Internet Society



Anti-Scam Initiative

Scam Strong Curriculum

September 2026

With support from Google.org

Background

This curriculum is part of the Internet Society's Anti-Scam Initiative, a global effort to ensure that people everywhere have an Internet experience that is safe, secure, and protects them online. Find out more about the Internet Society's Online Trust and Safety Hub here. This curriculum was developed with Google.org's support, and some content was adapted with permission from Google's Safety & Security resources.

Purpose

This curriculum is designed to support trainers in building and delivering engaging, in-person training sessions that help participants understand, prevent, and respond to online scams. The overall goal is to move participants beyond awareness and equip participants with practical skills and habits to avoid scams and navigate digital environments safely.

Intended users of the curriculum include community organizations, local law enforcement, high school teachers, and others working with participants who are vulnerable to online scams (e.g. youth, older populations, the newly online, etc.) This curriculum is designed to train everyday digital users, ranging from adolescents to adults, with no specialized technical knowledge. It is intended for a diverse, global audience, reflecting a wide range of cultural, educational, and socioeconomic backgrounds.

The unifying goal is to help individuals and communities become 'Scam Strong.'

Learning Objectives

To support participants in becoming Scam Strong, this curriculum targets three learning outcomes:

Conceptual understanding: Help participants develop a clear understanding of how online scams operate, how to identify them, how to prevent them, how to respond in the event of a scam, and how to support others in the community.

Individual and group reflection: Encourage participants to recognize their own behaviors, assumptions, and potential vulnerabilities to online scams.

Real-Life application and behavior change: Equip participants with practical strategies and habits they can apply immediately to reduce risk and respond effectively to online scams.

Curriculum

The curriculum consists of five modules, each of which covers the following topics:

Module 1: Understand: Know how and why scams work

Module 2: Identify: Change behavior to spot scams

Module 3: Prevent: Proactively reduce scam risk

Module 4: Respond and Report: Act quickly when something goes wrong

Module 5: Support: Support victims and Scam Strong communities

Training Format and Requirements

Format

This curriculum is designed for in-person delivery. (NOTE: you can find an online delivery version of the curriculum here.)

Presentations: Provide foundational knowledge, introduce key concepts, and frame the learning objectives. They combine lecture-style presentations with discussion questions.

Group activities: Enable participants to understand and apply concepts through discussion, problem-solving, and shared learning.

Individual activities: Encourage personal reflection and action planning, helping participants translate learning into concrete behavioral changes.

This curriculum is modular and customizable.

This means that the curriculum is broken into independent units that can be mixed and matched, allowing trainers to adapt the training based on audience needs and time available. Trainers can select from a range of delivery formats, including interactive presentations and discussions, group activities, and individual exercises, to create a tailored, engaging, and contextually relevant learning experience.

Time available: Short sessions may focus on one or two modules, while longer sessions can cover the full Scam Safe framework.

Audience needs: Adjust content depth and delivery formats depending on participants' familiarity with digital tools, risk exposure, and learning preferences. Trainers can also choose to prioritize and deliver specific modules (e.g., Identify, Prevent), depending on the needs of their audience.

Module	Time (Minutes)	Description	Page Number
Module 1: Understand			
1.1 Presentation and Discussion	30	Participants learn the scale of the problem, the types of scams online, as well as how online scams work.	6
1.2 Group Activity: Scam Story Deconstruction	35	Participants work in groups to deconstruct a fictional scam victim's experience, including (a) the type of scam being described, (b) the state of mind of the scam victim, (c) the manipulation tactics employed by the scammer, and (d) the attack channels used in the scam.	11
1.3 Individual Activity: My Scam Risk Reflection	20	Participants reflect on their own vulnerabilities so they are more self-aware when they encounter scams in the future.	25
Module 2: Identify			
2.1 Presentation and Discussion	30	Participants learn the ways to identify online scams.	29
2.2 Group Activity: Be Scam Ready	30	Participants work in small groups to play Google's 'Be Scam Ready' game (https://bescamready.withgoogle.com/).	31
2.3 Individual Activity: Spot the Red Flags	15	Participants complete the 'Spot the Red Flags' worksheet, trying to identify all the various red flags contained in example messages.	32
Module 3: Prevent			
3.1: Presentation and Discussion	30	Participants learn ways to prevent scams and improve online safety.	36
3.2 Group Activity: Secure This Scam Target	35	Participants work in small groups to identify prevention actions that might have helped a fictional scam target avoid getting scammed, or lessen the scam's severity.	39
3.3 Individual Activity: My Scam Strong Checklist	20	Participants identify various steps that they can commit to implementing in the next week that will help protect them from scams.	41
Module 4: Respond and Report			
4.1 Presentation and Discussion	30	Participants learn ways to respond to and report scams if they happen.	44
4.2 Group Activity: What Should I Do Next?	25	Participants work in small groups to identify things that a fictional scam victim can do to respond to an online scam, report the incident, and gather evidence of the event.	46
4.3: Individual Activity: My Personal Response Plan	15	Participants build a personal response plan in the event that they were to become victims of an online scam.	49
Module 5: Support			
5.1 Presentation and Discussion	30	Participants learn ways to support victims and build Scam Strong communities.	53
5.2 Group Activity: How to Be a Scam Strong Champion	30	Participants work in small groups to discuss how fictional 'Scam Strong champions' helped people in their community prevent and respond to scams.	55
5.3 Individual Activity: Who Can I Help?	15	Participants identify people within their community who might be particularly vulnerable to scams, along with concrete action they can take to support them.	60

Participants:

Each session is designed for approximately 25 participants. Trainers should be aware that some participants may be victims of scams in the past. If applicable, trainers should offer to connect these participants to support organizations in the relevant country.

Setting and Materials

This curriculum is designed for delivery through in-person training sessions. The training requires a facility with a large room to accommodate all participants, along with access to breakout spaces or flexible seating to accommodate small group discussions in the main room.

Required Materials Include:

- Access to a printer for preparing activity handouts
- A screen or projector for slide presentations
- Internet-enabled devices (e.g., phones, tablets, laptops) for participants, where available
- Low-connectivity modifications: The curriculum includes alternative content and approaches that are appropriate for low-connectivity settings.

Country-Specific Customization

At various points, this curriculum provides information on how the course content and activities can be customized to the needs and local realities of a relevant country/regional context. Look for the 'customization' boxes to get suggestions on how to find locally-relevant data and information that can be incorporated into the course, as well as guidance on how to adapt the content when relevant.

Additional Resources:

Trainers can find links to reports, blog posts, data sources, global campaigns, and other resources on page 63.

Module 1: Understand



1.1 Presentation and Discussion

Time: 30 minutes

Description: Trainers deliver a short, interactive presentation that introduces the scale of the problem, the types of scams online, as well as how online scams work. The trainer pauses regularly with questions to prompt discussion. Trainers can use the content and discussion questions from the 'Content and Resources' section included below to develop their presentations.

Logistics:

- **Format:** Instructor-led, whole group (25 participants)
- **Materials needed:** Slides (including prompt questions for group discussion)

Content and Resources:



Presentation Part 1.1.1 Introduction

Agenda: Trainers introduce course agenda found on page 4.



Customization:
Trainers use the 'Format' section to build an agenda (see page 3 for instructions)

The Scale of the Problem

- Online scams are a global problem affecting people of every age, income level, and background.
- Scams threaten millions of people around the world every day.
- Online fraud costs consumers hundreds of billions of dollars each year.
- In many countries, scams are among the most commonly reported crimes.
- The majority of scams go unreported due to embarrassment, fear, or uncertainty about where to turn.
- Scams are increasingly sophisticated due to new tools like generative AI. They are becoming faster, more personalized, and harder to distinguish from legitimate communication.
- Scams do not just affect certain people, they affect everyone.

Customization:

Trainers include up-to-date statistics on the severity of scams both globally and in the relevant country/regional context. These statistics are changing all the time. Possible resources:

Global Anti-Scam Alliance (GASA) Knowledge Base McAfee: State of the Scamiverse 2025

Presentation Part 1.1.2 Scam Types

Scam Types:

Investment scams: Scammers trick people into investing money by promising high or guaranteed returns with minimal risk. They use fake platforms, cryptocurrency schemes, or impersonate financial advisors to build trust.

