



30 MINUTE WORKSHOP

# **Protecting Your Digital Identity: A Guide to Cybersecurity and Fraud Prevention**

FACILITATOR GUIDE

---

---

# **TABLE OF CONTENTS**

## **WORKSHOP OVERVIEW & PREP**

Overview & Objectives—3

Agenda —4

Preparation Requirements—5

Facilitator Tips—7

## **WORKSHOP OUTLINE 8**

Intro: Why Cybersecurity Matters—9

Lesson: Understanding the Threats—10

Activity: Scam Checker Coach—11

Lesson: Spotting Red Flags—12

Lesson: Building Your Digital Defense—13

Lesson: Your Emergency Action Plan—14

Wrap-Up & Conclusion—15

---

# OVERVIEW

## & OBJECTIVES

**Workshop Title:** Protecting Your Digital Identity: A Guide to Cybersecurity and Fraud Prevention

**Target Audience:** Adults age 18+ who want to improve their financial health and learn more about protecting their personal and financial information online.

**Duration:** 90 minutes

### Learning Objectives

By the end of this session, participants will:

1. Understand the personal relevance and importance of digital security.
2. Learn the common tactics used by fraudsters, including phishing and common scams.
3. Brainstorm and learn concrete steps to build a strong digital defense, including password security and MFA.
4. Receive a clear action plan for what to do if they become a victim of fraud.
5. Know where to find additional resources to boost financial wellness.

---

# AGENDA

## & TIMELINE

#	Duration/Time	Activity	Facilitator	Materials
1	2-3 minutes	Why Cybersecurity Matters		
2	2-3 minutes	Lesson: Understanding the Threats		
3	5 minutes	Activity: Scam Checker Coach		
4	2-3 minutes	Lesson: Spotting Red Flags		
5	5 minutes	Lesson: Building Your Digital Defense		
6	5 minutes	Lesson: Your Emergency Action Plan		
7	5 minutes	Lesson: Wrap up & Conclusion		

---

# PREPARATION

## REQUIREMENTS

### Materials Prep

#### Copies to Make

Print copies of the following handout and worksheets for participants.

- ☐ Agenda— Update to to reflect your session details.
- ☐ Worksheet: Identity Theft Emergency Action Plan
- ☐ Worksheet: My Digital Security Pledge
- ☐ Handout: Scam Scenarios

#### Supplies

Supplies for each participant:

- ☐ Folder with printed materials for workshop
- ☐ Water bottle
- ☐ Notepad and pen for taking notes

---

## Technology Prep

### Presenter Slides

Copy the slideshow to your Google Drive or add them to your slideshow app and make the following customizations:

- ☐ Add presenter name on slide 1 (“PRESENTED BY”)
- ☐ Add logo on slides 1, 2, 6, 10, 12, and 16 ( “YOUR LOGO HERE”)
- ☐ Update subdomain in links on slides 7 and 15 (“yoursubdomain”)
- ☐ Add contact information on slide 16

### Online Links

Have the following pages open and ready (all accessible via your Banzai Wellness Center):

- Banzai Scam Checker Coach

## Room Setup and Logistics

### Equipment Requirements

- Computer for slides
- Projector/TV to display slides and resources
- Participants: computer or device and Wi-Fi accessibility, if you want them to complete activities on their own

### Room Layout Suggestions

- Tables and chairs facing whiteboard/projector wall
- Table at entry point with name tags for participants
- Table at the back with any additional handouts and resources

### At Each Seat

- Folder with printed materials for workshop
- Water bottle
- Notepad and pen for taking notes

---

# FACILITATOR

## TIPS

### **Presentation Style and Tone**

**Approachable and relatable.** Avoid jargon and overly technical terms. Explain concepts in simple, everyday language—the script in the workshop outline will strike the right tone.

**Friendly and welcoming.** Create a comfortable and non-judgmental atmosphere where participants feel safe to ask questions and share their experiences. Smile!

**Optimistic and enthusiastic.** Frame digital fraud prevention and awareness as a tool for reducing stress and fear and empowering the participants.

