



90 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: Your Digital Footprint—10

Lesson: Understanding the Threats—11

Lesson: Spotting Red Flags—13

Activity: Scam Checker Coach—14

Lesson: Building Your Digital Defense—16

Activity: Password Strength Test—18

Lesson: Your Emergency Action Plan—19

Wrap-Up & Conclusion—21

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	5 minutes	Why Cybersecurity Matters		
2	5 minutes	Lesson: Your Digital Footprint		
3	10 minutes	Lesson: Understanding the Threats		
4	5 minutes	Lesson: Spotting Red Flags		
5	20 minutes	Activity: Scam Checker Coach		
6	10 minutes	Lesson: Building Your Digital Defense		
7	10 minutes	Activity: Password Strength Test		
8	15 minutes	Lesson: Your Emergency Action Plan		
9	10 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
- ☐ Privacy tri-fold
- ☐ 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, 16, 17, 20, and 24 (“YOUR LOGO HERE”)
- ☐ Update subdomain in links on slides 16 and 24 (“yoursubdomain”)
- ☐ Add contact information on slide 24

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
- Whiteboard and markers
- 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
- Privacy tri-fold
- 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: 5 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."

"I want to tell you about a common situation. Jane got an urgent text message that looked like it was from her bank, warning her about a suspicious charge. It looked legitimate, so she clicked the link and entered her login details to 'verify' her account. Two days later, she was declined when buying groceries. When she checked her account, her entire checking balance had been drained. What followed wasn't just the financial loss; it was dozens of hours on the phone with fraud departments, filing police reports, and the lingering, stressful feeling of being violated. The criminals didn't break down her door; they walked right in through her phone. Today, we're going to learn how to lock that digital door."

Discussion Prompt

"Raise your hand if you've ever received a suspicious email or text message. You're not alone, and that's why we're here today."

Advance to slide 3 — Agenda

"This is the agenda for today's workshop." Before you begin, let participants know where the bathrooms are, where they can find water/snacks, and any expected break times.

LESSON

YOUR DIGITAL FOOTPRINT

Duration: 5 minutes

Key Messages

- Your online data trail, or "Digital Footprint," is valuable and needs protection.

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.”

“It's the collection of all your online activities, creating a unique picture of who you are. This footprint is made up of two different types:”

- Active Digital Footprint: This includes the data you intentionally and knowingly share. It's the information you actively post or send out. Examples include:
 - Sending an email.
 - Posting updates, photos, or comments on social media platforms like Facebook, Instagram, or LinkedIn.
 - Filling out an online form or subscribing to a newsletter.
- Passive Digital Footprint: This is the data trail you leave unintentionally, often without your direct action or awareness. It's information that is collected in the background as you move across the web. Examples include:
 - Websites installing cookies on your browser to track your visits and preferences.
 - Social media platforms and advertisers tracking your likes and shares to build a profile of your interests.
 - Your IP address being logged when you visit a website, revealing your general location.

“Every piece of this footprint, both active and passive, combines to create a detailed digital representation of your life, habits, and personality. Understanding this concept is the first step in learning how to manage and protect it.”

Discussion Prompts

What surprises you about your digital footprint? Were you aware of all the different trails of data you're leaving online?

LESSON

UNDERSTANDING THE THREATS

Duration: 10 minutes

Key Messages

- Fraudsters use predictable tactics like phishing to steal your information.

Script

Advance to slide 5 – Understanding Threats

"Let's pull back the curtain on how fraudsters operate. One of the most common ways your digital footprint is targeted is through scams.

If you use a phone or have an email account, you have almost certainly been the target of a scam.

The goal of a scammer is simple: to get your money or your sensitive personal information. They do this by pretending to be someone they aren't to trick you. This is often called Phishing when it happens through emails, fake websites, or texts.

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."

Advance to slide 6—Malware

Types of Scams

Malware is malicious software that can infiltrate computer networks, steal sensitive information, and disrupt your device's normal operations. Common examples include viruses and ransomware.

Example: You receive an email from a friend with the subject "You have to see this!" and an attached video file. When you click to open the video, nothing seems to happen. In the background, however, the file has installed a "keylogger" on your computer. The next time you log in to your bank's website, the malware records your username and password, sending it directly to the scammer.

Advance to slide 7—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.

Example: You receive an email with the subject "Action Required: Your Subscription is On Hold." The email looks like it's from Netflix or another streaming service and states that they were unable to process your last payment. It asks you to click a button to update your billing details, but the link takes you to a fake website designed to steal your credit card and password information.

Continued on page 11

Continued from page 11

Advance to slide 8—Impersonation

Impersonation scams involve scammers pretending to be someone else to deceive individuals for financial gain or personal information. Scammers pose as trusted entities and manipulate victims into divulging sensitive information or transferring funds.

