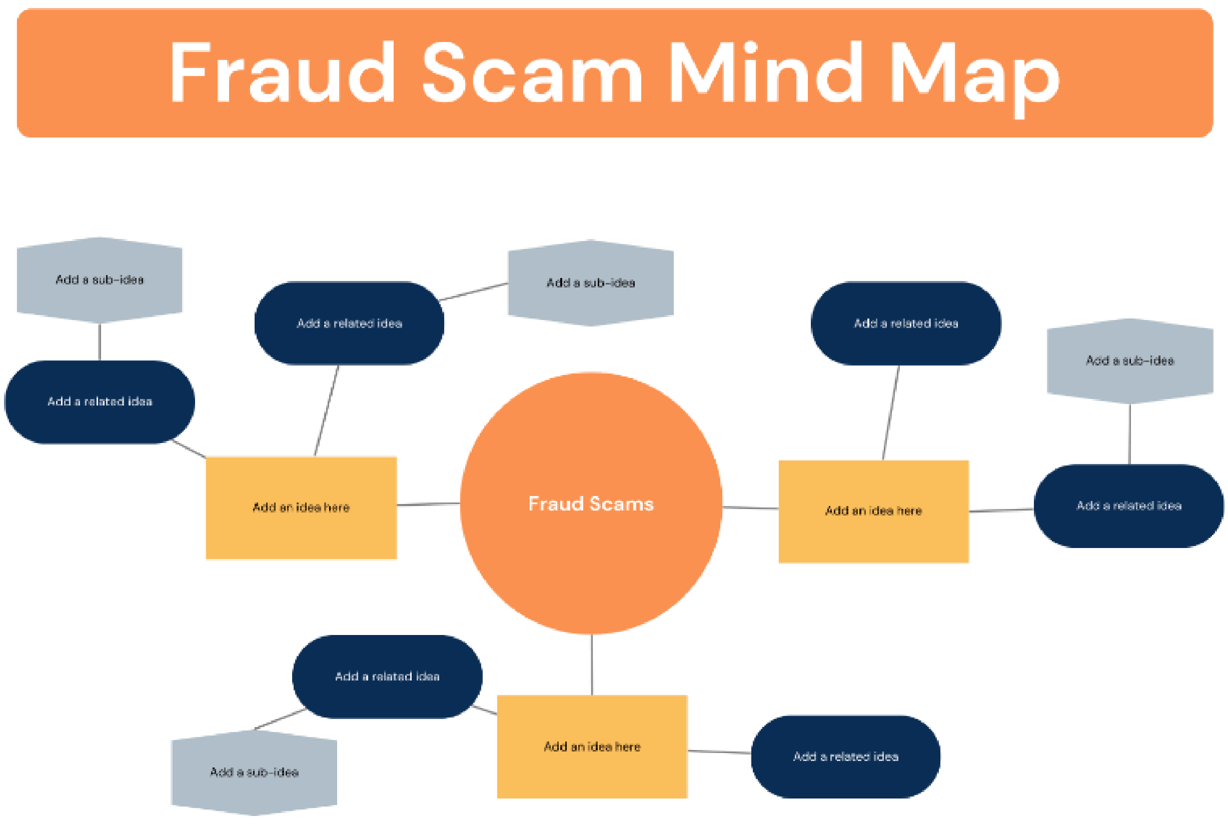
Module 6 | Fraud Scam Mind Map

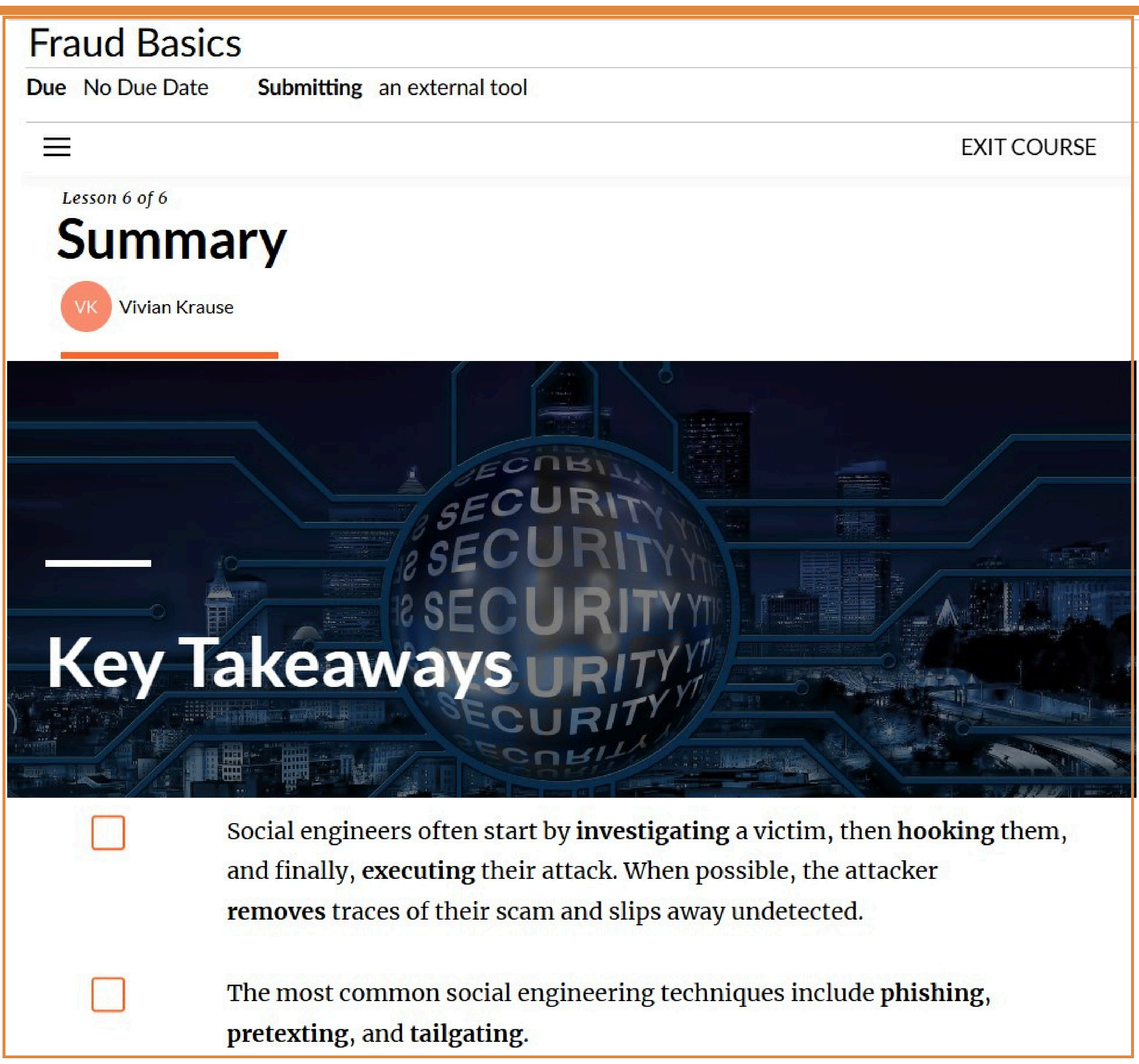
Instructions:

Create a mind map for "fraud scams." See the example map below. Your map can be created digitally or on a piece of paper. Your mindmap can be as simple or elaborate as you'd like – use the design/colors/approach/layout that best aligns with your mental model "Fraud and Scams." Include all your thoughts related to "fraud and scams" right now. Remember, there's no correct or incorrect way to express your views on "Fraud Scams" as long as it genuinely reflects your perspective. When you're done, take a photo or save a copy of your mind map. Click reply and share a copy of your mind map.

Important:

- Please share an image of your mind map in the post. Do not attach as a file.
- You must complete this activity before starting the next module.





Fraud Basics

Due No Due Date **Submitting** an external tool

Lesson 6 of 6

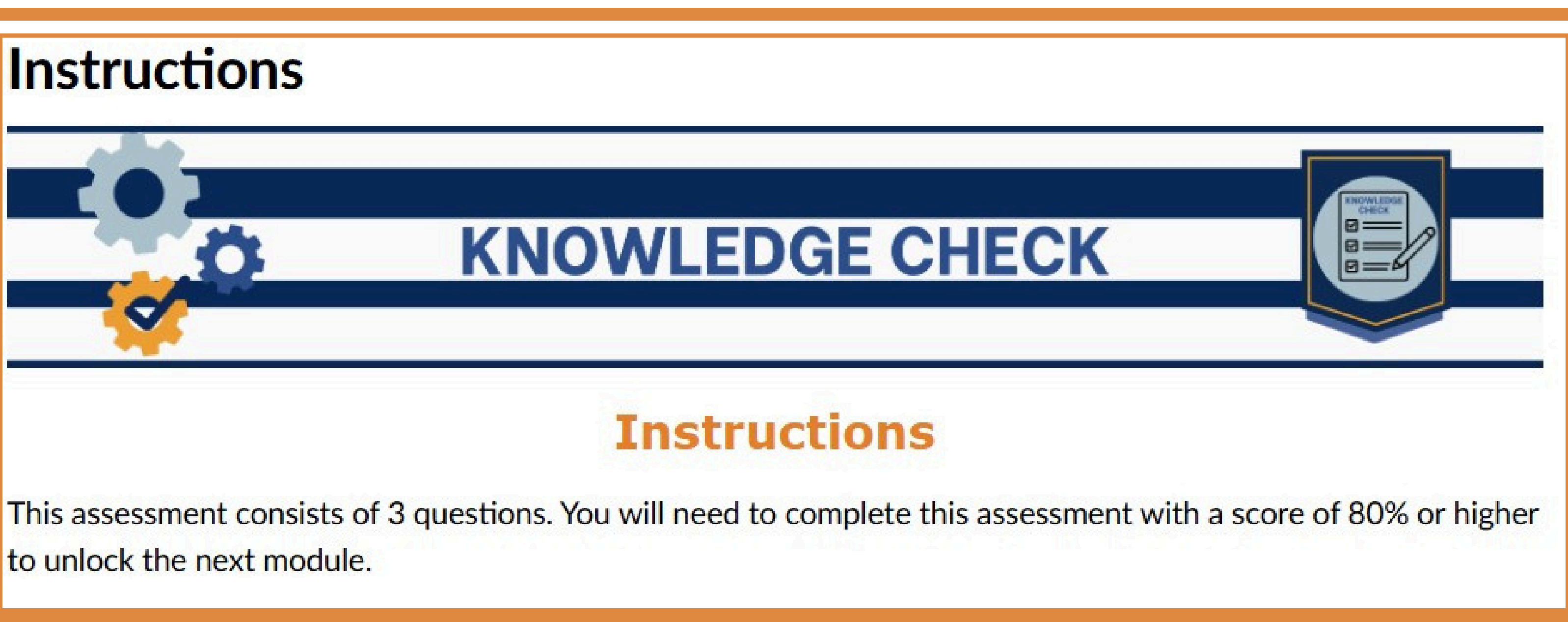
Summary

VK Vivian Krause

Key Takeaways

□ Social engineers often start by **investigating** a victim, then **hooking** them, and finally, **executing** their attack. When possible, the attacker **removes** traces of their scam and slips away undetected.