**Practical and knowledgeable.** Focus on actionable steps and real-world examples that participants can implement immediately. Be prepared to offer helpful resources, tools, and tips beyond the core content.

### **Presentation & Engagement Techniques**

**Rotate presenters often.** Consider rotating presenters for every segment of the workshop. This keeps participants' interest, and different styles of presenting can speak to different attendees.

**Keep stories brief.** Share personal anecdotes to illustrate points and build connections, but keep stories to a few minutes or less.

**Use breaks if necessary.** For longer workshops, build in 5-minute breaks for participants to stretch their legs and check their phones.

**Vary presentation styles.** Include icebreakers, large and small group discussions, visual aids, and more.

**Stay on the clock.** Be mindful of the time—even use a stopwatch—to keep the workshop from dragging.

---

# WORKSHOP OUTLINE

## FACILITATOR GUIDE



---

# INTRO

## WHY CYBERSECURITY MATTERS

**Duration: 2-3 minutes**

---

### Key Messages

- The goal of this workshop is empowerment, not fear.

### Script & Instructions

*Begin slideshow on slide 1—Welcome*

"Welcome to (your financial institution)'s cybersecurity workshop. Thank you for your time and trust."

Briefly introduce yourself and your position at the institution.

*Begin slideshow on slide 2—Stats*

"I want to start with a number: \$10.3 billion. According to the Federal Trade Commission, that was the amount of money lost to fraud by Americans in 2023 alone. That's a 14% increase from the year before. This isn't a problem that's going away; it's growing, and it's affecting people in our community every single day."

"Today, we'll focus on simple, powerful actions, not complicated tech, that can help you protect your digital details."

*Advance to slide 3 — Agenda*

"This is the agenda for today's presentation."

---

# LESSON

## UNDERSTANDING THE THREATS

**Duration: 2-3 minutes**

---

### Key Messages

- Combine threat awareness with immediate, practical solutions.

### Script

*Advance to slide 4 – Digital Footprint*

“When you walk along a sandy beach, you leave behind a trail of footprints. In the same way, every time you use the internet, you leave behind a trail of data. This trail is your Digital Footprint.”

*Advance to slide 5 – Understanding Threats*

“The most common ways your digital footprint is targeted is through scams. Specifically, phishing in the form of email and text messages.

*Advance to slide 6—Phishing*

Phishing scams are fraudulent attempts to deceive people into revealing sensitive information. Phishing uses fake emails, messages, or websites that appear to be from trustworthy sources.

Scammers often pose as trusted entities and manipulate victims into divulging sensitive information or transferring funds.”

---

# ACTIVITY

## SCAM CHECKER COACH

**Duration: 5 minutes**

---

### Key Messages

- This provides a hands-on, memorable experience of how to analyze a suspicious message in real-time.

*Advance to slide 7—Scam Checker Coach*

### Script

"To succeed, scammers are very good at creating a situation that triggers a sense of fear or urgency, trying to get you to act before you have time to think. So, for the next few minutes, we're going to pull back the curtain on their playbook by learning the major red flags to watch for."

"We are going to use the Banzai 'Scam Checker' Coach. We will go through one example of a suspicious message together, and then give you a handout of few scenarios to go through at home."

Project the "Scam Checker" tool (using [your-subdomain\).banzai.org/wellness/resources/scam-checker-coach](https://(your-subdomain).banzai.org/wellness/resources/scam-checker-coach))

Click **Get Started** to begin the Coach, and answer the questions based on the text message scenario.

*Advance to slide 8—Scam Scenario*

"Imagine you receive this text message:

(Your Financial Institution Name) ALERT: A payment of \$749.50 to CryptoWallet has been authorized from your account. If this was NOT you, you must log in immediately to cancel the payment: [bit.ly/bank-cancel-pay]."

### Discussion Prompts

"What are the red flags that this is a scam?"

Possible answers:

- Urgency: It demands immediate action to prevent financial loss.
- Impersonation: It uses the name of a trusted institution (their financial institution).
- Suspicious Link: It uses a link shortener (bit.ly), which is not how a real financial institution would send a security link.

Now, distribute to the Scam Scenarios handout. Have them work through the remaining at home.

