Navy Federal Credit Union

SECURITY

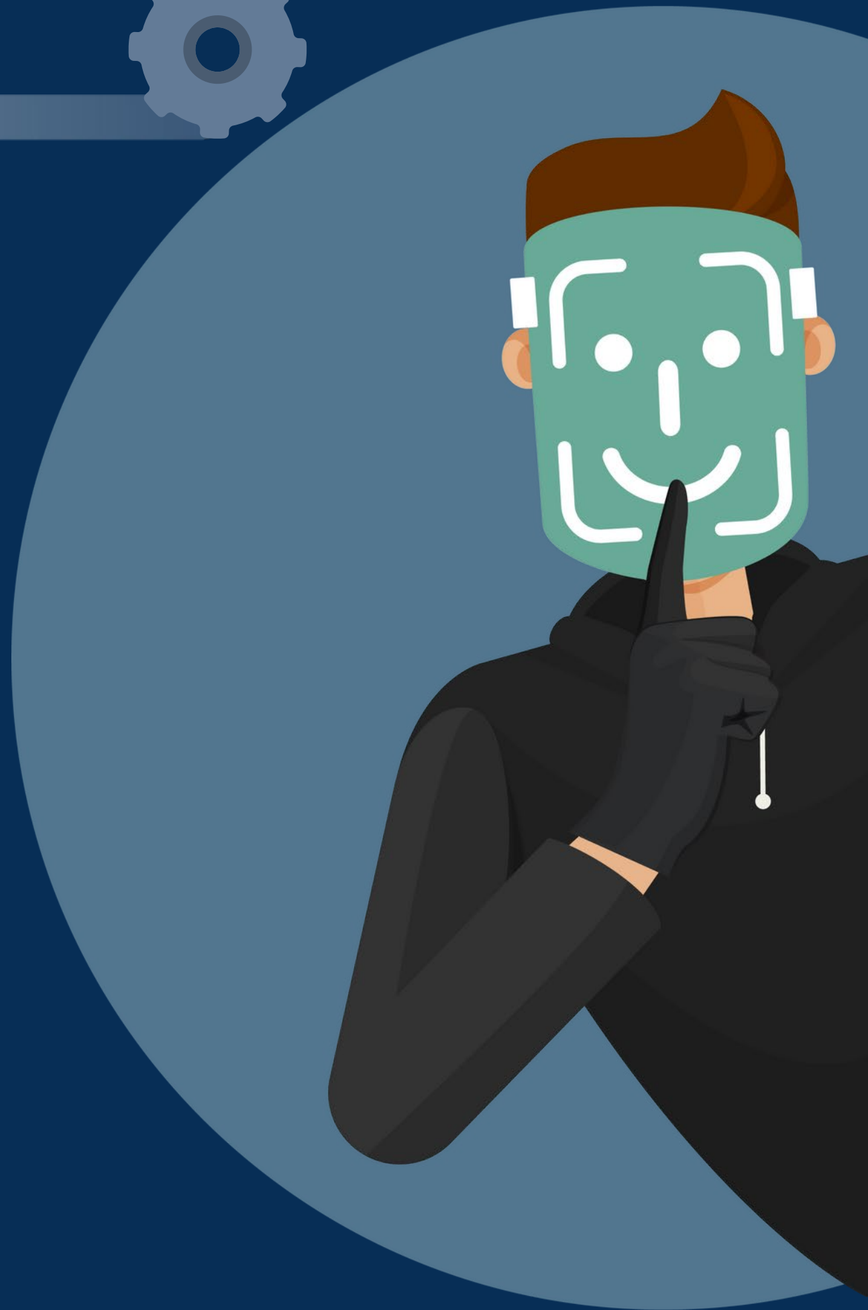
BASIC TRAINING COURSE

HOUSEKEEPING

- Respect Others
- Distractions
- Participate
- Virtual Hand Raise
- Meeting Chat
- Ask questions

OBJECTIVES

- Discuss fraud scam scenarios
- Identify how to distinguish different types of scams based on victim’s activity
- Recognize strategies scammers use to steal information
- Explain the best practices for fraud prevention

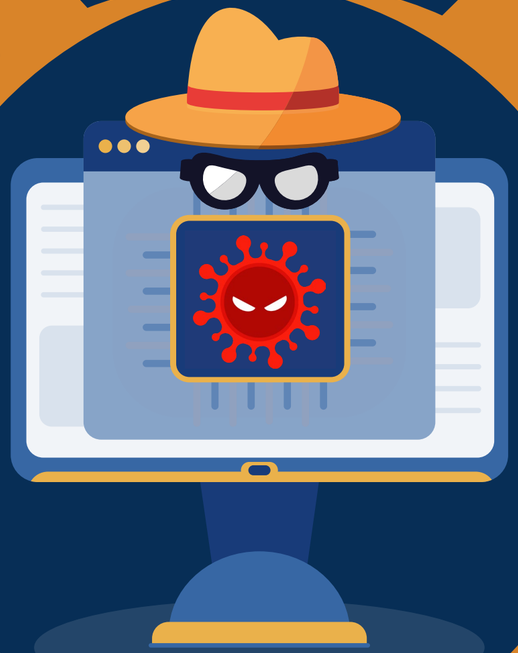


TYPES OF SCAMS

Smishing

Phishing

Scareware



Pharming

Vishing

Pretexting

SCAMMER TACTICS

KNOW THE RED FLAGS AND TATICS OF SCAMMERS

Scammer
Starts with a promise of something desirable. Devious plan.

Target
Reach out to potential victim. This could be anyone at anytime.

Hook
Lure victim with initial message that seems reasonable. The hook.

Conversation
Start dialogue to engage victims just enough to get them interested in their plan.