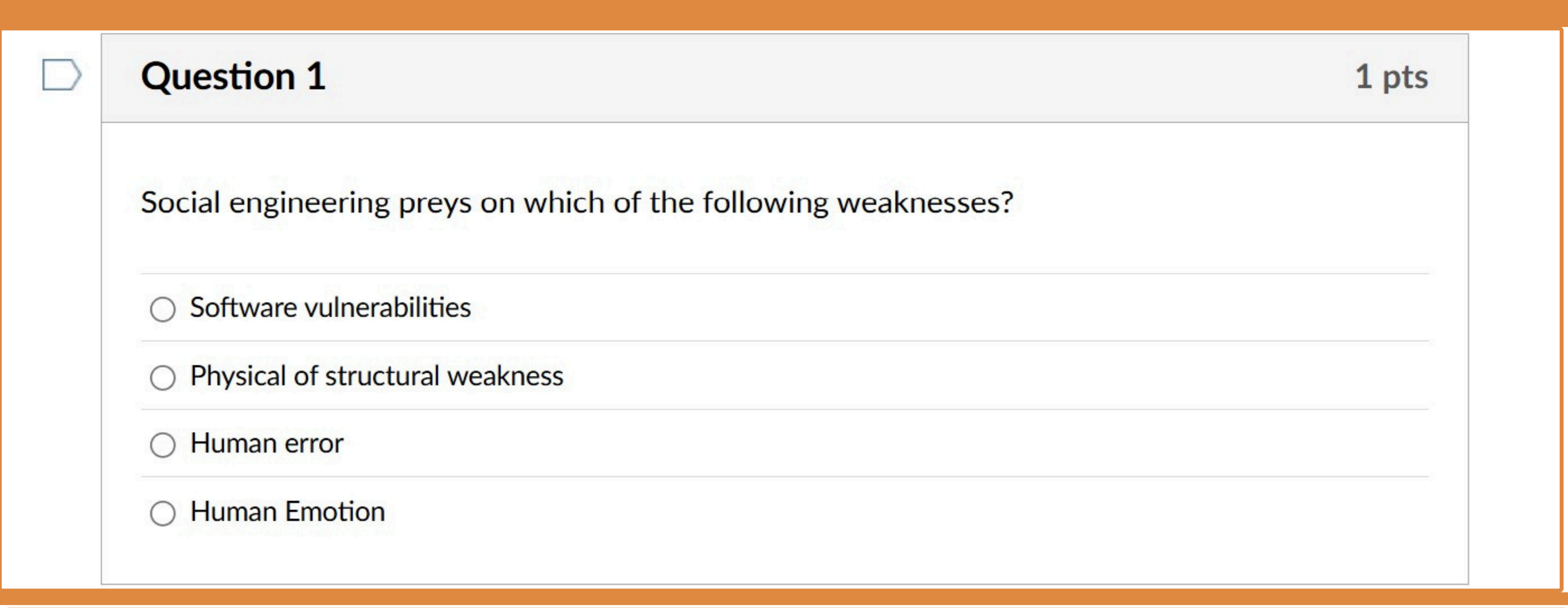
□ The most common social engineering techniques include **phishing**, **pretexting**, and **tailgating**.



Instructions

Instructions

This assessment consists of 3 questions. You will need to complete this assessment with a score of 80% or higher to unlock the next module.



Question 1 1 pts

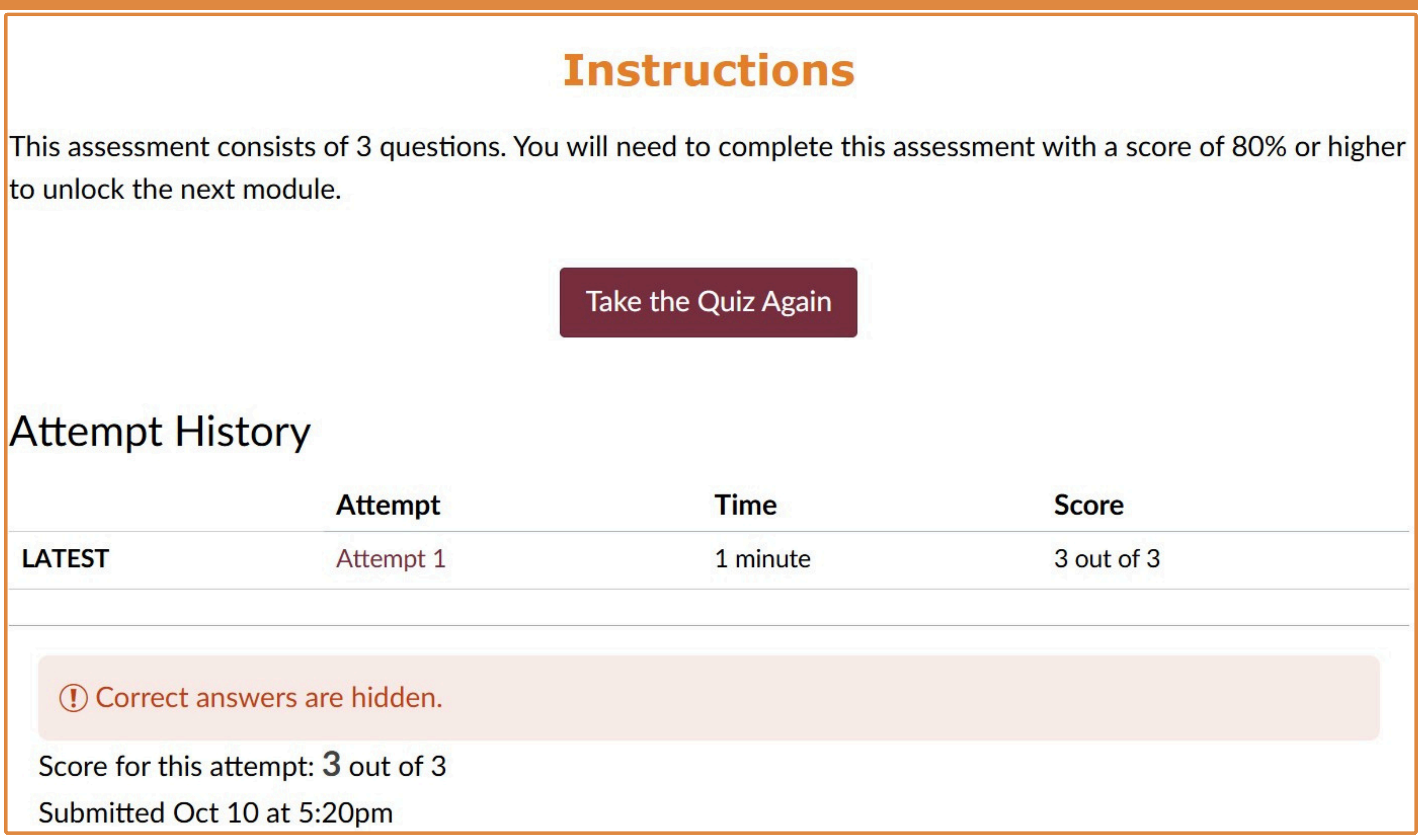
Social engineering preys on which of the following weaknesses?

○ Software vulnerabilities

○ Physical of structural weakness

○ Human error

○ Human Emotion



Instructions

This assessment consists of 3 questions. You will need to complete this assessment with a score of 80% or higher to unlock the next module.

Take the Quiz Again

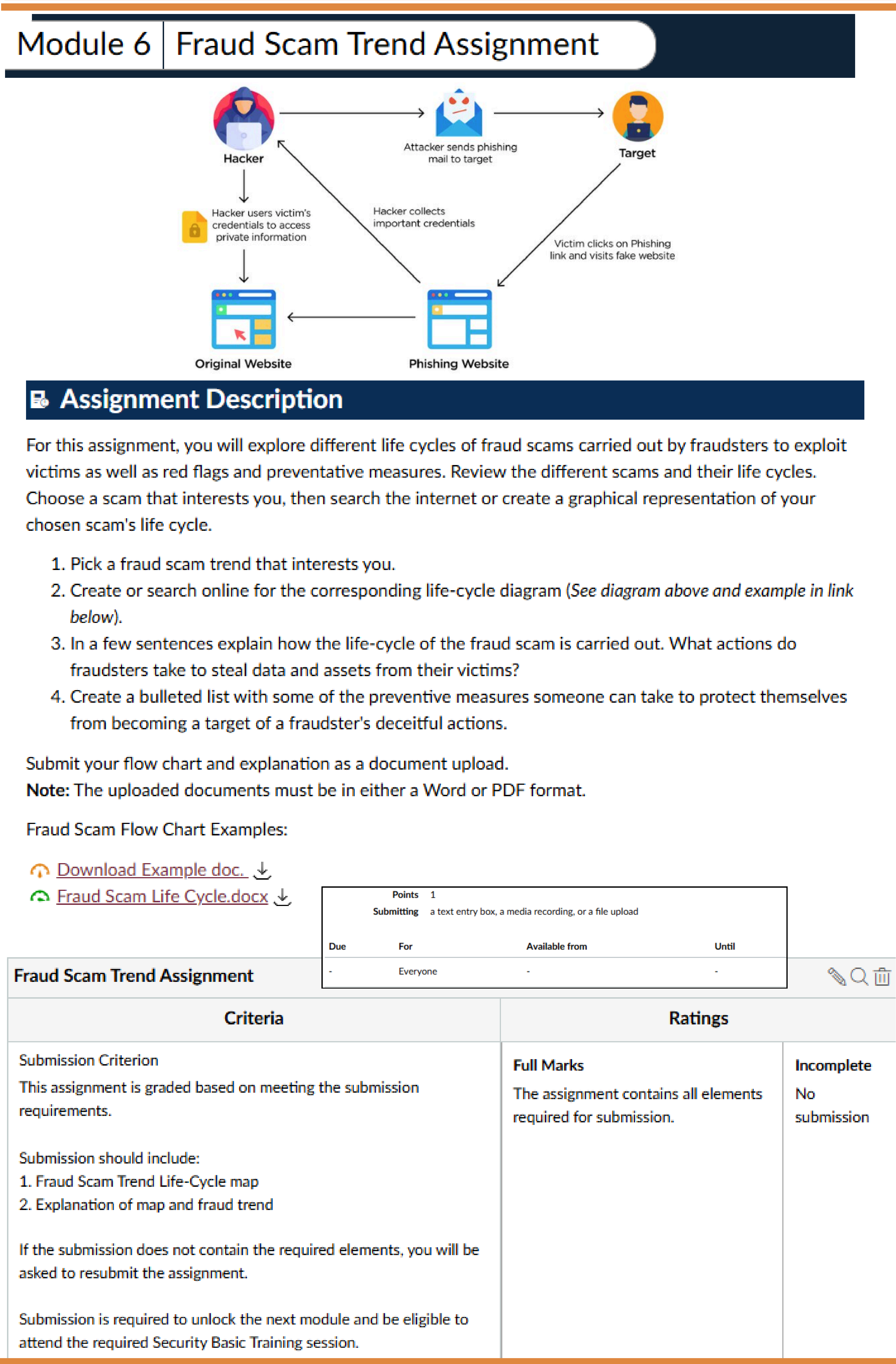
Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	1 minute	3 out of 3

Correct answers are hidden.