Shopping and travel scams: Scammers create fake online stores, counterfeit goods, or fraudulent travel deals. They often use social media ads or spoofed websites to appear legitimate. Victims pay for products, tickets, or accommodation that never arrive or do not exist.

Unexpected money scams: Scammers claim that targets have won a prize, inherited money, or are entitled to a refund or benefit. To receive the funds, scammers ask targets to pay fees, taxes, or provide personal information. The promised money never arrives.

Government and business impersonation scams: Scammers pose as trusted institutions such as tax authorities, police, banks, or well-known companies and pressure targets into sending money or sharing sensitive information. They create urgency by claiming that people owe money, that their account is at risk, or that legal action is pending.

Family or friend impersonation scam: Scammers pretend to be a family member or friends in distress. They claim to be injured, arrested, or in urgent need of funds. Targets often feel panic and emotional pressure, so they bypass verification. These scams are also known as “emergency” scams.

Job offer scams: Scammers pose as recruiters and advertise fake jobs with attractive salaries or remote work opportunities. They ask targets to pay application fees, purchase equipment, or share personal data. In some cases, scammers use targets to move stolen funds.

Business email compromise (BEC) scam: Scammers impersonate executives, suppliers, or partners to request that businesses pay urgent invoices or change their banking details.

Romance scams: Scammers build emotional relationships online through dating platforms or social media. Over time, they create a crisis—such as medical bills or travel costs—and ask targets for financial help. Scammers often manipulate targets over weeks or months across platforms before requesting money.

Charity scams: Scammers exploit natural disasters, conflicts, or humanitarian crises by posing as charitable organizations. They pressure people to donate quickly, often through unverified links or payment methods.

Threats and extortion scams: Scammers use intimidation to demand money or information. Scammers threaten to release private images, claim to have hacked devices, or accuse targets of illegal activity. The pressure purposefully creates fear and prompts immediate payment.

Customization:

Trainers include information about the most common scam types in the relevant country/ regional context.

Discussion Questions:

- What do you think are the most common scam types in our country/region? Why is that?
- Who do you think might be most vulnerable to these types of scams?

Presentation Part 1.1.3 State of Mind

State of Mind: Why Does Your State of Mind Matter?

Scammers take advantage of psychological and behavioral vulnerabilities when targeting people.

Overconfidence: People believe they would never fall for a scam—especially if they are tech-savvy or financially experienced. Scammers rely on this confidence. When people assume they are too knowledgeable to be deceived, they skip important steps such as double-checking information.

High trust: People generally trust friends, family, institutions, or messages that look familiar. Scammers copy trusted brands, government agencies, and individuals because they know that trust lowers a person's guard. Scammers know that people are less likely to question messages that feel official or friendly.

Impulsivity: Scammers know that people act quickly when something seems urgent or exciting. Flash sales, limited-time investments, or emergency messages intend to push people into fast decisions.

Emotional state: When people are stressed, lonely, afraid, or excited, it's harder to think clearly. Scammers create emotional highs (romance, winnings) or lows (threats, emergencies) on purpose. Strong emotions can override people's usual caution.

Mental overload: When people are busy, distracted, or overwhelmed, they are more likely to miss small red flags. Scammers often make contact when people are multitasking or dealing with complex tasks, hoping that potential targets won't slow down to verify what's happening.

Financial dissatisfaction: Scammers exploit financial pressure by presenting risky or fake solutions as easy fixes. If people are worried about money or looking for new opportunities, an offer of quick income or guaranteed returns can feel especially appealing.

Discussion Questions:

- What do you think is a more important factor in people's vulnerability to online scams: their age, their education level, or their state of mind when they encounter a scam?

Presentation Part 1.1.4 Manipulation Tactics

Manipulation Tactics: How Do Scammers Manipulate You?

Scammers use powerful persuasion tactics to push people into acting.

Fear: Fear can shut down rational thinking and make people comply quickly. Scammers tell a potential target that something bad will happen if they don't act immediately—their account will close, private information will be exposed, authorities will arrest them, or a loved one will be in danger.

Urgency: Urgency prevents people from pausing to verify a scammer's request. Scammers tell people that they must act now—within minutes or hours—or they'll lose money, an opportunity, or face consequences.

Curiosity: Curiosity gets people to engage before they have assessed the risk. Scammers play on natural curiosity—a prize win, an unexpected refund, a suspicious login alert. Scammers are hoping that potential targets will click because they want to know more.

Emotional connection or compassion: Scammers play on people's desire to build a connection with someone who seems kind, attractive, or in need. They know that emotional connection makes requests feel personal and harder to refuse.

Scarcity and fear of missing out ('FOMO'): Scarcity makes risky opportunities feel valuable. Scammers tell people that an offer is exclusive or available for a limited time. Scammers also use current events—like a natural disaster—to pressure targets into acting fast so that they don't miss out on a chance to make a donation.

Social proof: When others seem to trust something, potential targets are more likely to trust it too. This is why scammers use fake testimonials, online reviews, celebrity endorsements, or messages that appear to come from colleagues or friends.

Escalating requests: Scammers often start small, then escalate requests once people are emotionally or financially invested. After they invest time, share personal information, or send a small payment, people feel committed.

Authority and legitimacy: Scam messages often appear to come from someone with power—a government agency, bank, employer, or senior executive. Authority makes demands feel official and harder to question.

Social obligation: Scammers exploit people's desire to be polite, cooperative, or respectful, especially to members of their family or community. They may pressure someone to respond because "it's the right thing to do," or because refusing would seem rude or selfish.

Discussion Questions:

- Which manipulation tactics do you think are most effective in getting people to act quickly without verifying? Why?

Presentation Part 1.1.5 Attack Channels

Attack Channels: How Do Scammers Reach You?

Scammers meet potential targets on the platforms and devices that they use every day. Many scams combine more than one attack channel.

Common channels scammers use:

- **In person:** Not all scams happen online. Scammers might watch potential targets as they enter a PIN (shoulder surfing), steal an unlocked device, or leave behind an infected USB drive.
- **Email:** Scammers send messages that look like invoices, account alerts, delivery notices, or requests from a boss or bank. The email contains a malicious link or attachment, or asks people to change payment details. Once targets click or respond, scammers try to steal credentials or redirect payments.
- **Messaging and chat apps:** Texts or messages on platforms like WhatsApp, Telegram, or Facebook Messenger include urgent requests, fake job offers, delivery problems, or links to "verify" accounts. Because these messages feel personal and informal, potential targets are less cautious than with email.
- **Social media platforms:** Scammers create fake profiles, post malicious ads, or send direct messages pretending to be recruiters, investors, romantic partners, or customer support. They also leave scam links in comments under popular posts to reach large audiences quickly.
- **Phone calls:** Scammers make calls that appear to come from banks, the police, or a government agency. They can spoof caller ID to look legitimate. Scammers can hijack or spoof Internet-based phone or voice-over-IP (VoIP) systems. The scammer pressures potential targets to share codes, move money, or provide sensitive information during the call.
- **Mobile apps:** Scammers design apps to look like trusted tools—banking apps, cryptocurrency wallets, shopping platforms, or security software. Once installed, these apps can steal data, monitor activity, or redirect payments.
- **Websites:** Scammers build fake online stores, cloned login pages, and lookalike banking sites to capture passwords and payment details. Scammers drive traffic to these sites through ads, search results, or links in messages.
- **Online payment and financial platforms:** Scammers ask potential targets to send money through a payment app, wire transfer, gift cards, or cryptocurrency. Some scams use fake payment portals or fraudulent cryptocurrency exchanges that disappear once funds are deposited. Payments that victims send this way are often difficult to recover.

Customization:

Trainers mention specific messaging apps that are most commonly used in the relevant country/regional context (e.g., WhatsApp, Signal, Telegram, LINE, Kakaotalk, Viber).

Discussion Questions:

- Why do some scammers use multiple communication channels and move between them (e.g., social media, messaging apps, payment platform) instead of staying in one place?
- Do you think some attack channels are more common in low connectivity settings vs high-connectivity settings?

1.2 Group Activity: Scam Story Deconstruction

Time:

35 minutes (20 minutes small group discussion + 15 minutes debrief discussion)

Description:

Participants work in small groups of 3-5. Each group is assigned two different scam target persona videos from the Internet Society's Digital Toolkit. They then have to choose the cards (see print-ready cards on page 23) that match each story with (a) the type of scam being described, (b) the state of mind of the scam victim, (c) the manipulation tactics employed by the scammer, and (d) the attack channels used in the scam. Groups discuss their reasoning for each choice. Repeat the process for a second persona.

