



YOUR LOGO HERE

Protect Your Digital Identity

A Guide to Cybersecurity and Fraud Prevention



PRESENTED BY:



\$10.3 billion

The amount of money lost to fraud by Americans

01

Introduction

02

Your Digital Footprint

03

Understanding the
Threats

04

Spotting Red Flags

05

Coach: Scam Checker

06

Building Your Digital
Defense

07

Password Strength
Test

08

Your Emergency
Action Plan

09

Conclusion & Personal
Action Plan

Agenda

What we'll discuss today

Your digital footprint



The goal of a scammer is simple:
to get your money and personal
information.



Malware

What it is: Malicious software that can infiltrate networks & steal info

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.

Phishing

What it is: Attempts to deceive people into revealing sensitive info

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.

Impersonation Scams

What it is: Scammers pretending to be someone else, like a trusted entity

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.

Tech Support Scams

What it is: Fraudsters pose as technical support 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.

Government Imposter Scams

What it is: Scammers falsely claim to represent government agencies.

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.

Job Scams

What it is: Scammers target people seeking employment.

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.

Affinity Scams

What it is: A scammer takes advantage of the trust within a specific group.

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."

Spotting *Red Flags*

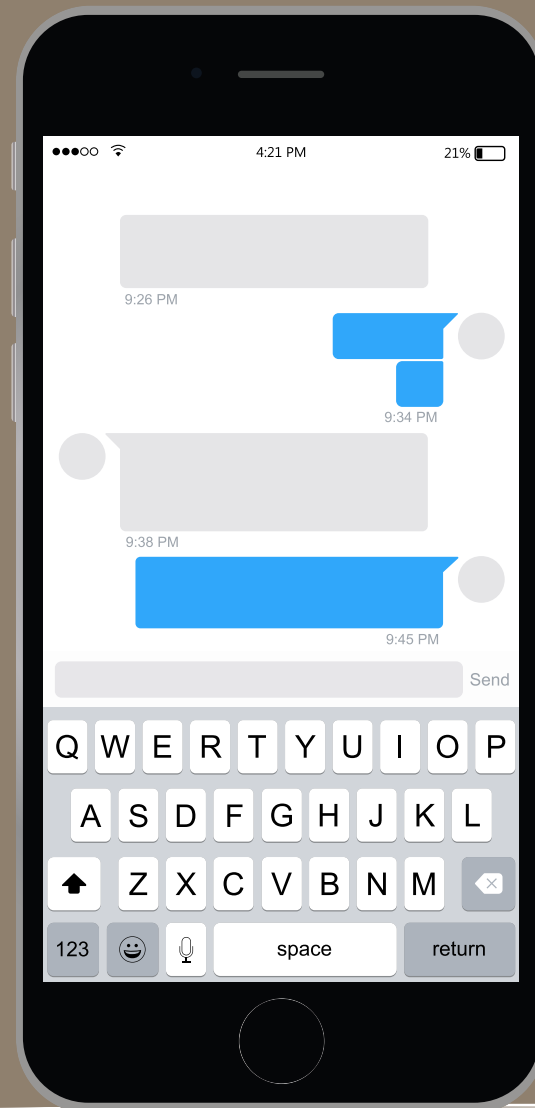
- Pressure to act quickly
- Requests for sensitive information
- Requests for payments in unusual ways
- Offers that seem too good to be true





What's the most important
thing to do?
Pause.

Scam Scenario



(Your Bank 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]