Score for this attempt: 3 out of 3

Submitted Oct 10 at 5:20pm



Module 6 Fraud Scam Trend Assignment

Hacker
Attacker sends phishing mail to target
Target
Hacker users victim's credentials to access private information
Hacker collects important credentials
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

Assignment Description

For this assignment, you will explore different life cycles of fraud scams carried out by fraudsters to exploit victims as well as red flags and preventative measures. Review the different scams and their life cycles. Choose a scam that interests you, then search the internet or create a graphical representation of your chosen scam's life cycle.

1. Pick a fraud scam trend that interests you.
2. Create or search online for the corresponding life-cycle diagram (*See diagram above and example in link below*).
3. In a few sentences explain how the life-cycle of the fraud scam is carried out. What actions do fraudsters take to steal data and assets from their victims?
4. Create a bulleted list with some of the preventive measures someone can take to protect themselves from becoming a target of a fraudster's deceitful actions.

Submit your flow chart and explanation as a document upload.
Note: The uploaded documents must be in either a Word or PDF format.

Fraud Scam Flow Chart Examples:

Download Example doc.

Fraud Scam Life Cycle.docx

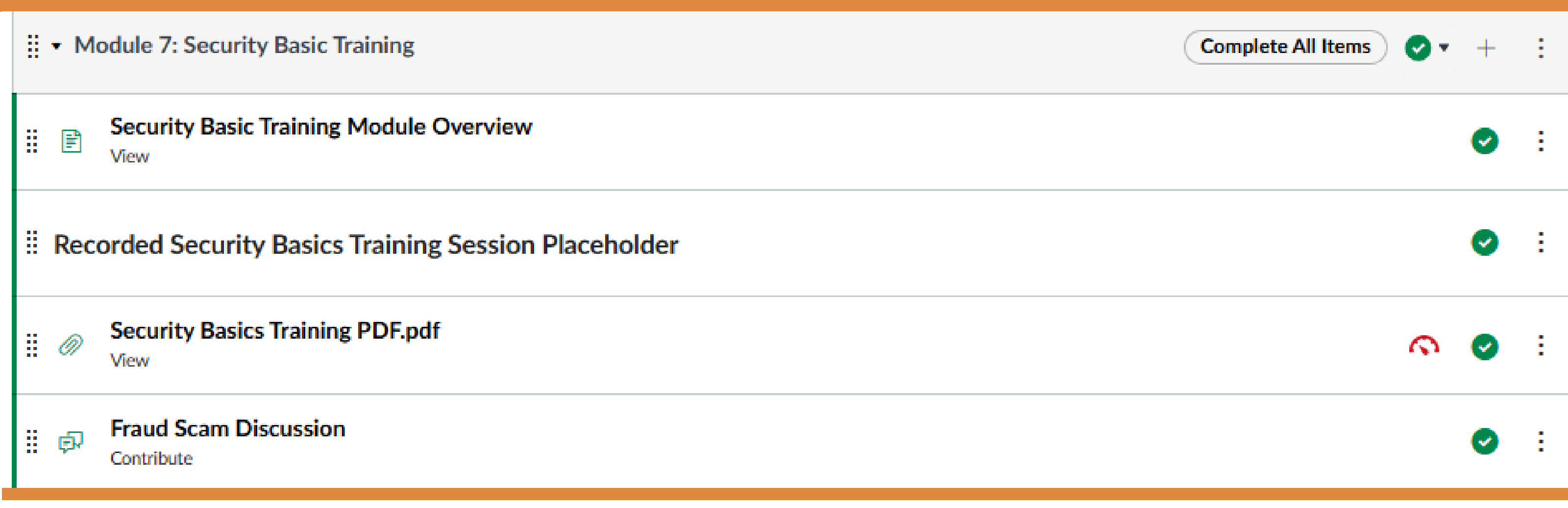
Points 1

Submitting a text entry box, a media recording, or a file upload

Due	For	Available from	Until
-	Everyone	-	-

Fraud Scam Trend Assignment

Criteria	Ratings	
Submission Criterion This assignment is graded based on meeting the submission requirements. Submission should include: 1. Fraud Scam Trend Life-Cycle map 2. Explanation of map and fraud trend If the submission does not contain the required elements, you will be asked to resubmit the assignment. Submission is required to unlock the next module and be eligible to attend the required Security Basic Training session.	**Full Marks** The assignment contains all elements required for submission.	**Incomplete** No submission

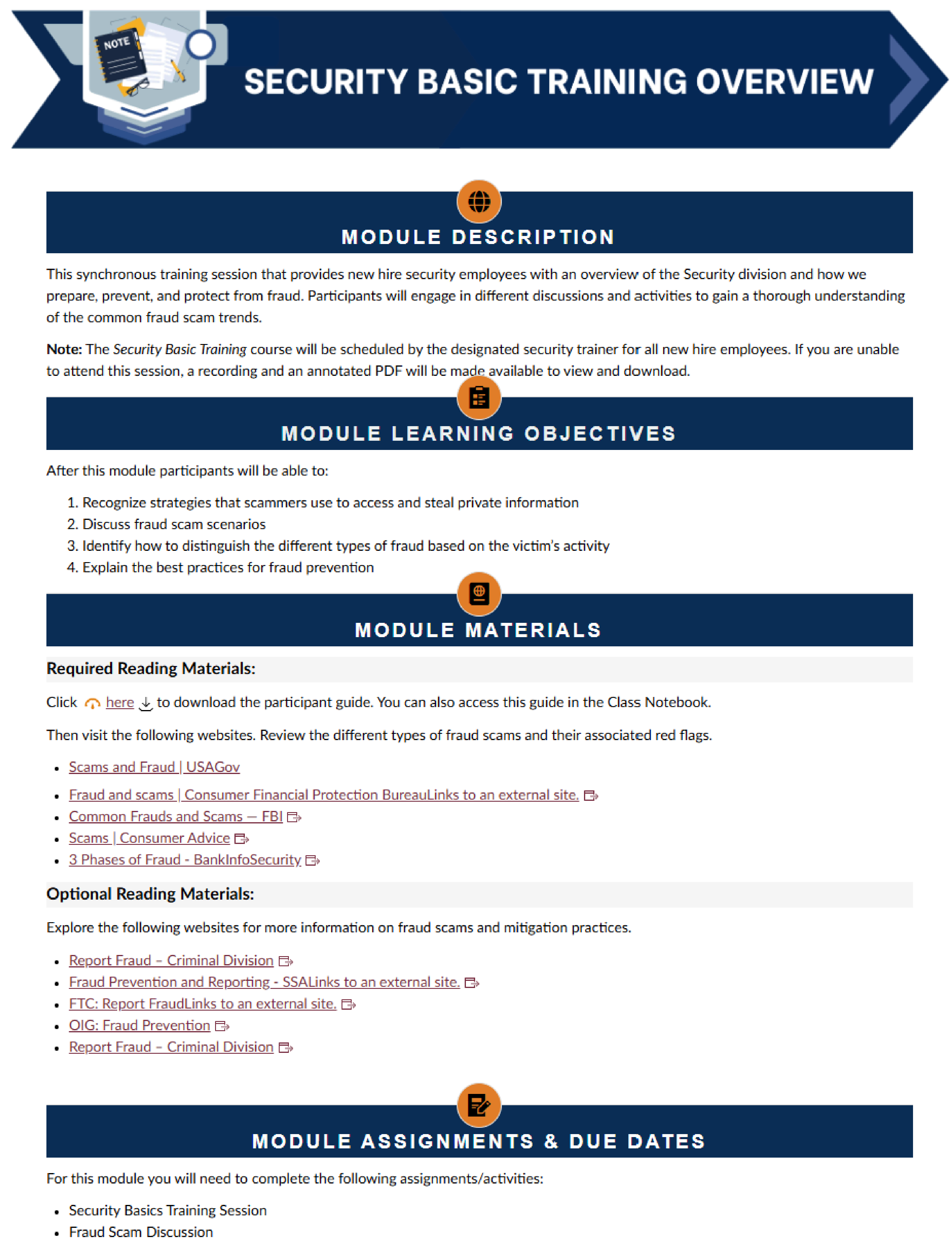

Module 7: Security Basic Training

Security Basic Training Module Overview
View

Recorded Security Basics Training Session Placeholder

Security Basics Training PDF.pdf
View

Fraud Scam Discussion
Contribute


SECURITY BASIC TRAINING OVERVIEW

MODULE DESCRIPTION

This synchronous training session that provides new hire security employees with an overview of the Security division and how we prepare, prevent, and protect from fraud. Participants will engage in different discussions and activities to gain a thorough understanding of the common fraud scam trends.

Note: The *Security Basic Training* course will be scheduled by the designated security trainer for all new hire employees. If you are unable to attend this session, a recording and an annotated PDF will be made available to view and download.

MODULE LEARNING OBJECTIVES

After this module participants will be able to:

1. Recognize strategies that scammers use to access and steal private information
2. Discuss fraud scam scenarios
3. Identify how to distinguish the different types of fraud based on the victim's activity
4. Explain the best practices for fraud prevention

MODULE MATERIALS

Required Reading Materials:

Click here to download the participant guide. You can also access this guide in the Class Notebook.

Then visit the following websites. Review the different types of fraud scams and their associated red flags.