Example: You get a text message that appears to be from the USPS. It says a package is being held due to an unpaid customs fee of \$2.99. The message includes a link to a website that looks official and asks for your credit card information to pay the small fee. The goal is to steal your card number for larger fraudulent purchases.

Advance to slide 9—Tech Support

Tech support scams involve fraudsters posing as technical support representatives from well-known companies.

Example: A pop-up window appears that looks like a security alert from Microsoft or Apple. It warns that your computer is infected with a virus and your data is at risk. The pop-up instructs you to immediately call a toll-free number. When you call, a fake technician pressures you into giving them remote access to your computer and paying hundreds of dollars for useless "repairs" or software.

Advance to slide 10—Government Imposter

Government imposter scams involve individuals falsely claiming to represent government agencies such as the Internal Revenue Service (IRS), Social Security Administration (SSA), or local law enforcement.

Example: You receive a voicemail from an "Officer" claiming to be with the Social Security Administration. The message says your Social Security number has been linked to criminal activity and has been suspended. To avoid arrest and legal action, you are instructed to call them back immediately. When you call, they demand you pay a "fine" by sending money via wire transfer or by purchasing gift cards and reading the numbers over the phone.

Advance to slide 11—Job Scam

Job scams often target individuals seeking employment, with scammers posing as recruiters or representatives of legitimate-sounding companies.

Example: You apply for a remote "Data Entry Clerk" position online. A "hiring manager" quickly contacts you, conducts a brief interview over a messaging app, and offers you the job. To begin, they inform you that you must purchase a new laptop and specific software through their "preferred vendor" to ensure compatibility. They promise you'll be reimbursed in your first paycheck. After you pay the "vendor," the hiring manager and the job offer disappear.

Advance to slide 12—Affinity Scam

Affinity fraud is a scam in which a scammer takes advantage of the trust and shared interests within a specific group, such as a religious, ethnic, or social community, to carry out fraudulent schemes.

Example: A long-standing, respected member of a local church or social club introduces a "can't-miss" investment opportunity to the group. They claim it is an exclusive real estate deal available only to community members and promises high, guaranteed returns. Because the recommendation comes from a trusted friend within their shared social circle, several members invest their savings without doing proper research, only to discover later that the entire investment was a scam run by their "friend."

Discussion Prompts

How can you use this information to empower you?

LESSON

SPOTTING RED FLAGS

Duration: 5 minutes

Key Messages

- Recognizing the red flags is a critical skill.

Advance to slide 13—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.”

Advance to slide 14—Pause

“So, what's the single most important thing you can do? It's simple: PAUSE.”

“If you get a message or call that makes you feel rushed, pressured, or suspicious in any way, just stop. Hang up the phone. Don't click the link. Don't reply to the text.”

“Instead, verify the situation through an official channel. If you get a suspicious email from your financial institution, don't click the link in the email. Open a new browser window, go to your financial institution's official website, and check your account there. If you get a call from someone claiming to be from a government agency, hang up and call that agency back using the official phone number from their website.”

ACTIVITY

SCAM CHECKER COACH

Duration: 10 minutes

Key Messages

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

Advance to slide 15—Scam Scenario

Script

"Now let's try a hands-on activity. We are going to use the Banzai 'Scam Checker' Coach.

We will go through one example of a suspicious message together, and then you'll have time to work through a few scenarios on your own."

"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]

Advance to slide 16—Coach: Scam Checker

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.

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, direct attendees to the Scam Scenarios handout. Have them work through the remaining three scenarios, on their own, giving them 5-10 minutes. Then reconvene as a group to discuss the examples and red flags.

Continued from page 14

Discussion Prompts

“What are the red flags in example 2?”

- Plausibility: A small customs or redelivery fee is a common, legitimate occurrence.
- Impersonation: It claims to be from a well-known entity (USPS).
- Fake URL: The website address is designed to look official but is not the real USPS.com. The goal is to steal credit card information.

“What are the red flags in example 3?”

- Fear of Loss: It threatens the loss of a service many people use daily.
- Routine Action: Updating billing information is a normal task, making people less suspicious.
- Credential Theft: The goal is to get the user to enter their login and password, and then their credit card information, on a fake site.

“What are the red flags in example 4?”

- Intimidation: It threatens to turn off a critical utility like electricity.
- Extreme Urgency: The "2 hours" deadline is designed to create panic.
- Unusual Payment Method: This is the biggest red flag. A legitimate utility company will never demand payment via Zelle, gift cards, or a prepaid debit card.

LESSON

BUILDING YOUR DIGITAL DEFENSE

Duration: 10 minutes

Key Messages

- Strong, unique passwords and Multi-Factor Authentication (MFA) are your most powerful defenses.
- Security is a combination of technology and good habits.

Script

Advance to slide 17—Your Digital Defense

"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. This is a software application that securely stores, manages, and autofills your passwords and other login details. It helps you create strong, unique passwords, store them in a secure digital vault, and access them from different devices without having to memorize them."