Customization:

When choosing which scam target personas to use, trainers prioritize the scams that are most common in the relevant country/regional context.

In low-connectivity settings: print out scam target persona cards found on pages 13-22.

Debrief:

Each small group chooses one of their personas to describe to the wider group, and then provides a 'story deconstruction' to the wider group: summarize the persona, and describe to the group why it worked:

- What was the victim's state of mind?
- What manipulation tactics were used?
- How did the scammer reach them?

Logistics:

- **Format:** Small groups of 3-5
- **Materials needed:**
  - Personal laptops/phones/tablets to access persona videos OR printed persona cards for low-connectivity settings (see print-ready persona cards on pages 13-22), one copy per group
  - Printed cards of different scam types, states of mind, manipulation tactics, and attack channels (see print-ready cards on page 23), one copy per group

---

Content and Resources:

Print-ready cards: Scam Strong target personas

Instructions: For low-connectivity settings: Print one copy of each of the 10 Scam Strong target personas, one per page (one-sided printing only)

MEET DANIEL



42 | United Kingdom
Mid-level IT manager

Background: Married with two children. Recently received a modest inheritance and has been looking for ways to grow his savings faster than traditional bank interest rates.

Daniel prides himself on being tech-savvy. But lately, he'd been frustrated with low returns on his savings—and juggling work and family left little time to research investments carefully.

A sponsored social media ad caught his eye: a limited-time crypto currency opportunity with glowing testimonials and "verified" results. His friend recently invested in cryptocurrency and has been encouraging Daniel to look into it too. The website looked professional and early dashboard profits made it feel real.

The scammers encouraged Daniel to "act now" to guarantee high returns on his investment and exclusive access to the investment opportunity. They then moved the conversation to a private messaging app and guided him to transfer funds through a cryptocurrency platform.

When Daniel tried to withdraw his money, the site disappeared.



MEET AISHA



58 | Saudi Arabia Retired school administrator

Background: Saving for years to perform Hajj with her sister. Active on Facebook and WhatsApp groups that share religious travel advice and community updates.

She's 58 and has dreamed for years of performing Hajj. This year, she finally feels financially ready. When she sees posts in a community Facebook group about a "last remaining" Hajj package at a discounted rate, she feels hopeful—and relieved.

Several people in the comments thank the travel agency and say they've already secured their spots. The website looks polished, with official logos and photos of pilgrims in Mecca. Aisha doesn't want to miss the opportunity, and packages are "almost sold out."

She messages the company through WhatsApp. The representative responds quickly, warmly, and professionally, explaining that demand is unusually high and payment must be completed within 24 hours to guarantee her visa and accommodation.

Wanting to secure her place—and trusting what appears to be a legitimate travel agency that others recommend—Aisha transfers the deposit through an online payment link.

Weeks later, her confirmation documents stop arriving. The website disappears. The WhatsApp number no longer works.



MEET EMRE



35 | Türkiye
Sales representative for a construction supply company

Background: Married, one young child. Recently feeling financial pressure due to rising living costs. Frequently checks email on his phone between client visits.

He's 35 and constantly on the move for work. Lately, money has felt tight. So, when he receives an email saying he is entitled to a large refund from his go-to e-commerce platform, it grabs his attention.

The message looks official—complete with logos, a reference number, and formal language. The email warns that he must process a claim within five days, or he forfeits the funds.

Curious—and hopeful—Emre clicks the link. The website shows a balance in his name and prompts him to pay a small "processing fee" to release the transfer. The amount seems minor compared to the payout.

He enters his credit card details.

Shortly after, additional charges appear. The promised refund never arrives. The website stops loading.



MEET SIOBHÁN



51 | Ireland
Owner of a small logistics company

Background: Runs the business with a small team outside Cork. Handles payroll, supplier payments, and tax filings herself. Known for being organized and careful, but currently juggling compliance deadlines and staffing shortages.

She's 51 and manages all the operations of her logistics company. Lately, she's been stretched thin—a driver is out sick, fuel prices are rising, and tax filing deadlines are approaching.

One afternoon, she receives a phone call that appears to come from the national tax authority. The caller knows her business name and registration number. He explains there's a discrepancy in her latest tax filing and warns that enforcement action could begin within hours.

Her heart races. She has always paid on time.

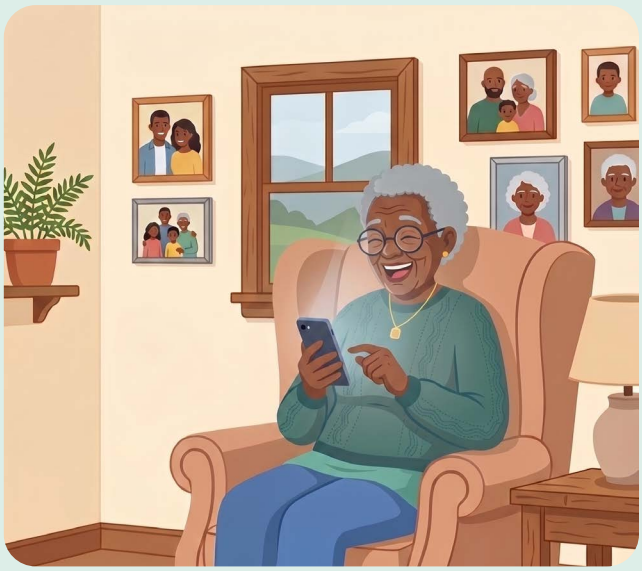
The caller says the issue can be resolved immediately if she confirms company details and makes a same-day payment to avoid penalties. His tone is calm but firm, as if he's doing her a favor.

Wanting to protect her business—and under pressure to fix the problem quickly—she clicks the link that the caller sends her through text and follows the instructions.

Later, when she contacts the tax office to confirm that the payment went through, she learns there was no issue at all. The money she paid is gone.



MEET MARGARET



74 | United States
Retired nurse

Background: Widowed, lives alone in Georgia. Close to her two grandchildren, who live in another state. Uses Facebook to stay in touch and has recently started using text messaging more regularly.

She's 74 and retired. She may not be the most tech-savvy, but she uses her phone to text and call her family and checks her family's social media posts regularly for updates on her grandchildren.

Late one evening, she receives a text message from an unfamiliar number. "Grandma, it's Ethan. I'm in trouble. Please don't tell Mom and Dad."

Her heart pounds. The message says he's been in a minor accident while traveling and needs money wired immediately to cover legal fees. He's embarrassed. He begs her not to call his parents.

The conversation moves quickly. The person texting knows Ethan's name, where he goes to university, even details about a recent trip.

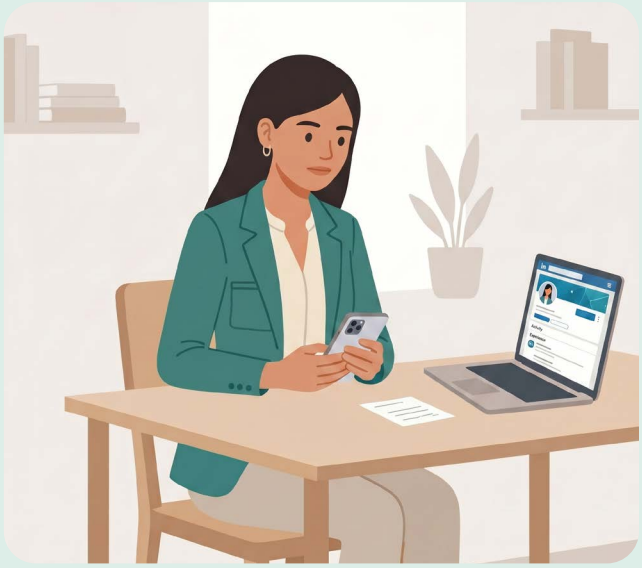
Margaret doesn't want to delay. What if he's scared? What if he's alone?

She drives to a nearby store and sends money through a wire transfer service.

The next morning, she calls her daughter and learns Ethan is back home and had no issues with his trip.



MEET CARLA



24 | Philippines
Recent university graduate in marketing

Background: Actively searching for remote work to support her family. Spends hours each day on LinkedIn and job platforms. Eager to secure stable employment quickly.