- Scams and Fraud | USAGov
- Fraud and scams | Consumer Financial Protection BureauLinks to an external site.
- Common Frauds and Scams — FBI
- Scams | Consumer Advice
- 3 Phases of Fraud - BankInfoSecurity

Optional Reading Materials:

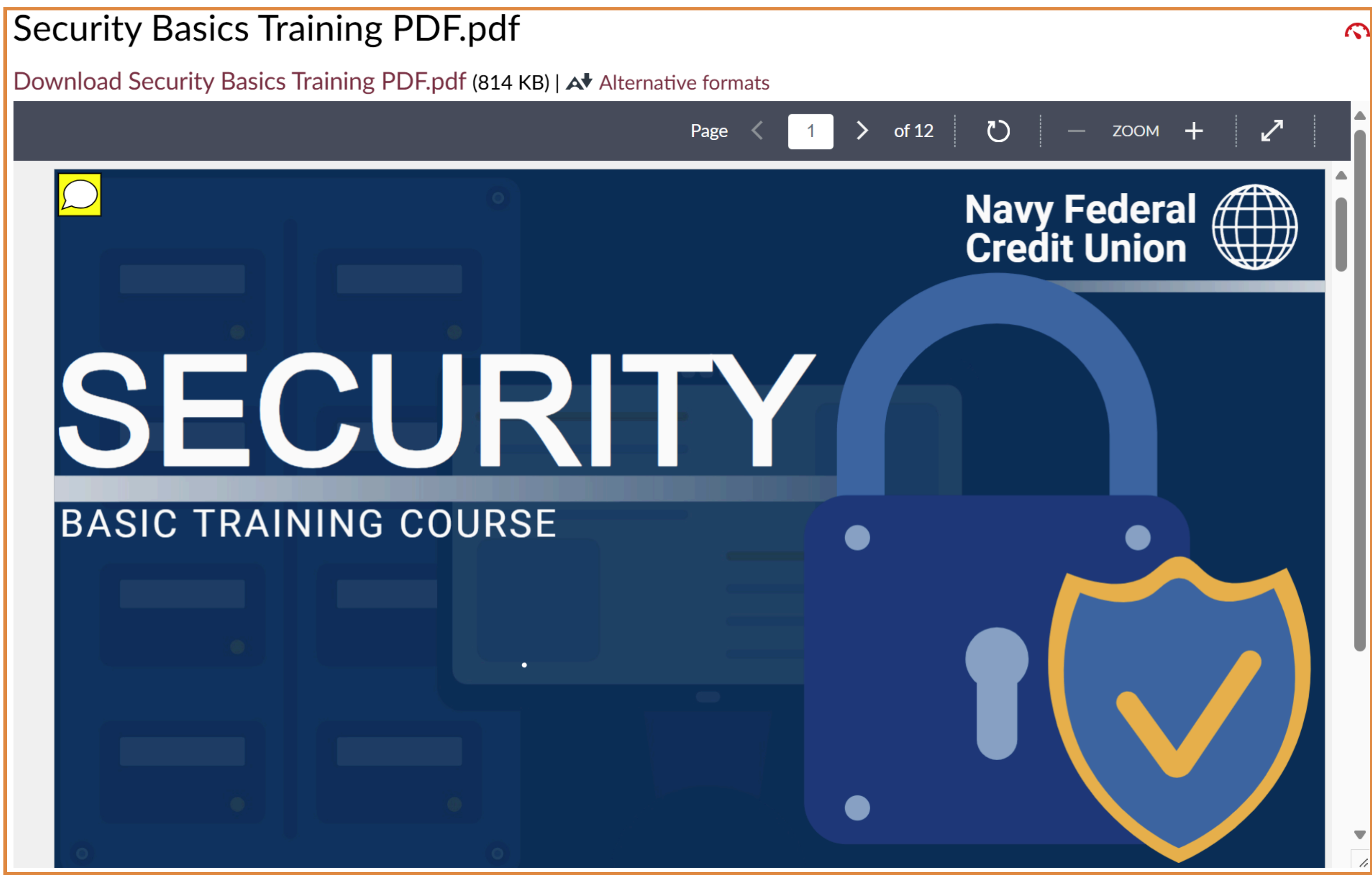
Explore the following websites for more information on fraud scams and mitigation practices.

- Report Fraud – Criminal Division
- Fraud Prevention and Reporting - SSALinks to an external site.
- FTC: Report FraudLinks to an external site.
- OIG: Fraud Prevention
- Report Fraud – Criminal Division

MODULE ASSIGNMENTS & DUE DATES

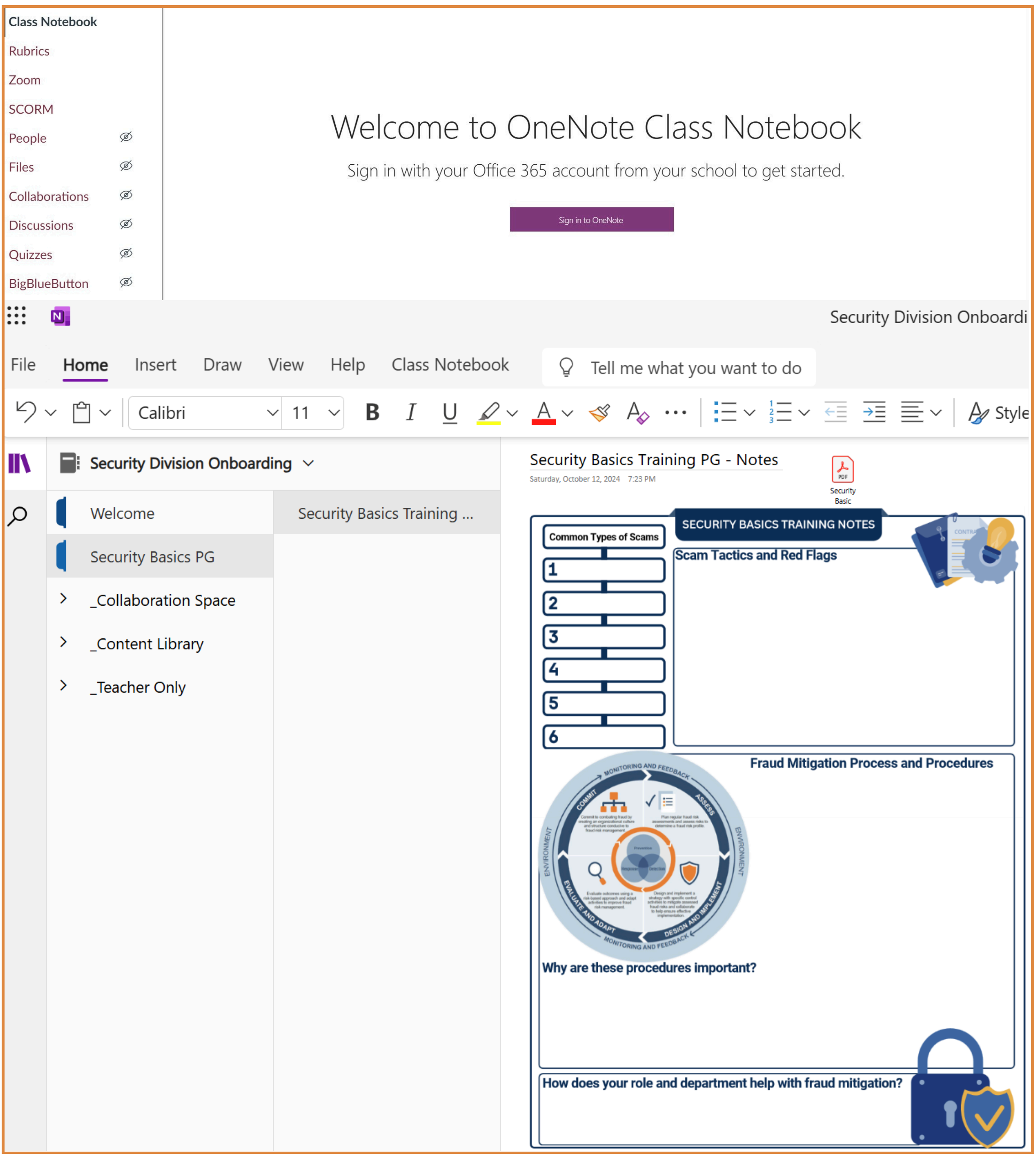
For this module you will need to complete the following assignments/activities:

- Security Basics Training Session
- Fraud Scam Discussion


Security Basics Training PDF.pdf

Download Security Basics Training PDF.pdf (814 KB) | Alternative formats

Click here to review the annotated PowerPoint presentation.
Click here to review the Lesson Plan.
Click here to review the design reflection.
Click here to review the synchronous lesson guided notes worksheet.



Welcome to OneNote Class Notebook

Sign in with your Office 365 account from your school to get started.

Security Basics Training PG - Notes

Saturday, October 12, 2024 7:23 PM

SECURITY BASICS TRAINING NOTES

Common Types of Scams

1

2

3

4

5

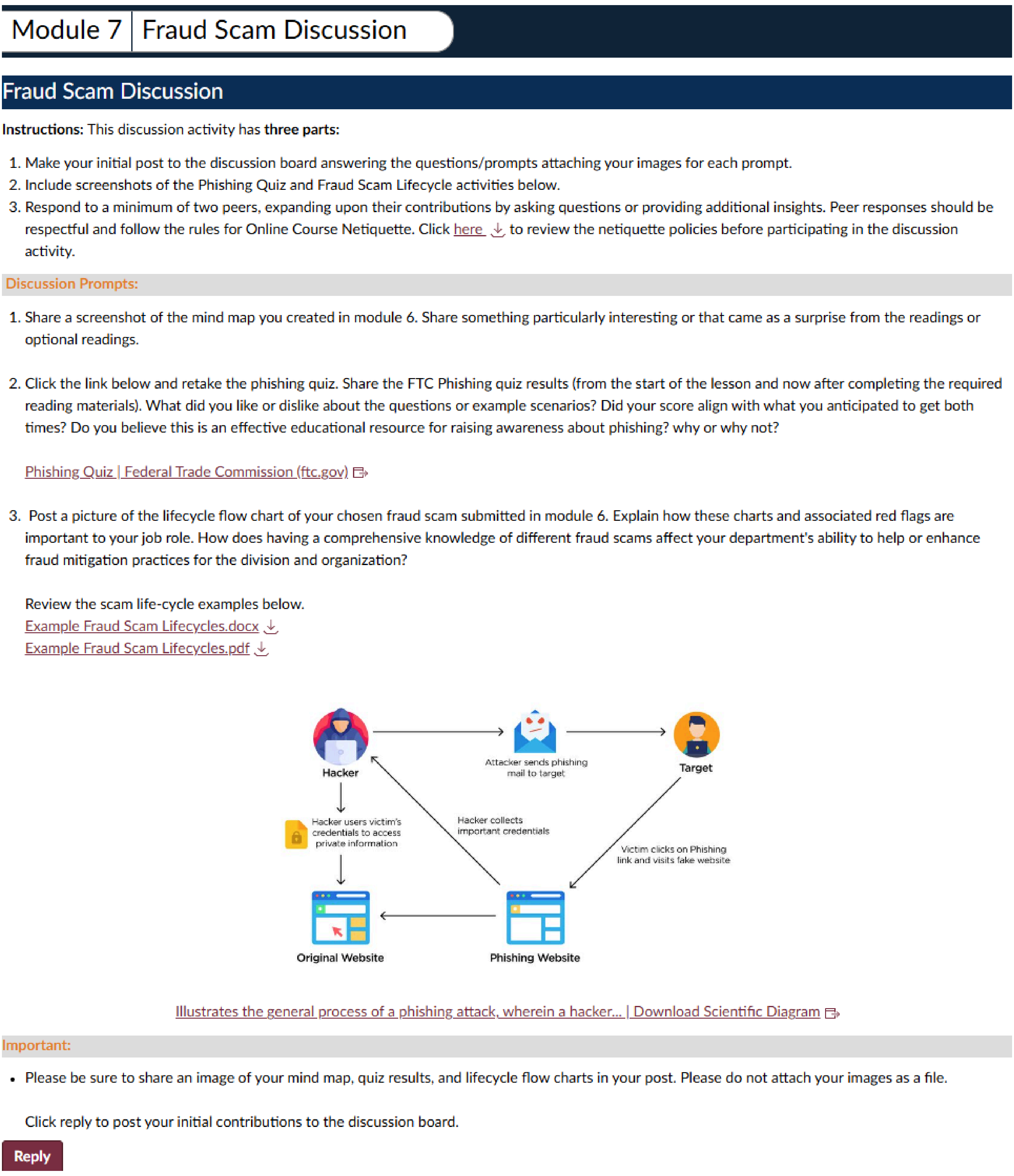
6

Scam Tactics and Red Flags

Fraud Mitigation Process and Procedures

Why are these procedures important?