Victim
Victim loses money or assets after scammers plan is completed.

FRAUD MITIGATION

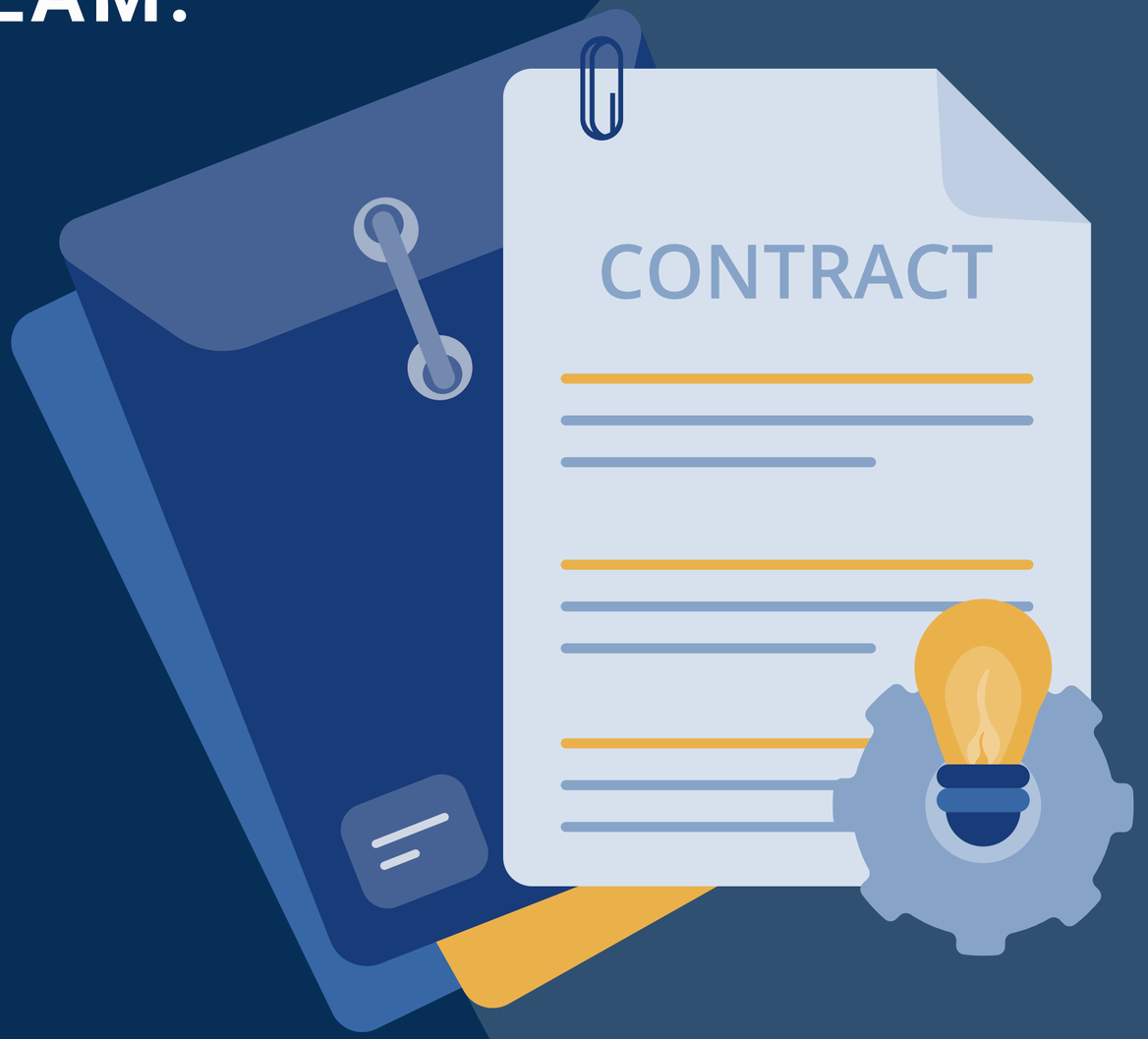
ESTABLISHING A RESPONSE TEAM:

Establish clear responsibilities:

- Assess the impact
- Contain the breach
- Communicate effectively
- Prevent recurrence.

Include individuals skilled in:

- Technology
- Communications
- System interfaces



FRAUD MITIGATION

FRAUD PREVENTION TIPS

COMMUNICATION PROTOCOLS

- Clear communication protocols during an incident are critical.
- Prompt information sharing within the team.
- Timely accurate reporting to affected parties and regulators.
- Minimize damage and restore operations swiftly.

FRAUD MITIGATION

POST INCIDENTS ANALYSIS:

Conduct a thorough analysis of how the incident occurred:

- What was compromised?
- How was the response handled?

What are the necessary updates in:

- Policies
- Procedures
- Technologies.

FRAUD MITIGATION

CONINUOUS IMPROVEMENT STRATEGIES

Refining is key to improving the organization’s defensive and reactive capabilities:

- Use incidents to continuously improve processes.
- Provide comprehensive training for employees.
- Upgrade systems.

FRAUD MITIGATION

REPORTING AND DOCUMENTING

It’s essential to report the incident appropriate agencies:

- Track down the perpetrators
- Potentially recover stolen data or assets

Importance of Response Documentation:

- Informs post-incident analysis
- Adhere to compliance and regulations
- Identify areas strengths and weaknesses
- Identify new Social Engineering fraud tactics.

FRAUD MITIGATION

- Team to identify patterns for prompt responses.
- Trace and determine source of Incident
- Analyze and document anlytical data of suspect activity
- Identify strengths and weaknesses for continuous improvement
- Enhance seamless collaboration among security systems

Questions?

THANK YOU FOR ATTENDING THIS COURSE