She's 24 and determined to land her first professional job. After months of applications and interviews that went nowhere, she's starting to feel discouraged.

Then a recruiter reaches out to her on a popular job site. The message praises her profile and says she's been shortlisted for a remote marketing role with an international company. The salary is higher than she expected. The recruiter says they're moving quickly and want to secure top candidates before the position closes.

The interview happens over a messaging app. The questions are simple. Within a day, she's told she's hired.

She's asked to download a company app to complete onboarding and pay a small fee for equipment delivery, which will be reimbursed with her first paycheck.

It feels like everything is finally falling into place.

After she sends the payment and uploads her ID documents, the recruiter disappears. The app stops working. The company never existed.



MEET ADRIAN



39 | Singapore
Finance manager at a mid-sized manufacturing company

Background: Oversees vendor payments and payroll. Known for being precise and risk-aware. Recently managing a system migration to a new cloud-based accounting platform while closing out quarterly reports.

He's responsible for ensuring millions of dollars in supplier payments go out on time. This week is especially intense—quarter-end reporting and a new accounting system rollout are happening simultaneously.

He receives an email that appears to come from the company's CEO. The tone is direct and confidential. The CEO explains that a strategic acquisition is underway and requires an urgent wire transfer to a partner account. Because of the sensitivity, he tells Adrian not to discuss it with others.

The email signature looks correct. The writing style feels familiar.

Adrian hesitates briefly but doesn't want to be the one who delays a major transaction. He processes the transfer through the company's online banking portal.

Later, when he mentions the acquisition in a meeting, confusion spreads across the room.

The CEO never sent the email. Adrian has already moved the funds overseas.



MEET LUCIANA



47 | Brazil
Small business owner

Background: Divorced, two teenage children. Active on Facebook and Instagram. Recently started using a new dating app after encouragement from friends.

She's 47 and hasn't dated seriously in years. When she matches with an American engineer, Karl, on a dating app, the conversations feel easy and thoughtful. He sends long messages every morning and seems genuinely interested in her life.

They soon start messaging on WhatsApp and even send short voice messages back and forth. After a couple of months, Karl talks about visiting Brazil to meet Luciana in person, and shares screenshots of various flight options.

Then a problem arises. The airline wouldn't accept Karl's credit card, so he asks if she could transfer some money to his bank account to purchase the flight. It's a temporary hold on his account, so things should get sorted out within days, if not hours. He promises to repay her as soon as possible.

Luciana hesitates. But she knows him well enough to trust him and sees that he's embarrassed to ask for help. After she transfers the money, he sends what looks like official ticketing information and receipts. He's bought the tickets, and he'll be in Brazil soon!

Soon after, the messages slow, and then stop entirely.



MEET DAVID



33 | Kenya
Bank customer service officer

Background: Active in his church and local community groups. Regularly donates to disaster relief efforts and shares fundraising links on social media.

He's 33 and believes strongly in helping others. When devastating floods hit a neighboring country, he sees a wave of donation appeals across social media.

One post stands out. It includes photos of people waiting in line for food, a logo resembling a well-known humanitarian organization, and comments from people saying they've already contributed. The message urges immediate donations, warning that "every hour counts."

David clicks the link. The website looks professional and displays a live donation tracker rising rapidly.

He feels compelled to act quickly—before scrolling past and forgetting—so he enters his card details and donates.

Moments later, he receives a confirmation email. But weeks pass, and he never sees updates about the campaign. When he searches for the organization independently, he can't find it.

The page has vanished.



MEET TOMASZ



22 | Poland
College student

Background: Lives in Warsaw. Confident online, comfortable with technology. Uses public Wi-Fi in cafés while doing his college assignments.

One morning, he opens his laptop and finds an email with his own password in the subject line.

The sender claims to have hacked his computer. The email says that, unless he makes a payment via cryptocurrency within 48 hours, they will send all his private text messages—including the ones he sent to his fiancée—to everyone in his contacts list.

The email includes technical language and references to his device, making it feel credible. A countdown timer is embedded in the message.

Tomasz knows scams exist—but seeing his real password shakes him. Tomasz also knows that he has re-used old passwords across multiple websites and accounts.

Panicked and worried about damage to his reputation, he transfers the cryptocurrency to the wallet address provided.

The message warns him not to contact authorities and not to ignore the threat.



Print-Ready Cards: Scam Types, State of Mind, Manipulation Techniques, Attack Channels

Instructions:

1. Print out five to eight copies of pages 23-24 (one-sided printing only), depending on the estimated number of three- to five-person small groups (one set of printouts per small group)

2. Cut out individual cards, sort them in small bags so that they can be easily distributed to small groups

Scam Types

Investment scam	**Shopping and travel scam**	**Unexpected money scam**	**Government and business impersonation scam**	**Family impersonation scam**
Job offer scam	**Business email compromise scam**	**Romance scam**	**Charity scam**	**Threats and extortion scam**

State of Mind

Over-confidence	**High trust**	**Impulsivity**
Emotional state	**Mental overload**	**Financial dissatisfaction**

Print-Ready Cards: Scam Types, State of Mind, Manipulation Techniques, Attack Channels

Instructions:

1. Print out five to eight copies of pages 23-24 (one-sided printing only), depending on the estimated number of three- to five-person small groups (one set of printouts per small group)

2. Cut out individual cards, sort them in small bags so that they can be easily distributed to small groups

Manipulation Techniques

Fear	**Urgency**	**Curiosity**
Emotional connection or compassion	**Scarcity and FOMO (fear of missing out)**	**Social proof**
Reciprocity and sunk cost	**Authority and legitimacy**	**Social obligation**

Attack Channels

In person	**Email**	**Messaging and chat apps**	**Social media platforms**
Phone calls	**Mobile apps**	**Websites**	**Online payment and financial platforms**

1.3 Individual Activity: My Scam Risk Reflection

Time:

20 minutes

Description:

Participants complete the 'My Scam Risk Reflection' worksheet (page 26). In this activity, they apply the four parts of the Understand module to their own lives. They identify which scam types they are most likely to encounter, when they may be more vulnerable based on their state of mind, which manipulation tactics might work on them, and which attack channels are most relevant to their everyday digital habits. The goal is to help participants understand their own vulnerabilities so they are more self-aware when they encounter scams in the future.

Note: This is a potential sensitive topic, intended for individual reflection only, not group discussion.

Logistics:

1. Format: Individual activity
2. Materials needed: Printed copies (one copy per participant) of the 'My Scam Risk Reflection' worksheet (page 26)

Content and Resources:

Instructions: Print copies of the 'My Scam Risk Reflection' worksheet, one copy per participant

My Scam Risk Reflection

Worksheet

Circle the scam types that you would be most vulnerable to at this moment in your life:

Investment scam	**Shopping and travel scam**	**Unexpected money scam**	**Government and business impersonation scam**
Job offer scam	**Business email compromise scam**	**Romance scam**	**Family impersonation scam**
Charity scam	**Threats and extortion scam**		

What roles/responsibilities do you have in your life that might make you a target (parent, job seeker, small business owner, caregiver, student, traveler, etc.)?

Check the scam types that you would most vulnerable to at this moment in your life:

- [ ] When I'm in the middle of a busy work day
- [ ] When my family might be at risk
- [ ] When I feel like I might lose money, overpay for something, or miss out on a good deal
- [ ] When I receive a message that looks like it's from a trusted organization (e.g., bank, employer, government)
- [ ] When I'm excited about an unexpected opportunity (e.g., prize, job offer, investment)
- [ ] When I feel social pressure to respond quickly (e.g., from a boss, colleague, or group)
- [ ] When something feels familiar or routine (e.g., invoices, bills, delivery notifications)
- [ ] When I'm communicating on informal channels (e.g., text or messaging apps) where I'm less cautious
- [ ] Other

Which manipulation tactics do you think would work best on you? Circle all that apply.

Fear	**Urgency**	**Curiosity**
Emotional connection or compassion	**Scarcity and FOMO (fear of missing out)**	**Social proof**
Reciprocity and sunk cost	**Authority and legitimacy**	**Social obligation**

Which channels do you use most often, where are you most likely to click quickly, respond without checking, or put yourself at risk?