How does your role and department help with fraud mitigation?



Module 7 | Fraud Scam Discussion

Fraud Scam Discussion

Instructions: This discussion activity has **three parts:**

1. Make your initial post to the discussion board answering the questions/prompts attaching your images for each prompt.
2. Include screenshots of the Phishing Quiz and Fraud Scam Lifecycle activities below.
3. Respond to a minimum of two peers, expanding upon their contributions by asking questions or providing additional insights. Peer responses should be respectful and follow the rules for Online Course Netiquette. Click here to review the netiquette policies before participating in the discussion activity.

Discussion Prompts:

1. Share a screenshot of the mind map you created in module 6. Share something particularly interesting or that came as a surprise from the readings or optional readings.

2. Click the link below and retake the phishing quiz. Share the FTC Phishing quiz results (from the start of the lesson and now after completing the required reading materials). What did you like or dislike about the questions or example scenarios? Did your score align with what you anticipated to get both times? Do you believe this is an effective educational resource for raising awareness about phishing? why or why not?

   Phishing Quiz | Federal Trade Commission (ftc.gov)

3. Post a picture of the lifecycle flow chart of your chosen fraud scam submitted in module 6. Explain how these charts and associated red flags are important to your job role. How does having a comprehensive knowledge of different fraud scams affect your department's ability to help or enhance fraud mitigation practices for the division and organization?

   Review the scam life-cycle examples below.
   Example Fraud Scam Lifecycles.docx
   Example Fraud Scam Lifecycles.pdf

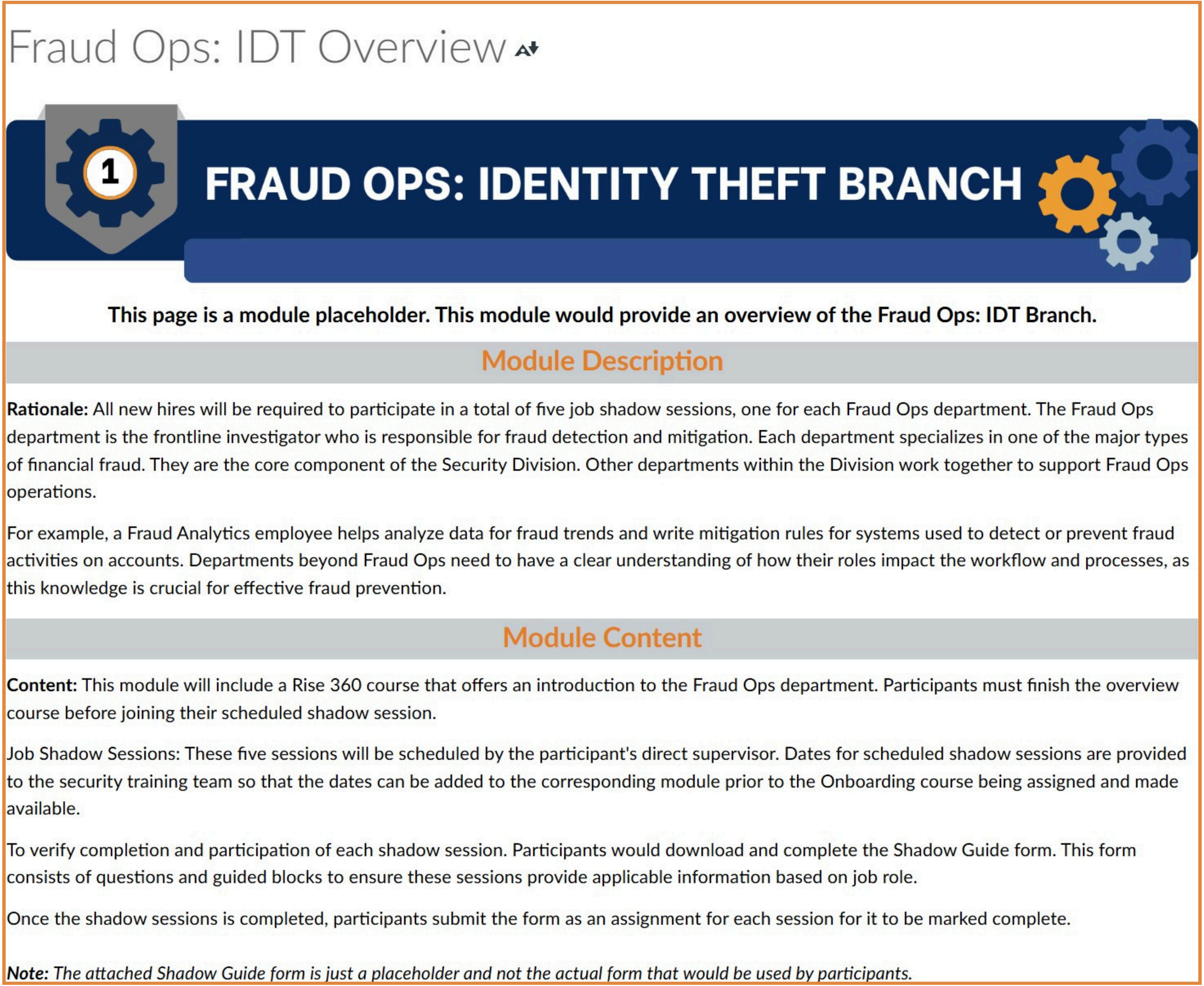
Hacker
Attacker sends phishing mail to target
Target
Hacker users victim's credentials to access private information
Hacker collects important credentials
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

Illustrates the general process of a phishing attack, wherein a hacker... | Download Scientific Diagram

Important:

- Please be sure to share an image of your mind map, quiz results, and lifecycle flow charts in your post. Please do not attach your images as a file.

Click reply to post your initial contributions to the discussion board.



Fraud Ops: IDT Overview

1

FRAUD OPS: IDENTITY THEFT BRANCH

This page is a module placeholder. This module would provide an overview of the Fraud Ops: IDT Branch.

Module Description

Rationale: All new hires will be required to participate in a total of five job shadow sessions, one for each Fraud Ops department. The Fraud Ops department is the frontline investigator who is responsible for fraud detection and mitigation. Each department specializes in one of the major types of financial fraud. They are the core component of the Security Division. Other departments within the Division work together to support Fraud Ops operations.

For example, a Fraud Analytics employee helps analyze data for fraud trends and write mitigation rules for systems used to detect or prevent fraud activities on accounts. Departments beyond Fraud Ops need to have a clear understanding of how their roles impact the workflow and processes, as this knowledge is crucial for effective fraud prevention.

Module Content

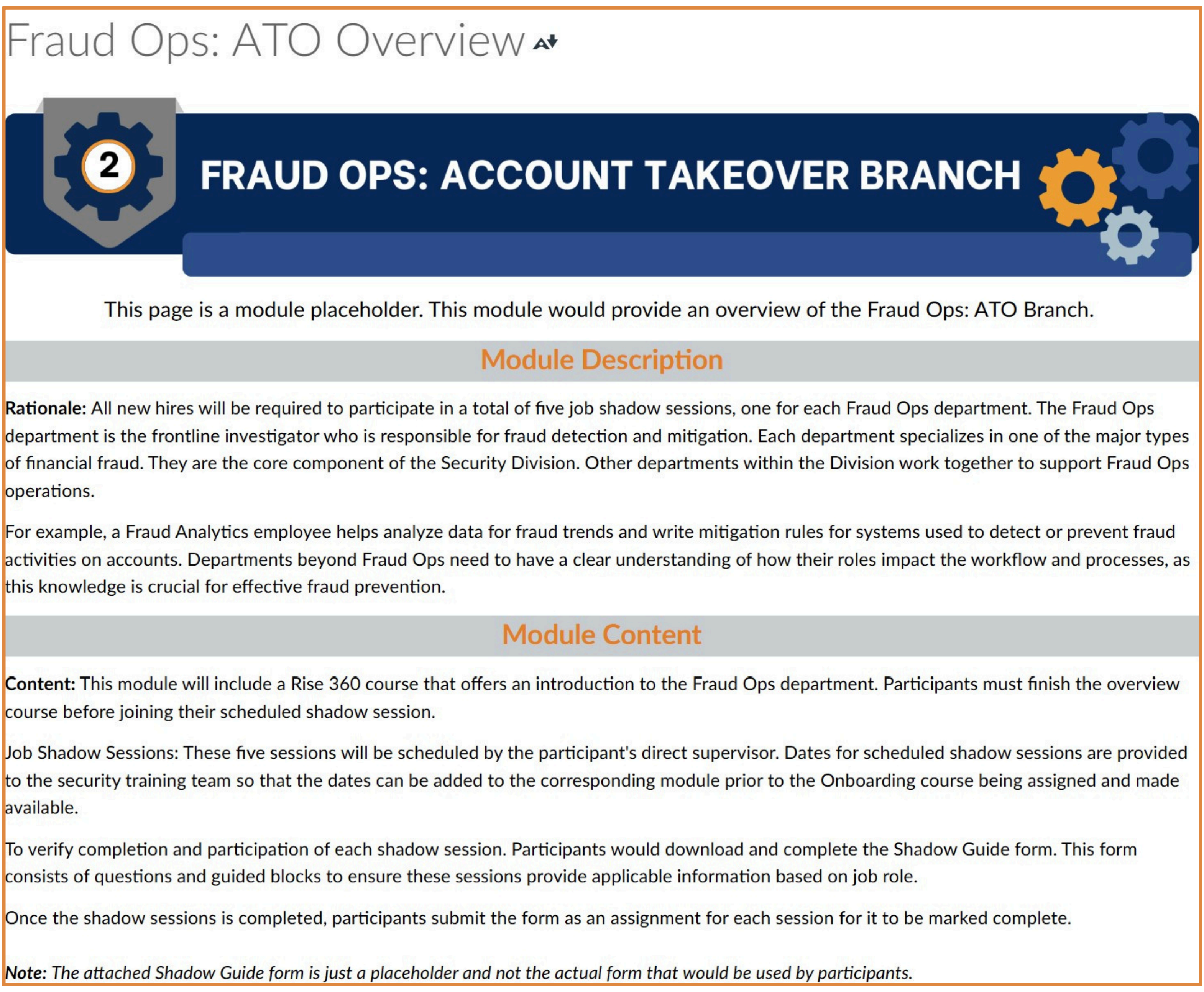
Content: This module will include a Rise 360 course that offers an introduction to the Fraud Ops department. Participants must finish the overview course before joining their scheduled shadow session.