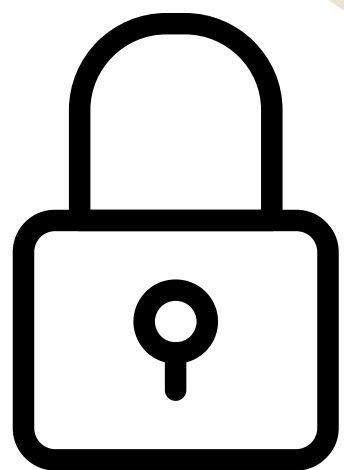
Coach: Scam Checker

yoursubdomain).banzai.org/
wellness/resources/
scam-checker-coach

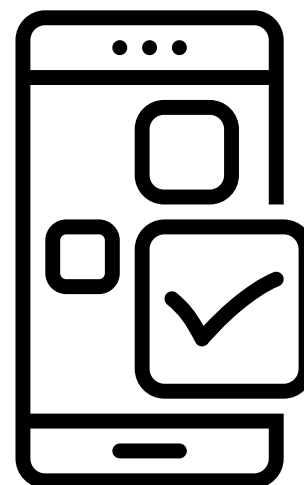


YOUR LOGO HERE

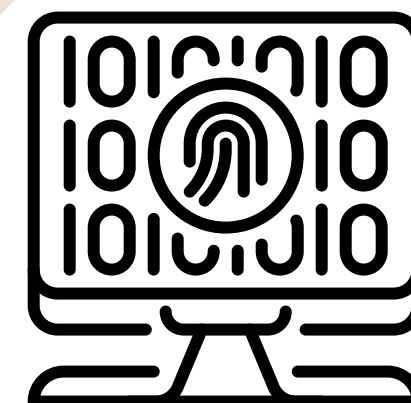
Your Digital Defense



**Password
Best Practices**



**Password
Manager**



**Multi-Factor
Authentication**



YOUR LOGO HERE

Your Digital Habits



Secure Wi-Fi



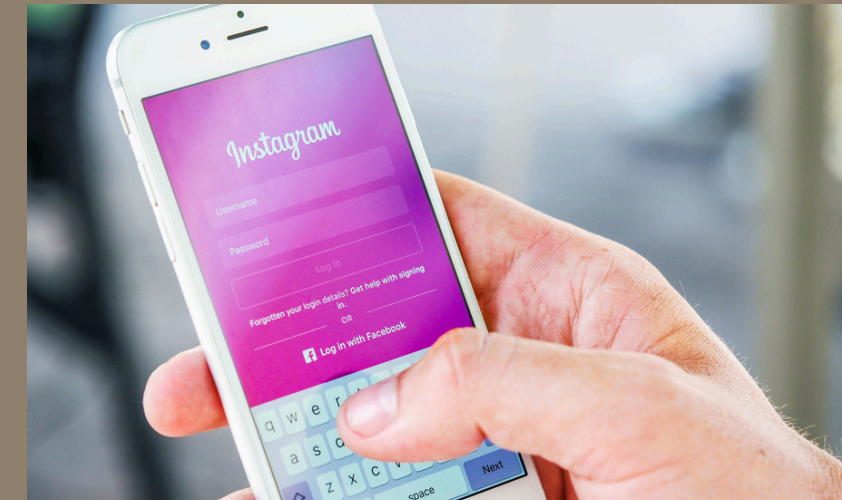
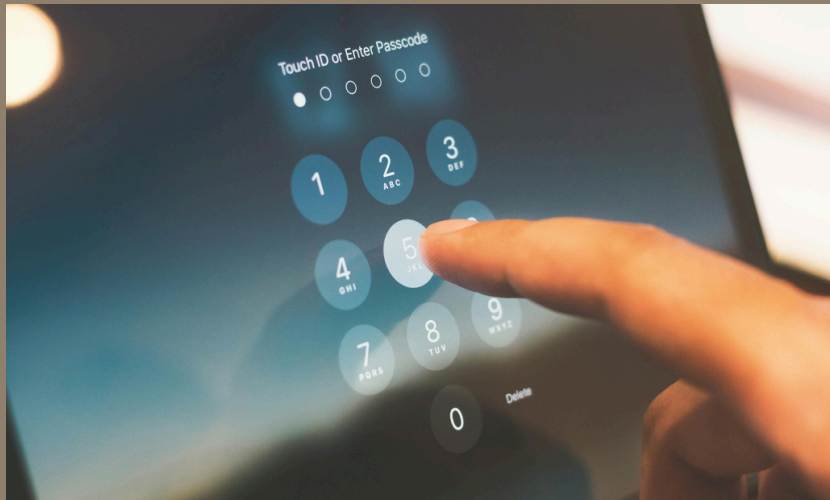
**Social Media
Privacy
Settings**



**Offline
Protection**



**Software
Updates**



Password Strength Test



Your Emergency Action Plan



1. Contact Your Financial Institutions
2. Change Your Passwords
3. Add a Fraud Alert
4. Freeze Your Credit
5. Report the Crime

What we learned

Be skeptical

**Pause before
acting**

**Mind your
digital
footprint**

**Build your
defenses**

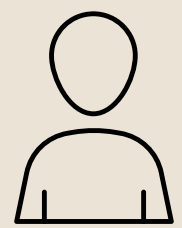
**Follow the
plan**

**Practice good
habits**



Your Personal Action Plan

Additional Resources



Digital Wellness Assessment

Find out how your use of technology is impacting you and what you can do about it.



Preventing Identity Theft

Stay alert against fraud and stay ahead of scammers and thieves.

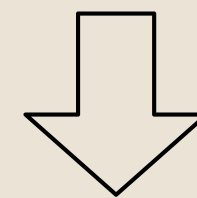
***Find these resources and more in our
Wellness Center:***

(yoursubdomain).banzai.org/wellness/



Coach: Workplace Cybersecurity

Learn how you can protect your company, and yourself, from common online threats.



Protect Yourself Online

Learn the basics of cybersecurity.



YOUR LOGO HERE

Thank you!

Call us

123-456-7890

Email us

hello@reallygreatsite.com

Visit our website

www.reallygreatsite.com