In person	**Email**	**Messaging and chat apps**	**Social media platforms**
Phone calls	**Mobile apps**	**Websites**	**Online payment and financial platforms**

Module 2: Identify

2.1 Presentation and Discussion

Time: 30 minutes

Description: Trainers deliver a short, interactive presentation that introduces the ways to identify online scams. The trainer pauses regularly with questions to prompt discussion. Trainers can use the content and discussion questions from the 'Content and Resources' section included below to develop their presentations.

Logistics:

1. Format: Instructor-led, whole group (25 participants)
2. Materials needed: Slides (including prompt questions for group discussion)

Content and Resources:

Presentation Part 2.1.1 Take Your Time

Scammers rely on people making quick judgments and reacting without thinking. Take a little extra time and avoid rushing to click a link, respond to urgent requests, or make a purchase. Slowing down helps make better decisions and creates space to recognize potential scams.

Pause before acting
If an online offer or message creates pressure to act immediately, pause first. Messages that create urgency are often a warning sign. It is important to allow emails or text messages to sit before responding. Instead of clicking on suspicious links, hover over the link with a cursor to reveal the full web address (URL) and check whether it leads to a legitimate or potentially harmful website.

Be aware of your state of mind
Scammers often exploit emotions to lower a person's guard. Messages trigger fear, guilt, or excitement to prompt quick action. Recognize these emotional cues and pause to regain composure and make safer decisions.

Verify online claims
If something appears too good to be true, or if a message claims to come from an authority such as a government agency, law enforcement, or a bank, avoid responding immediately. Instead, verify the information through trusted channels, such as official websites, verified phone numbers, or reliable news sources before taking action.

Discussion Questions:

- Let's link this back to our previous module—what are the states of mind in which you're most likely to fall victim to a scam, and how would these tactics help?

Presentation Part 2.1.2 Trust Your Instinct to Say No

Say no when something feels suspicious. Do not feel obligated to respond, explain, or comply. Treat pressure, guilt, or embarrassment as warning signs.

"Simple" requests might be a sign of future trouble. Be cautious of small or "harmless" requests, especially early in an interaction. Recognize that small requests are often used to build trust before larger demands. Refuse early requests if they seem unusual or unnecessary.

If something makes you uncomfortable, refuse. Do not share personal information, including passwords, PINs, multifactor authentication (MFA) codes, or financial details. Do not comply with requests that involve secrecy. If someone asks to keep something confidential, treat it as a warning sign and disengage.

Don't hesitate to ask questions. Ask questions before taking action. Request details and clarification without sharing personal information. Pay attention to how the other party responds. If answers are vague, inconsistent, or evasive—or if the person becomes frustrated—end communication.

Discussion Questions:

- What are some questions you would ask/send if you get an email from your boss requesting to make an urgent payment? What might make this difficult to do, in reality?

Presentation Part 2.1.3 Question the Hype

Be skeptical of messages that suggest widespread popularity or urgency. Do not assume something is safe just because others appear to be participating. Treat claims of popularity, authority, or urgency as potential manipulation tactics.

Verify testimonials or 'viral' trends. Do not rely on likes, comments, endorsements, or viral trends as proof of legitimacy. Independently verify claims using trusted sources. Use search engines or official websites to confirm whether a product, service, or offer is legitimate.

Don't be pressured into 'compliance'. Do not feel pressured to act because others are doing so. Recognize statements that encourage conformity as a tactic. Make decisions based on verification, not crowd behavior.

Discussion questions:

- When you see an ad for a product you are interested in on social media, how can you make sure you're buying from a legitimate seller?

Presentation Part 2.1.4 Spot the Changing Red Flags

While scams can be hard to spot, be aware of common red flags when using email, web search, calls, and text. Scams are always evolving, which means the red flags change as well. New technology like generative AI makes it easier for scammers to create convincing scams. Different red flags to look out for include:

- **Unknown email addresses**
- **Incorrect URLs and domains**
- **Poor grammar and spelling**
- **Links in texts from unknown numbers**
- **Automated warnings from your device**
- **Unusual website design and formatting**
- **Requests for personal information**
- **Requests for immediate action and deadlines**
- **Unusual payment requests or deposits**
- **Guaranteed rewards, prizes, or investment gains**
- **Requests for secrecy**

2.2 Group Activity: Be Scam Ready

Time:

30 minutes

Description:

Participants work in pairs to play Google's 'Be Scam Ready' game (https://bescamready.withgoogle.com/). Start by answering the 'warm up' questions together, talking through why you chose your answers. Each pair is assigned a different persona from the 'Be Scam Ready' game (Lin Mei, Sofia Lima, Priya Sharma, David Lim) and plays through the character's story, working quickly on the game's time-limited questions. At the end of each chapter in the story, pairs discuss and identify:

- The red flags that they noticed that should alert the persona to a potential scam
- The persona's mindset and the vulnerabilities it may cause
- Any psychological manipulation tactics that the scammer is using

Note for low-connectivity settings: Instructors may decide to skip this session.

Logistics:

1. Format: Pairs
2. Materials needed: At least one member of the pair needs an Internet enabled laptop/tablet/phone

2.3 Individual Activity: Spot the Red Flags

Time: 15 minutes

Description:

Each participant completes the 'Spot the Red Flags' worksheet, spending five minutes individually trying to identify all the various red flags contained in example messages provided. The objective is to work quickly and identify as many red flags as possible. After five minutes, the trainer goes over the 'Spot the Red Flags' answer sheet, so that participants can mark how many they got right and how many they missed. The trainer then leads a full-group discussion, asking trainees to describe the red flags they encountered.

Discussion Questions:

- Do you think if you were quickly reading through your emails, you would miss some of these red flags? Why?
- Are there times when legitimate emails can contain one or more of these red flags? If so, what are some verification methods you could use?

Logistics:

1. Format: Individual activity, followed by trainer-led discussion, whole group
2. Materials needed: Printed copies (one copy per participant) of the 'Spot the Red Flags' worksheet and answer sheet (page 33)

Content and Resources:

Instructions: Print copies of the 'Spot the Red Flags' worksheet and answer sheet, one copy per participant. Note: Distribute answer sheet only after participants have completed the worksheet.

Spot the Red Flags

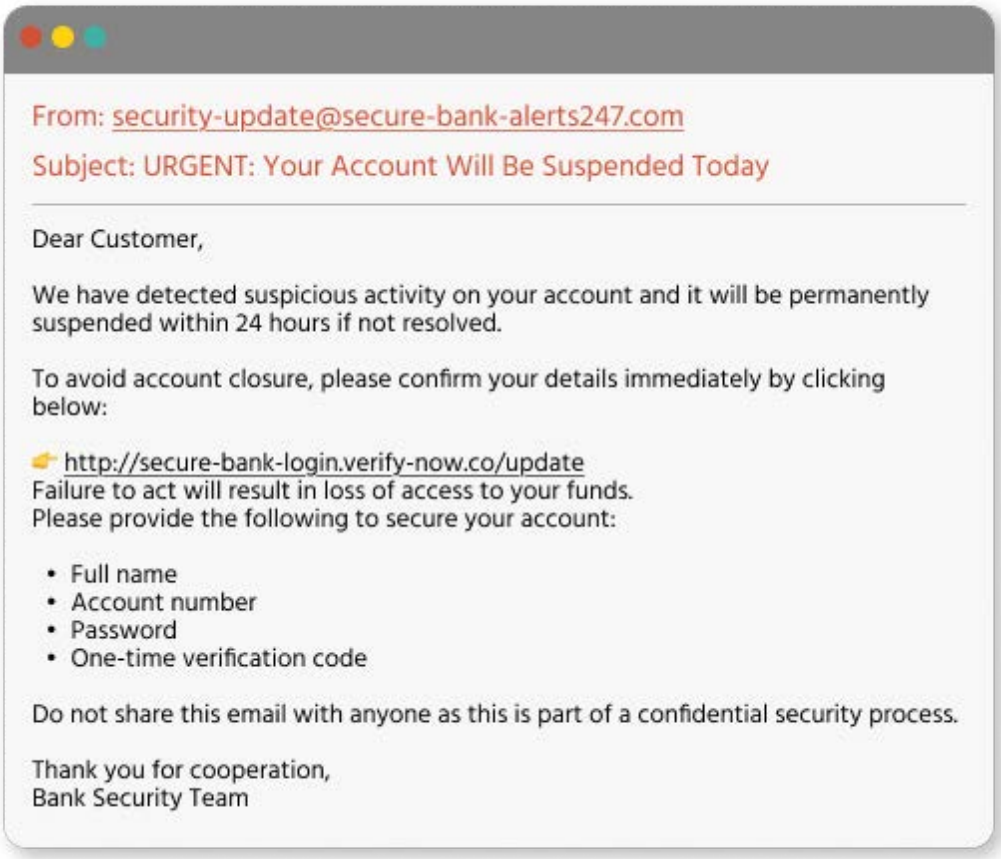
Worksheet

Find as many of the following red flags in the three example messages below

1. Unknown email addresses
2. Incorrect URLs and domains
3. Poor grammar and spelling
4. Links in texts from unknown numbers
5. Automated warnings from your device
6. Unusual website design and formatting
7. Requests for personal information
8. Requests for immediate action and deadlines
9. Unusual payment requests or deposits
10. Guaranteed rewards, prizes, or investment gains
11. Requests for secrecy

When you spot a red flag, add the corresponding number to the worksheet e.g. if you spot an unknown email address, mark it with the number '1.'