Job Shadow Sessions: These five sessions will be scheduled by the participant's direct supervisor. Dates for scheduled shadow sessions are provided to the security training team so that the dates can be added to the corresponding module prior to the Onboarding course being assigned and made available.

To verify completion and participation of each shadow session. Participants would download and complete the Shadow Guide form. This form consists of questions and guided blocks to ensure these sessions provide applicable information based on job role.

Once the shadow sessions is completed, participants submit the form as an assignment for each session for it to be marked complete.

***Note:** The attached Shadow Guide form is just a placeholder and not the actual form that would be used by participants.*



Fraud Ops: ATO Overview

2

FRAUD OPS: ACCOUNT TAKEOVER BRANCH

This page is a module placeholder. This module would provide an overview of the Fraud Ops: ATO Branch.

Module Description

Rationale: All new hires will be required to participate in a total of five job shadow sessions, one for each Fraud Ops department. The Fraud Ops department is the frontline investigator who is responsible for fraud detection and mitigation. Each department specializes in one of the major types of financial fraud. They are the core component of the Security Division. Other departments within the Division work together to support Fraud Ops operations.

For example, a Fraud Analytics employee helps analyze data for fraud trends and write mitigation rules for systems used to detect or prevent fraud activities on accounts. Departments beyond Fraud Ops need to have a clear understanding of how their roles impact the workflow and processes, as this knowledge is crucial for effective fraud prevention.

Module Content

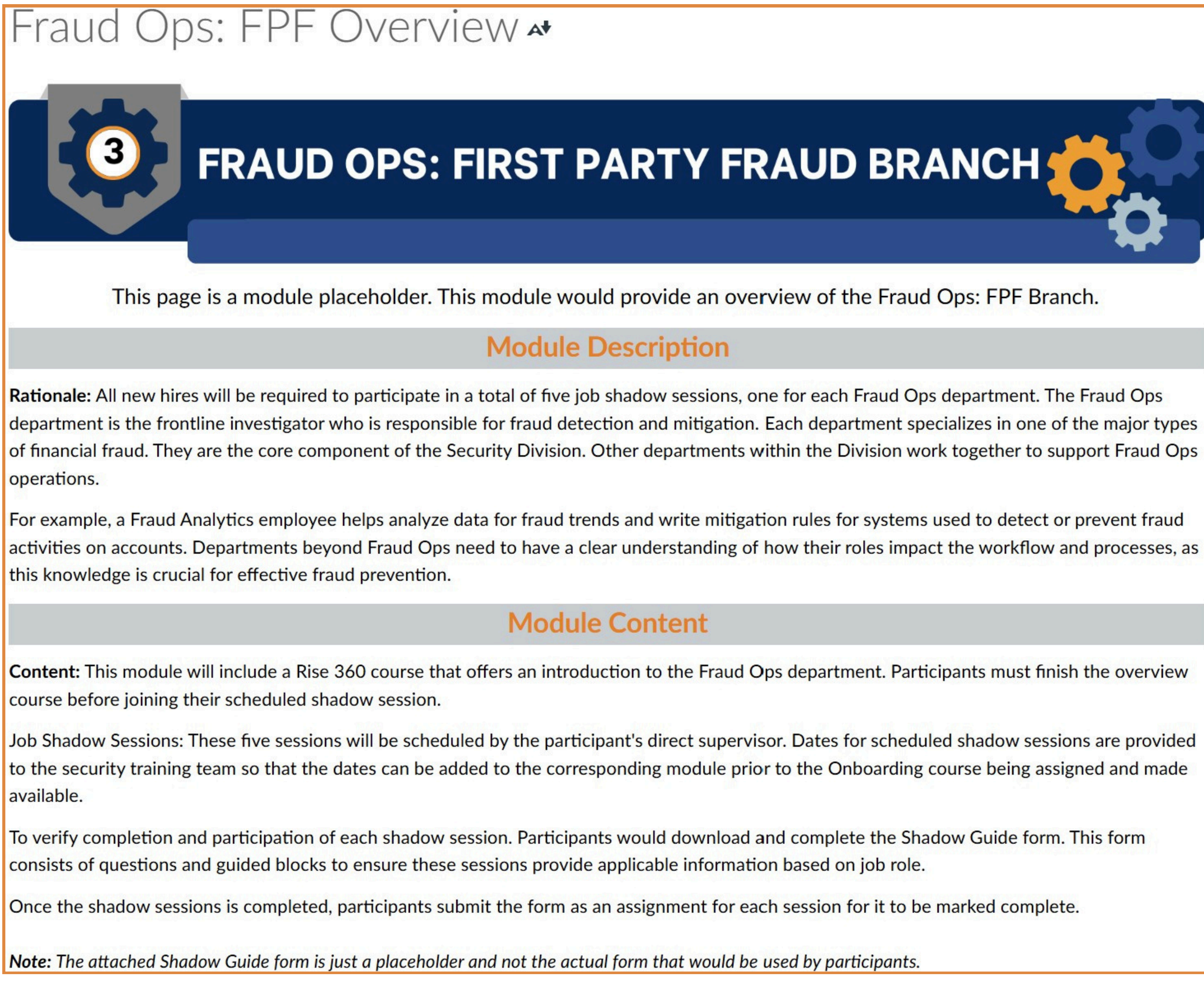
Content: This module will include a Rise 360 course that offers an introduction to the Fraud Ops department. Participants must finish the overview course before joining their scheduled shadow session.

Job Shadow Sessions: These five sessions will be scheduled by the participant's direct supervisor. Dates for scheduled shadow sessions are provided to the security training team so that the dates can be added to the corresponding module prior to the Onboarding course being assigned and made available.

To verify completion and participation of each shadow session. Participants would download and complete the Shadow Guide form. This form consists of questions and guided blocks to ensure these sessions provide applicable information based on job role.

Once the shadow sessions is completed, participants submit the form as an assignment for each session for it to be marked complete.

***Note:** The attached Shadow Guide form is just a placeholder and not the actual form that would be used by participants.*



Fraud Ops: FPF Overview

3

FRAUD OPS: FIRST PARTY FRAUD BRANCH

This page is a module placeholder. This module would provide an overview of the Fraud Ops: FPF Branch.

Module Description

Rationale: All new hires will be required to participate in a total of five job shadow sessions, one for each Fraud Ops department. The Fraud Ops department is the frontline investigator who is responsible for fraud detection and mitigation. Each department specializes in one of the major types of financial fraud. They are the core component of the Security Division. Other departments within the Division work together to support Fraud Ops operations.

For example, a Fraud Analytics employee helps analyze data for fraud trends and write mitigation rules for systems used to detect or prevent fraud activities on accounts. Departments beyond Fraud Ops need to have a clear understanding of how their roles impact the workflow and processes, as this knowledge is crucial for effective fraud prevention.

Module Content

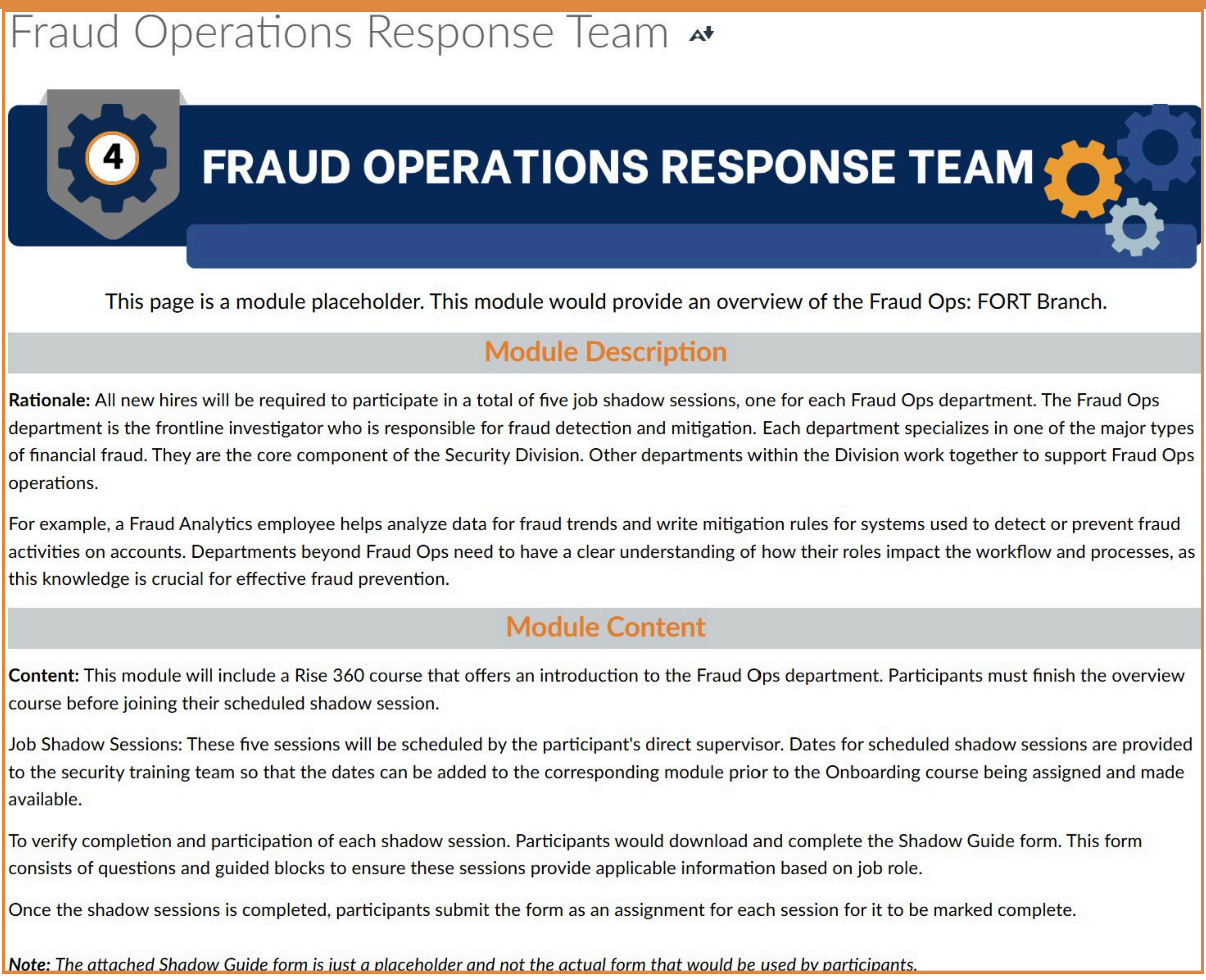
Content: This module will include a Rise 360 course that offers an introduction to the Fraud Ops department. Participants must finish the overview course before joining their scheduled shadow session.

Job Shadow Sessions: These five sessions will be scheduled by the participant's direct supervisor. Dates for scheduled shadow sessions are provided to the security training team so that the dates can be added to the corresponding module prior to the Onboarding course being assigned and made available.