"Multi-Factor Authentication (MFA) is another tool to consider. 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 18—Digital Habits

"Beyond passwords, let's talk about daily habits."

"Whenever possible, use secure Wi-Fi. Be very careful on public Wi-Fi. Use a Virtual Private Network, VPN, for privacy. A VPN is a service that creates a secure, encrypted connection. It makes it harder to track your online activity and access your data. You can get subscriptions for a VPN service for around \$10 a month, and even less if you sign up for a longer-term plan."

"When it comes to using social media, make sure to review your privacy settings. A good rule of thumb is: If you wouldn't put it on a billboard, don't post it publicly."

"Offline protection is still crucial. Shred any documents with personal information, including receipts, financial statements, and credit card offers."

"Lastly, make sure to stay on top of software updates. Always keep your computer and phone software updated to patch security holes. Keep your operating systems, browsers, and antivirus software up to date."

Discussion Prompts

Do any of these digital defenses or digital habits stand out as a habit you need to work on?

ACTIVITY

PASSWORD STRENGTH TEST

Duration: 10 minutes

Key Messages

- A visual demonstration of password vulnerability can be very impactful.

Script

Advance to slide 19— Password Strength

“Think of a common password similar to something you’ve used in the past. Maybe password123 or fluffy2025. Let’s use a password-strength checker website to see how quickly these easy passwords can be cracked.”

Pull up a public, safe password-strength checker website, like security.org’s How Secure is my Password tool. Enter a few of the examples from attendees.

Next, demonstrate how a long, complex passphrase is significantly stronger.

Discussion Prompts

What was your reaction to seeing how quickly a common password can be cracked?

Based on the demonstration, what seems to be the most important factor in creating a strong password: its length or its complexity?

Thinking about your own habits, what is the biggest challenge that prevents people from using a unique, strong password for every single online account?

LESSON

YOUR EMERGENCY ACTION PLAN

Duration: 15 minutes

Key Messages

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

Script

Advance to slide 20-Emergency Plan

"Okay, we've spent a lot of time talking about prevention. But what if the worst happens? What if you get that notification from your financial institution, or you realize a sensitive account has been compromised?"

"The moments after you discover a breach are critical. Acting quickly and in the right order can save you months of headaches and thousands of dollars. Panicking is a normal reaction, but having a clear plan is the antidote to panic. For the next few minutes, we are going to walk through that plan step-by-step. This is your emergency action plan."

"First, Contact Your Financial Institutions. This means immediately calling the fraud department for any financial institution or credit card company where you know fraudulent activity has occurred. Use the phone number on the back of your card or from their official website—never from a suspicious email. Tell them you are a victim of fraud, and they will lock the affected accounts and cards and begin their investigation."

"Second, Change Your Passwords. Start with the account that was compromised. Then, and this is crucial, you must change the password on *every other account* that used the same or a similar password. This is why using a password manager and unique passwords for each site is so important. Criminals know that people reuse passwords, and they will immediately try the stolen password on your email, social media, and other financial accounts."

"Once you've stopped the immediate damage, your next priority is to protect your name and your credit from future harm. This is where you lock down your credit profile."

"You have two main tools for this: a Fraud Alert and a Credit Freeze. A fraud alert is like putting a note in your file that tells lenders to take extra steps to verify your identity before opening a new account. It's good, but a Credit Freeze is much stronger."

"The final step is to create an official record of the crime. This is essential for recovery and for resolving any disputes down the road."

"Your first and most important stop is IdentityTheft.gov. This is the official resource from the Federal Trade Commission (FTC). Filing a report here is critical because it will provide you with a personalized recovery plan and an official affidavit that proves you are a victim."

"You should also file a Local Police Report. While local police may not be able to investigate every case, having a police report provides an extra layer of documentation. Your FTC affidavit will make this process much smoother."

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. This is a document you can take home and put somewhere safe."

"Now, looking at these three major steps—Contain, Protect, and Report—I want to open it up for a brief discussion."

Discussion Prompt

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

Facilitate the discussion, affirming that while all steps are crucial, the speed of "Containing the Damage" often has the biggest impact on limiting the financial and logistical fallout.

WRAP UP

& CONCLUSION

Duration: 10 minutes

Key Message

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

Script

Advance to slide 21—What We Learned

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

- "Be Skeptical: Scammers rely on you acting quickly without thinking."
- "Mind Your Digital Footprint: Be aware of where you are leaving an information trail online."
- "Build Your Defenses: Strong passwords and MFA are your digital seatbelts."
- "Pause Before Acting: Don't let scammers get into your head. Pause and think rationally before reacting to any texts, calls, or emails that could be from fraudsters."
- "Follow the Plan: If you suspect a problem, use the emergency action plan immediately."
- "Practice good habits: Take precautions to protect your data and identity online and offline."

Advance to slide 22—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."

"Any final questions before we close?"

Advance to slide 23—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 24—Contact Info

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