When you're done, find the red flags you missed using the answer sheet provided



From: security-update@secure-bank-alerts247.com

Subject: URGENT: Your Account Will Be Suspended Today

Dear Customer,

We have detected suspicious activity on your account and it will be permanently suspended within 24 hours if not resolved.

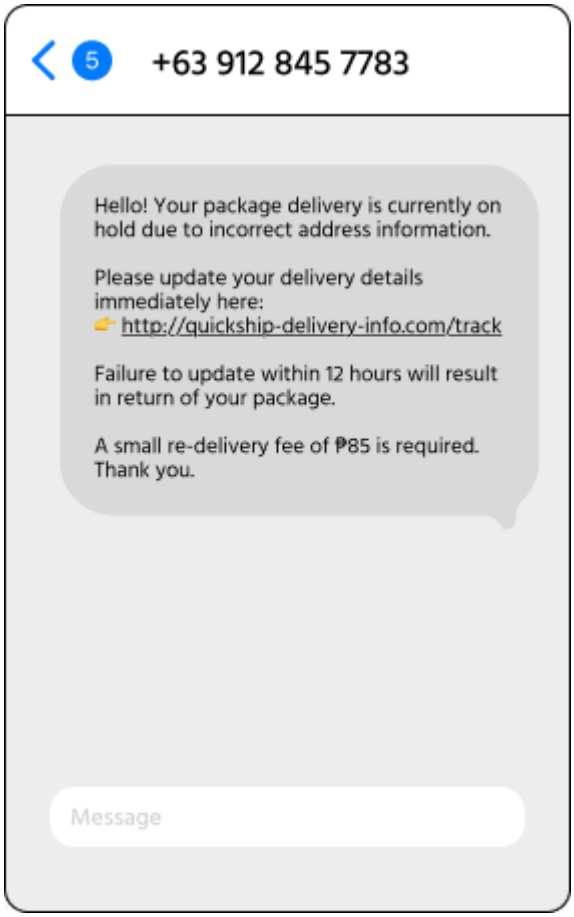
To avoid account closure, please confirm your details immediately by clicking below:

👉 http://secure-bank-login.verify-now.co/update
Failure to act will result in loss of access to your funds.
Please provide the following to secure your account:

- Full name
- Account number
- Password
- One-time verification code

Do not share this email with anyone as this is part of a confidential security process.

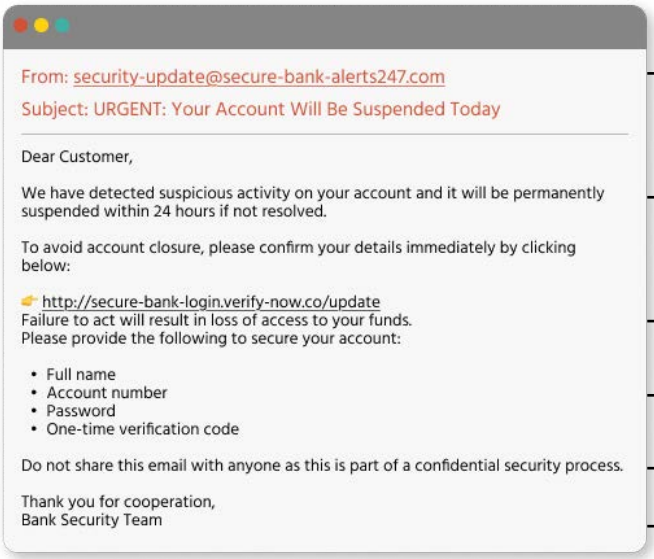
Thank you for cooperation,
Bank Security Team


5
+63 912 845 7783
Hello! Your package delivery is currently on hold due to incorrect address information.
Please update your delivery details immediately here:
http://quickship-delivery-info.com/track
Failure to update within 12 hours will result in return of your package.
A small re-delivery fee of ₱85 is required. Thank you.
Message

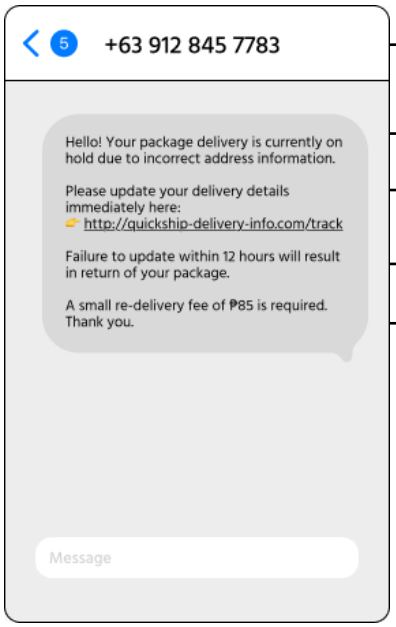

WARNING: Your Device Has Been Infected!
Your phone is infected with (3) viruses that may damage your SIM card and steal your personal data!
Immediate action is required.
http://mobile-secure-protect-now.net/install
If you do not act immediately, your photos, contacts, and banking apps may be compromised.
Limited-time offer: Install now and receive FREE premium protection for 1 year! Do NOT close this page or your device may be locked.

Spot the Red Flags

Answer Sheet



- Unknown email address
- Urgency and deadlines
- Incorrect domain/URL
- Request for personal information
- Request for secrecy
- Poor grammar



- Unknown number
- Generic message
- Link sent via text + suspicious URL
- Urgency
- Payment request



- Urgency
- Suspicious link
- Urgency
- Guaranteed reward

Module 3: Prevent

3.1: Presentation and Discussion

Time: 30 minutes

Description: Trainers deliver a short, interactive presentation that introduces ways to prevent scams and improve online safety. The trainer pauses regularly with questions to prompt discussion. Trainers can use the content and discussion questions from the 'Content and Resources' section included below to develop their presentations.

Logistics:

1. Format: Instructor-led, whole group (25 participants)
2. Materials needed: Slides (including prompt questions for group discussion)

Content and Resources:

Presentation Part 3.1.1 Protect Your Online Accounts

Online accounts act as gateways to personal information. If scammers gain access to one account, they may be able to then access email accounts to reset passwords for other services, impersonate the account holder, and even steal identities.

Use strong, unique passwords for every account: Do not use the same password for multiple accounts. Make passwords hard to crack or guess. Avoid names, birthdays, or short passwords. Instead, opt for long phrases or combinations of random words, as well as numbers and symbols.

Use a password manager: A password manager can generate long, complex passwords and store them securely. While password managers do pose a minor risk by storing multiple passwords in one place, the risk is smaller than using common, repeated passwords.

Turn on multi-factor authentication (MFA): MFA adds an extra layer of protection by requiring a second step in addition to passwords to log in to accounts. This can take the form of a code sent to a phone or a code that another authentication app generates before logging in. A scammer who steals a password will not be able to access an account without that second layer of information.

Enable account alerts: Enable notifications from banks, email providers, and social media platforms that provide real-time alerts through email or text message about logins, password changes, or transactions made from unfamiliar locations or devices. These notifications can help spot suspicious activity early.

Log in only through official apps or websites: Instead of clicking links in emails or text messages, go directly to the company's official website or open the official app. This helps avoid fake login pages that aim to steal credentials and personal information.



Presentation Part 3.1.2 Secure Your Devices and Networks

Reduce risk by securing physical devices like mobile phones, laptops, tablets, and Wi-Fi routers, which are also gateways to personal information online.