---

# LESSON

## SPOTTING RED FLAGS

**Duration: 5 minutes**

---

### Key Messages

- Recognizing the red flags is a critical skill.

*Advance to slide 9—Red Flags*

### Script

“No matter the specific story they tell you, most scams share a few common warning signs. Here are the biggest ones to look out for.”

- **First, a feeling of pressure to act quickly.** Scammers know that if you have time to think or do research, you'll see through their scam. They create a sense of urgency by threatening you, maybe saying a loved one is in trouble or that you'll lose access to an account.
- **Second, requests for sensitive information.** Scammers will try to get your passwords, Social Security number, or bank account numbers. You should know that legitimate companies and government agencies will almost never ask you for this kind of information in an email or text.
- **Third, requests for payment in unusual ways.** A major red flag is if someone asks you to pay for something using wire transfers, cash, or especially gift cards. They do this because it's very difficult to trace or cancel those types of transactions.
- **And finally, an offer that seems too good to be true.** This is a classic for a reason. Scammers often use the lure of a prize, a lottery winning, or a great deal to get you to let your guard down.”

---

# LESSON

## BUILDING YOUR DIGITAL DEFENSE

**Duration: 5 minutes**

---

### Key Messages

- Strong, unique passwords and Multi-Factor Authentication (MFA) are your most powerful defenses.

### Script

*Advance to slide 10—Your Digital Defense*

"An old adage says the best offense is a good defense—and that's true for protecting your digital identity, too."

"Your first and most important line of defense is how you access your accounts."

"You want to start with password best practices. Your passwords should be long (at least 12-15 characters), complex (a mix of cases, numbers, and symbols), and unique for every important account."

"To manage this, a Password Manager is an essential tool. It creates and remembers long, unique passwords for every site, so you only have to remember one."

"Multi-Factor Authentication (MFA) is another tool. This requires something you know (your password) and something you have (like a code on your phone). It is a critical layer of security and you should enable it everywhere it is offered."

*Advance to slide 11—Pause*

"Finally, the human firewall. Scammers need you to act fast and feel emotion. Your best defense is to simply pause and think before clicking any link or downloading any attachment."

---

# LESSON

## YOUR EMERGENCY ACTION PLAN

**Duration: 5 minutes**

---

### Key Messages

- Having a clear action plan reduces panic and allows for a swift, effective response to fraud.

### Script

*Advance to slide 12-Emergency Plan*

"Okay, we've spent time talking about prevention. But what if the worst happens? There are three steps you can quickly take. Think of this as your First Aid kit for identity theft."

"Step one: Lock Down. Immediately call the fraud department for any financial institution or credit card company to report fraud and block all accounts."

"Step two: Freeze. Place a credit freeze with the three major credit bureaus: Equifax, Experian, and TransUnion. This stops new accounts from being opened in your name."

"Step three: Report. File an official report at [IdentityTheft.gov](https://www.identitytheft.gov)."

*Distribute the "Emergency Action Plan" handout.*

"The handout I'm passing around summarizes the three steps we just discussed, along with the names and websites for the three credit bureaus and [IdentityTheft.gov](https://www.identitytheft.gov). This is a document you can take home and put somewhere safe."

### Discussion Prompt

"What do you think is the single most important step in this action plan? Why?"

---

# WRAP UP

## & CONCLUSION

**Duration: 5 minutes**

---

### Key Message

- Encourage the audience to commit to at least one set towards better cyber practices

### Script

*Advance to slide 13—What We Learned*

"Before we wrap up, let's review what we learned today:"

- Get a password manager
- Enable multi-factor authentication everywhere you can
- Pause before you click

*Advance to slide 14—Personal Plan and distribute the "Personal Action Plan" handout.*

"I want you to take out your Personal Action Plan handout. Write down ONE thing you will do this week to improve your digital security."

*Advance to slide 15—Resources*

"Here are some additional online resources we provide related to your digital identity and cybersecurity, accessed via our Wellness Center."

Feel free to note other websites, seminars, and workshops provided by your financial institution.

*Advance to slide 16—Contact Info*

Provide contact information for further assistance. "Thank you for participating today."