To verify completion and participation of each shadow session. Participants would download and complete the Shadow Guide form. This form consists of questions and guided blocks to ensure these sessions provide applicable information based on job role.

Once the shadow sessions is completed, participants submit the form as an assignment for each session for it to be marked complete.

***Note:** The attached Shadow Guide form is just a placeholder and not the actual form that would be used by participants.*



Fraud Operations Response Team

4 FRAUD OPERATIONS RESPONSE TEAM

This page is a module placeholder. This module would provide an overview of the Fraud Ops: FORT Branch.

Module Description

Rationale: All new hires will be required to participate in a total of five job shadow sessions, one for each Fraud Ops department. The Fraud Ops department is the frontline investigator who is responsible for fraud detection and mitigation. Each department specializes in one of the major types of financial fraud. They are the core component of the Security Division. Other departments within the Division work together to support Fraud Ops operations.

For example, a Fraud Analytics employee helps analyze data for fraud trends and write mitigation rules for systems used to detect or prevent fraud activities on accounts. Departments beyond Fraud Ops need to have a clear understanding of how their roles impact the workflow and processes, as this knowledge is crucial for effective fraud prevention.

Module Content

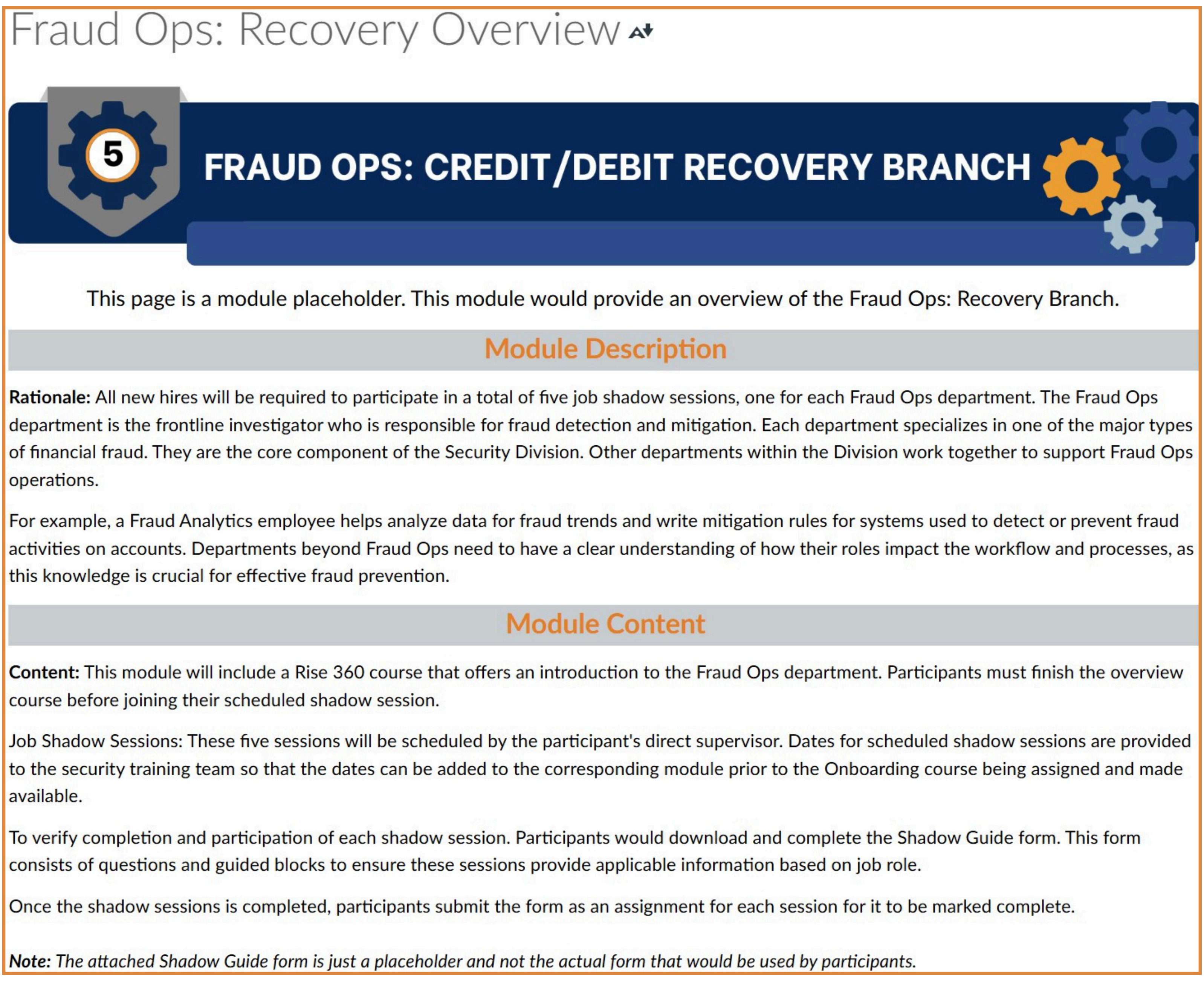
Content: This module will include a Rise 360 course that offers an introduction to the Fraud Ops department. Participants must finish the overview course before joining their scheduled shadow session.

Job Shadow Sessions: These five sessions will be scheduled by the participant's direct supervisor. Dates for scheduled shadow sessions are provided to the security training team so that the dates can be added to the corresponding module prior to the Onboarding course being assigned and made available.

To verify completion and participation of each shadow session. Participants would download and complete the Shadow Guide form. This form consists of questions and guided blocks to ensure these sessions provide applicable information based on job role.

Once the shadow sessions is completed, participants submit the form as an assignment for each session for it to be marked complete.

***Note:** The attached Shadow Guide form is just a placeholder and not the actual form that would be used by participants.*



Fraud Ops: Recovery Overview

5 FRAUD OPS: CREDIT/DEBIT RECOVERY BRANCH

This page is a module placeholder. This module would provide an overview of the Fraud Ops: Recovery Branch.

Module Description

Rationale: All new hires will be required to participate in a total of five job shadow sessions, one for each Fraud Ops department. The Fraud Ops department is the frontline investigator who is responsible for fraud detection and mitigation. Each department specializes in one of the major types of financial fraud. They are the core component of the Security Division. Other departments within the Division work together to support Fraud Ops operations.

For example, a Fraud Analytics employee helps analyze data for fraud trends and write mitigation rules for systems used to detect or prevent fraud activities on accounts. Departments beyond Fraud Ops need to have a clear understanding of how their roles impact the workflow and processes, as this knowledge is crucial for effective fraud prevention.

Module Content

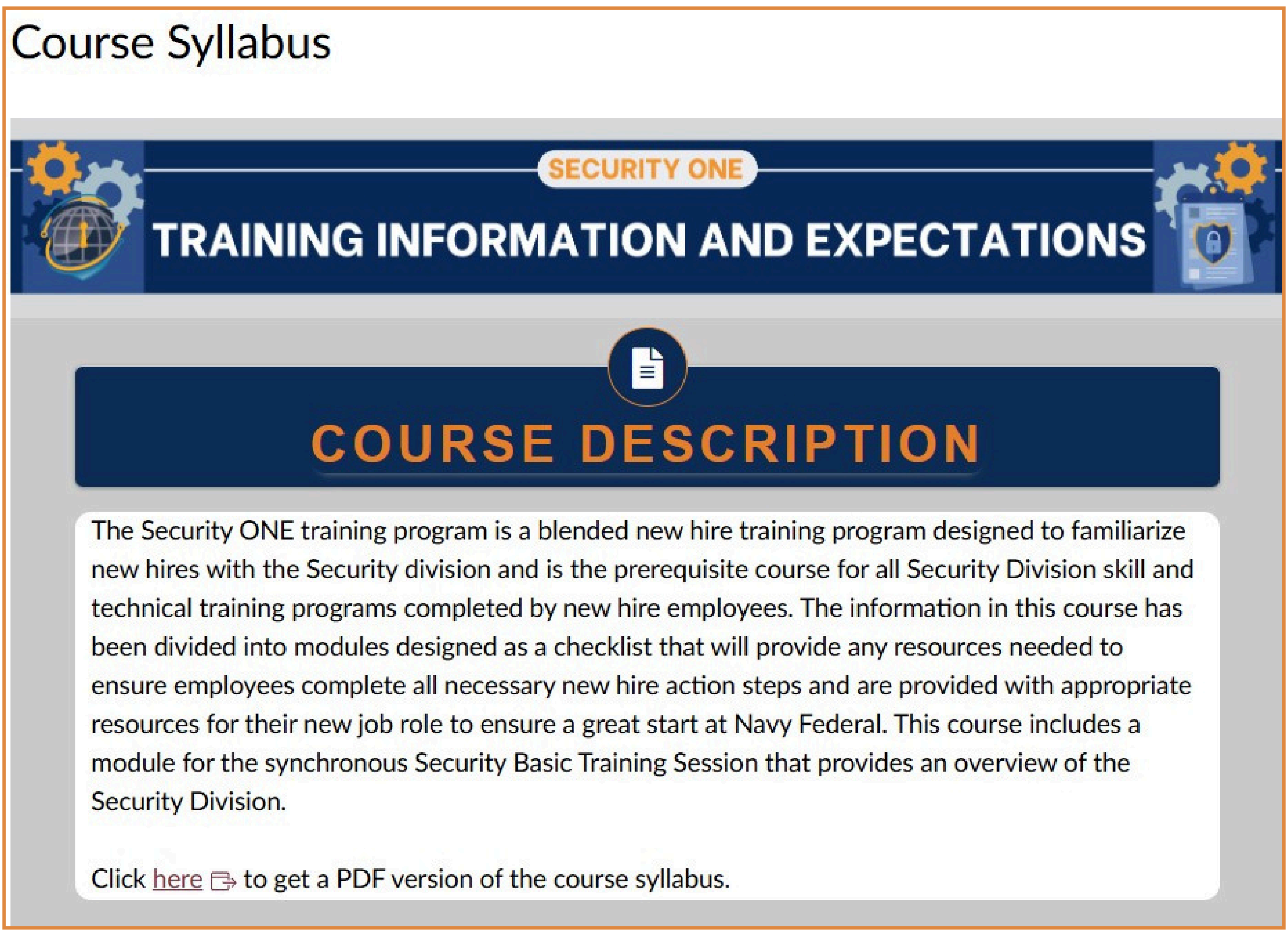
Content: This module will include a Rise 360 course that offers an introduction to the Fraud Ops department. Participants must finish the overview course before joining their scheduled shadow session.

Job Shadow Sessions: These five sessions will be scheduled by the participant's direct supervisor. Dates for scheduled shadow sessions are provided to the security training team so that the dates can be added to the corresponding module prior to the Onboarding course being assigned and made available.

To verify completion and participation of each shadow session. Participants would download and complete the Shadow Guide form. This form consists of questions and guided blocks to ensure these sessions provide applicable information based on job role.

Once the shadow sessions is completed, participants submit the form as an assignment for each session for it to be marked complete.