Keep your devices updated: Software updates fix security vulnerabilities. Turn on automatic updates for phones, computers, browsers, and apps whenever possible.

Secure your home Wi-Fi: Do not keep the default Wi-Fi password provided by an Internet company during setup. Create strong Wi-Fi passwords and make sure Wi-Fi security is set to the highest protection option (usually called WPA3 or WPA2). This makes the Internet connection harder to hack. Create a special Wi-Fi network just for guests.

Be cautious of public Wi-Fi requirements: Free Wi-Fi in airports, cafés, and hotels can be risky. If a public Wi-Fi network requires a download to access the network, do not comply and opt for a private network. Additionally, when using public Wi-Fi, double check that all sites have 'HTTPS' in the address bar, since this protects sensitive data like passwords and credit card numbers.

Install reputable security software: Antivirus and security tools can help detect if a scammer installs malware onto a device or if someone accesses malicious websites on the device.

Lock your devices: Use PINs, passwords, or biometrics (like fingerprints or eye scanners) to lock phones, tablets, and computers. Turn on the ability to erase devices remotely, which enables users to wipe data from a distance if devices are lost or stolen.



Presentation Part 3.1.3 Guard Your Finances and Money Online

These steps can make it more difficult for scammers to access personal financial information:

Use payment methods with built-in protections whenever possible: Formal bank accounts and credit cards often provide fraud protection and dispute mechanisms. When using mobile money or digital wallets, understand what consumer protections exist and how to report unauthorized transactions.

Protect your mobile money account like a bank account: Never share a PIN or one-time verification codes with anyone else, even if someone offers to help enter a PIN. Report lost phones immediately.

Secure sensitive financial and identification documentation: Safely store account numbers, identification documents, credit cards, and SIM registration details in a lockbox for physical copies, or encrypted storage for digital copies. Avoid sharing these details through text or images via messaging apps unless they use end-to-end encryption, like Signal or Whatsapp.

Review accounts and transactions regularly: Check bank account transactions and statements, mobile money records, or SMS confirmations for any unfamiliar activity. Even small unexplained transfers or payments can be warning signs. Close any unused accounts that may also be subject to future hacks.

Confirm before you send money: Before sending money to someone, use a separate, trusted channel to confirm the transaction. If possible, call the recipient to verify their account. Also, confirm that websites are secure by looking for 'HTTPS' or the 'lock' icon in the address bar before entering payment or personal information.

Presentation Part 3.1.4 Build Safe Online and Offline Habits

Safer everyday online and offline habits can make it harder for scammers:

Limit what you share publicly: Details like birth dates, home address, travel plans, children's names or school details, or workplace can give scammers the information they need to build a convincing, targeted scam. Review social media privacy settings and avoid posting information that a scammer might use to impersonate someone, guess a password, or answer security questions.

Stay informed about common and emerging scams: Scammers are always using new tactics and technologies to trick their targets, especially with the rise of tools like generative AI, fake videos, and voice cloning. Stay informed by following trusted government offices, financial institutions, and consumer protection agencies.

Periodically review your security settings: Every few months, set a reminder to check account and device settings. Make sure details like recovery emails and phone numbers are still correct, and that mechanisms like multi-factor authentication (MFA) are still enabled. Review privacy settings to make sure your information isn't widely accessible.

Browse and communicate safely: Ensure "HTTPS" is visible on the browser, especially for sensitive sites such as bank accounts or health records. If given the option, opt for secure communication platforms that use end-to-end encryption, such as Whatsapp and Signal, rather than SMS, email, and Facebook Messenger.

Create a family 'safe word' or verification question: New AI tools are capable of cloning voices, which makes scams like family or friend impersonation scams more convincing. Agree on a private phrase, word, or question that is known only to family or close friends. If someone calls or messages claiming to be a family member, ask for the safe word or answer to make sure it's them.

Talk openly about scams: Scammers rely on embarrassment and silence, especially from scam victims. If people have been a target of online scams, sharing what they know with family, friends, and co-workers will help protect others.

Discussion Questions:

- What is a habit or tool that you already use to protect your online accounts? Do you think these are working well, or are you now considering doing something else to protect your accounts?
- Which of the prevention methods feels the hardest or most inconvenient to use? Why?
- Do you think it's realistic to implement all these prevention measures in real life? If not, which ones would you prioritize?

3.2 Group Activity: Secure This Scam Target

Time:

35 minutes (20 minutes small group discussion + 15 minutes debrief discussion)

Description:

Participants work in small groups of three to five. Each group is assigned a scam target persona video from the Internet Society's Digital Toolkit. They then use the Scam Strong Prevention Summary (print-ready version found on page 40) to identify specific prevention actions that might have helped the persona avoid getting scammed, or lessen the scam's severity.

Debrief:

Each small group describes their persona to the wider group. Then, summarize the persona and describe:

- What were the victim's top two to three vulnerabilities?
- What prevention measures might have helped to make them more secure?

Logistics:

1. Format: Small groups of three to five
2. Materials needed: Personal laptops/ phones/ tablets to access persona videos or printed persona cards for low-connectivity settings (see print-ready persona cards on page 13-22), one copy per group
3. Printed copies of the cards from the Scam Strong Prevention Summary (print-ready version found on page 40), one copy per participant

Content and Resources:

Print-ready page: Scam Strong Prevention Summary

Instructions: Print one copy of the 'Scam Strong Prevention Summary' (page 40) for each participant

Scam Strong Prevention Summary

Protect Your Online Accounts



Use strong, unique passwords for every account



Use a password manager



Turn on multi-factor authentication (MFA)



Enable account alerts



Log in only through official apps or websites

Secure Your Devices and Networks



Keep your devices updated



Secure your home Wi-Fi



Be cautious on public Wi-Fi

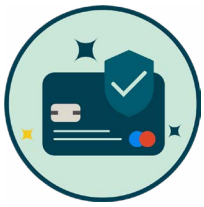


Install reputable security software

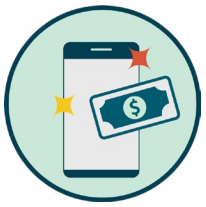


Lock your devices

Guard Your Finances and Money Online



Use payment methods with built-in protections whenever possible



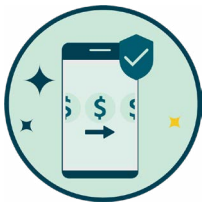
Protect your mobile money account like a bank account



Secure sensitive financial and identification documentation



Review transactions regularly



Confirm before you send money

Build Safe Online and Offline Habits



Limit what you share publicly



Stay informed about common and emerging scams



Periodically review your security settings



Create a family ‘safe word’



Talk openly about scams

3.3 Individual Activity: My Scam Strong Checklist

Time:

20 minutes

Description:

Participants complete the 'Scam Strong Checklists' worksheet (pages 42 and 43). Participants check off steps that they can commit to implementing in the next week that will help protect their various apps and they cross off items that they have already done. Once done, each participant pairs up with the person next to them to discuss what they prioritize and why, creating some sense of accountability.

Where possible, trainers urge participants to implement one to three concrete actions while in the room (e.g. turn on multi-factor authentication (MFA), update a password, or delete an unused app.)

Logistics:

- **Format:** Individual activity, followed by paired discussion
- **Materials needed:** Printed copies (one copy per participant) of the 'Scam Strong Checklists' worksheet (page 42 & 43)

Content and Resources:

Instructions: Print copies of the 'Scam Strong Checklists' worksheet, one copy per participant.

Scam Strong Checklists

Worksheet

Check off the prevention steps that you can put in place within the next week.
Choose only the accounts/apps that are most relevant to you (e.g. if you don't use mobile money, skip that section). Cross off those items that you have already done.



Protect My Online Bank Account

- [ ] Use a strong, unique password stored in a password manager.
- [ ] Enable biometrics and/or multi-factor authentication (MFA) using an authenticator app or secure code.
- [ ] Turn on real-time transaction alerts for withdrawals, transfers, and login attempts.
- [ ] Review your transactions and continue to do so regularly.
- [ ] Set up account recovery options (backup email/phone) and keep them updated.
- [ ] Close any unused online bank accounts.