***Note:** The attached Shadow Guide form is just a placeholder and not the actual form that would be used by participants.*



Course Syllabus

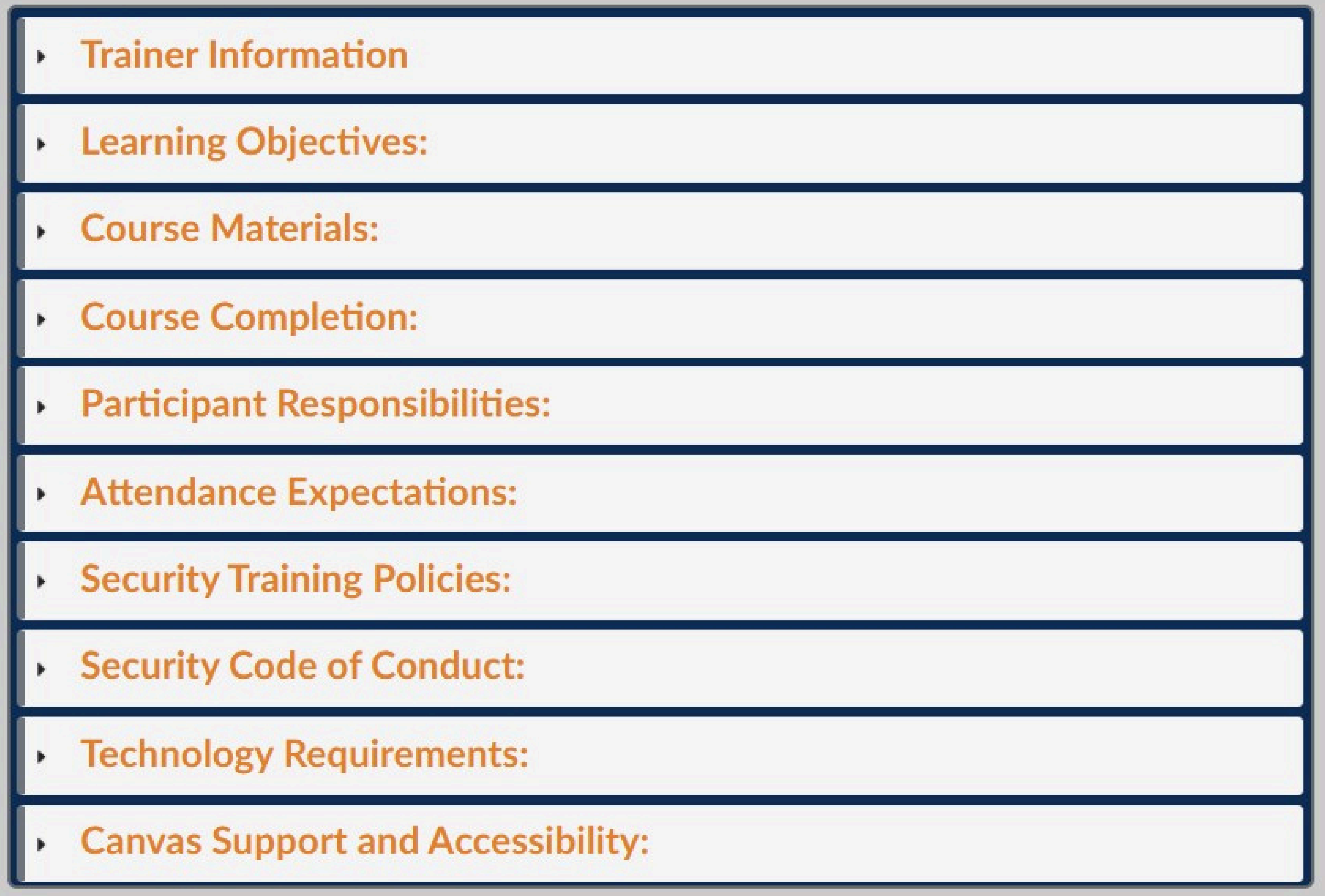
SECURITY ONE

TRAINING INFORMATION AND EXPECTATIONS

COURSE DESCRIPTION

The Security ONE training program is a blended new hire training program designed to familiarize new hires with the Security division and is the prerequisite course for all Security Division skill and technical training programs completed by new hire employees. The information in this course has been divided into modules designed as a checklist that will provide any resources needed to ensure employees complete all necessary new hire action steps and are provided with appropriate resources for their new job role to ensure a great start at Navy Federal. This course includes a module for the synchronous Security Basic Training Session that provides an overview of the Security Division.

Click here to get a PDF version of the course syllabus.



▸ Trainer Information

▸ Learning Objectives:

▸ Course Materials:

▸ Course Completion:

▸ Participant Responsibilities:

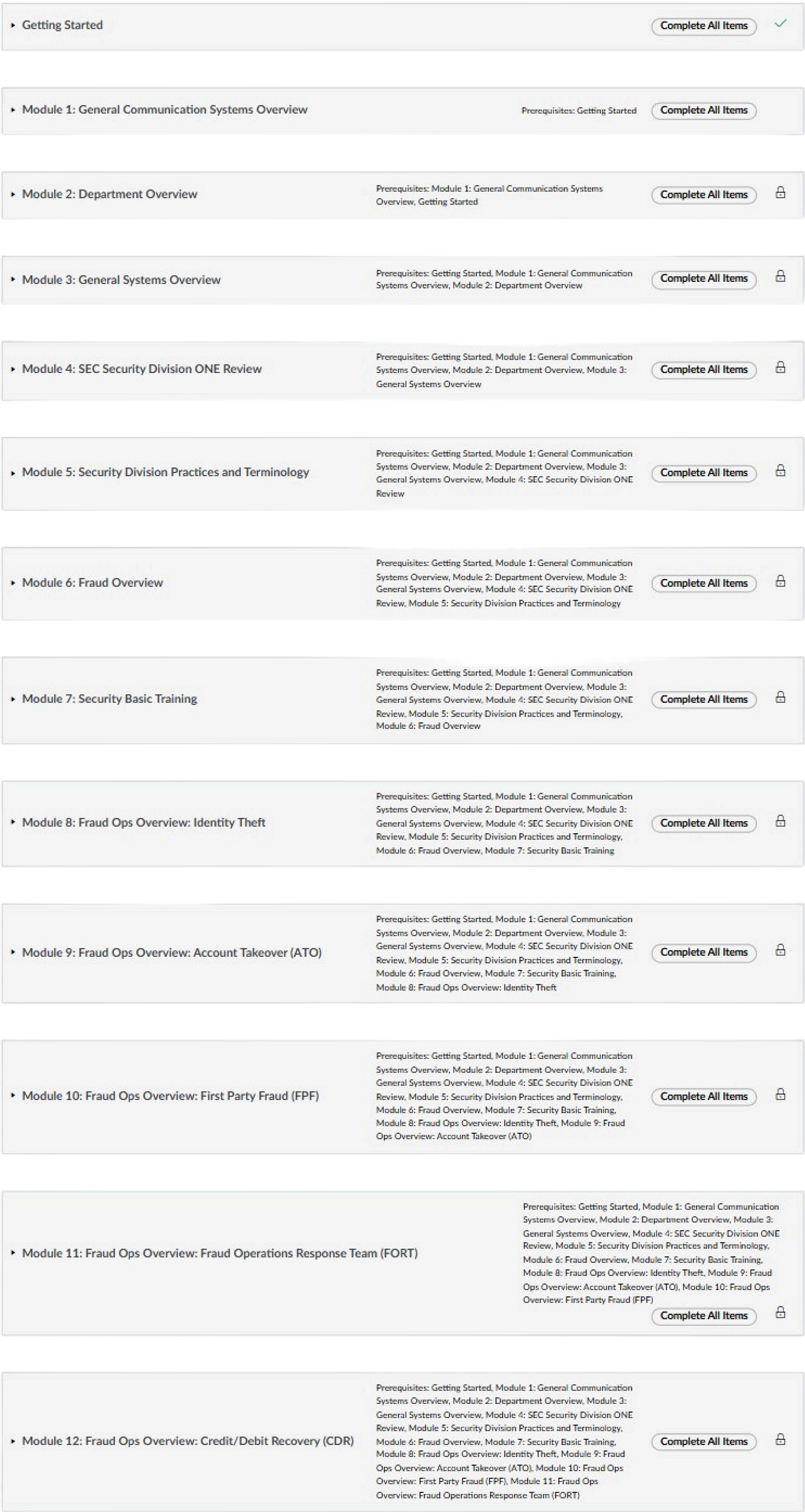
▸ Attendance Expectations:

▸ Security Training Policies:

▸ Security Code of Conduct:

▸ Technology Requirements:

▸ Canvas Support and Accessibility:



▸ Getting Started — Complete All Items ✓

▸ Module 1: General Communication Systems Overview — Prerequisites: Getting Started — Complete All Items

▸ Module 2: Department Overview — Prerequisites: Module 1: General Communication Systems Overview, Getting Started — Complete All Items 🔒

▸ Module 3: General Systems Overview — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview — Complete All Items 🔒

▸ Module 4: SEC Security Division ONE Review — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview — Complete All Items 🔒

▸ Module 5: Security Division Practices and Terminology — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review — Complete All Items 🔒

▸ Module 6: Fraud Overview — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology — Complete All Items 🔒

▸ Module 7: Security Basic Training — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview — Complete All Items 🔒

▸ Module 8: Fraud Ops Overview: Identity Theft — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview, Module 7: Security Basic Training — Complete All Items 🔒

▸ Module 9: Fraud Ops Overview: Account Takeover (ATO) — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview, Module 7: Security Basic Training, Module 8: Fraud Ops Overview: Identity Theft — Complete All Items 🔒

▸ Module 10: Fraud Ops Overview: First Party Fraud (FPF) — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview, Module 7: Security Basic Training, Module 8: Fraud Ops Overview: Identity Theft, Module 9: Fraud Ops Overview: Account Takeover (ATO) — Complete All Items 🔒

▸ Module 11: Fraud Ops Overview: Fraud Operations Response Team (FORT) — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview, Module 7: Security Basic Training, Module 8: Fraud Ops Overview: Identity Theft, Module 9: Fraud Ops Overview: Account Takeover (ATO), Module 10: Fraud Ops Overview: First Party Fraud (FPF) — Complete All Items 🔒

▸ Module 12: Fraud Ops Overview: Credit/Debit Recovery (CDR) — Prerequisites: Getting Started, Module 1: General Communication Systems Overview, Module 2: Department Overview, Module 3: General Systems Overview, Module 4: SEC Security Division ONE Review, Module 5: Security Division Practices and Terminology, Module 6: Fraud Overview, Module 7: Security Basic Training, Module 8: Fraud Ops Overview: Identity Theft, Module 9: Fraud Ops Overview: Account Takeover (ATO), Module 10: Fraud Ops Overview: First Party Fraud (FPF), Module 11: Fraud Ops Overview: Fraud Operations Response Team (FORT) — Complete All Items 🔒