Protect My Email Account

- [ ] Use a strong, unique password stored in a password manager.
- [ ] Enable biometrics and/or multi-factor authentication (MFA) using an authenticator app or secure code.
- [ ] Review your account recovery email and phone number.
- [ ] Turn on login alerts for new devices or locations.
- [ ] Check your "sent" folder for messages you didn't send, and continue to do so regularly.
- [ ] Remove apps you no longer use that have access to your email.
- [ ] Log out of shared or public computers.



Protect My Social Media

- [ ] Use a strong, unique password stored in a password manager.
- [ ] Enable biometrics and/or multi-factor authentication (MFA) using an authenticator app or secure code.
- [ ] Review who can see your posts, friends list, and personal information.
- [ ] Set your account to private (if appropriate for you).

- [ ] Remove your phone number or email from public view.
- [ ] Go through your ‘friends list’ on social media, and delete those you do not recognize.
- [ ] Review your posts to make sure you did not publicly share travel plans, location details, or sensitive personal information.



Protect My Home Wi-Fi

- [ ] Change the default router password immediately after setup. Create a strong Wi-Fi password that is different from your device passwords.
- [ ] Update your router’s firmware, and continue to do so regularly.
- [ ] Set up a separate guest network for visitors.
- [ ] Put your router in a secure physical location.
- [ ] Rename your network so it does not reveal your name or address.



Protect My Device (Phone, Tablet, Computer)

- [ ] Lock your device with a PIN, strong password, fingerprint, or face recognition.
- [ ] Turn on automatic software and security updates.
- [ ] Remove apps you no longer use.
- [ ] Enable “Find My Device” features.
- [ ] Enable remote wipe features.
- [ ] Install reputable security or antivirus software.
- [ ] Back up your data, and continue to do so regularly.



Protect My Mobile Money Account

- [ ] Secure your phone with a password, PIN, fingerprint, or face recognition so others cannot access your mobile wallet.
- [ ] Choose a strong PIN for your mobile money account.
- [ ] Review SMS confirmations or your transaction history for unfamiliar transfers or withdrawals.
- [ ] Close any unused mobile money accounts.

Module 4: Respond and Report



4.1 Presentation and Discussion

Time: 30 minutes

Description: Trainers deliver a short, interactive presentation using slides that introduce ways to respond to and report scams if they happen. The presentation covers key concepts from the 'Content and Resources' section below. The trainer pauses regularly to prompt discussion. Trainers use the content and discussion questions below to develop their presentations.

Logistics:

- **Format:** Instructor-led, whole group (25 participants)
- **Materials needed:** Slides (including prompt questions for group discussion)
- **Space:** Large lecture room

Content and Resources:



4.1 Presentation and Discussion

Acting quickly and seeking help from the right places can help lessen the impact of a scam:

Stop further harm immediately: Cut off all communication with the scammer immediately by blocking them or deleting an account entirely. Contact bank or mobile money providers to stop any pending payments or transfers. Secure compromised accounts by changing passwords and enabling additional protections like multi-factor authentication. Disconnect affected devices if a scammer has infected them with malware or accessed them remotely.

Secure financial accounts: Contact your bank, payment providers, mobile money platforms, government ID agencies, or financial institutions to report fraud. Provide details about the transaction so that they can secure accounts and begin investigating the fraud. Request account freezes or transaction reversals where possible. Monitor accounts closely for additional suspicious activity. Cancel or replace compromised credit cards. Close any unused accounts that may also be subject to future hacks.

Protect your identity and credit: Notify credit reporting or monitoring services, if locally available. They may be able to help protect and restore credit ratings, and to help monitor credit for any potential future fraud. Place alerts or restrictions on credit files when identity information has been exposed. Document which personal details were shared or compromised.

Presentation Part 4.1.2 Report

Preserve evidence like messages, transaction records, and screenshots of your interactions with the scammer. Save copies of emails, text messages, chat conversations, payment confirmations, account numbers, and any related screenshots. Avoid deleting these records until the incident has been reported. They may be useful when working with financial institutions, reporting to authorities, or supporting an investigation.

Report the incident to law enforcement or cybercrime authorities. Where available, report scams to local police or the national cybercrime reporting center. Provide details about how the scam occurred, the accounts or phone numbers the scammer used, and any financial transactions involved. While recovery is not always possible, reporting helps authorities track criminal activity and may support future investigations. Resources like www.scam.org can provide information on relevant local organizations and authorities.

Report the scam to the platform where it happened. If the scam happened through social media, messaging apps, email, or an online marketplace, use the platform's reporting tools to flag the account, message, or advertisement.

Notify consumer protection or national anti-fraud organizations. Many countries have agencies that collect reports of scams and help warn the public. These include consumer protection authorities, fraud reporting centers, or financial regulatory bodies. Submitting a report can help warn others, identify emerging scam patterns, and sometimes connect a case to larger investigations.

Customization:

Trainers include information and contact information for the major organizations and authorities for scam reporting in the relevant country/regional context.

Presentation Part 4.1.3 Get Support

Recognize that scams are designed to deceive you. This is not a personal failure. Being targeted or affected by a scam is not a personal mistake. Anyone can be deceived. Understanding this can help reduce feelings of shame and make it easier to seek help and take steps to move forward.

Seek support from people you trust—family, friends, or community organizations. Becoming a victim of a scam can be a traumatic event, and it requires similar support. Sharing what happened with a trusted individual—such as a friend, family member, or community organization—can help victims review the situation, consider options, and take the next steps more confidently.

Access victim support services or helplines where available. Look for consumer protection agencies, fraud reporting centers, or nonprofit organizations that offer confidential advice and support. These services may offer guidance on reporting the scam, protecting your finances and identity, and coping with the emotional stress that scams can cause.

Customization:

Trainers include information and contact information for the major organizations where scam victims can get support in the relevant country/regional context.

Discussion Questions:

- What do you think might stop someone from reporting a scam?
- If you became a victim of a scam right now, who are the first three people or organizations you would contact? Why?

4.2 Group Activity: What Should I Do Next?

Time: 25 minutes

Description: Participants divide into four groups of roughly equal size (i.e. six to seven for a 25-person training). Each group is assigned a scam target persona videos from the Internet Society's Digital Toolkit.

Note for low-connectivity settings: Print out Scam Strong persona cards found on pages 13-22.

After watching the video, the group is given a series of printed 'action cards' that the persona can take after they are scammed (see print-ready cards on pages 48-49). They sort these cards into the following piles as quickly as possible:

- Do in the first five minutes (immediate actions)
- Do in the first 24 hours (follow-up actions)
- Never do (risky or harmful actions)

As soon as each group is done, the team raises their hands. The trainer then reads out the answers and whichever group finished the quickest and had all the correct answers, wins. The trainer then leads a discussion with the whole group.



Discussion Questions:

- What are the kinds of evidence that your persona should retain for an investigation?
- Which platform(s) or institution(s) can your persona contact to report the scam?

Logistics:

- **Format:** Four groups of six to seven
- **Materials needed:** Personal laptops/phones/tablets to access persona videos or printed persona cards for low-connectivity settings (see print-ready persona cards on pages 13-22), one copy per group
- Printed copies (one per group) of the 'What Should I Do Next?' action cards (pages 48-49)

Content and Resources:

Instructions: For low-connectivity settings: Print one copy of each of four scam target personas (pages 56-59)

Print four copies of the 'What Should I Do Next?' action cards

Cut out individual cards, sort them in small bags so that they can be easily distributed to each of the four groups

What Should I Do Next?

Action Cards

Pile 1: Do in First Five Minutes (Immediate Actions)

Contact your bank or payment provider to report the transaction
Freeze or block your credit/debit card
Stop all communication with the suspected scammer
Save screenshots of messages, emails, and transaction details
Secure your accounts (change passwords, enable MFA if not already active)

Pile 2: Do in First 24 Hours (Follow-Up Actions)

Flag or report the account on the platform where the scam occurred
Monitor bank and financial accounts closely for further suspicious activity
Inform a trusted friend, family member, or colleague for support
Warn others in your network (without sharing harmful links or sensitive details)
Report the incident to relevant consumer protection, scam reporting organizations, or other relevant authorities

Pile 3: Never Do (Risky or Harmful Actions)

Wait to see if the scammer responds or returns the money
Send additional money to recover lost funds
Delete messages, emails, or transaction records
Close all accounts immediately without consulting your bank
Share scam links or materials with others



4.3: Individual Activity: My Personal Response Plan

Time:

15 minutes

Description:

Participants complete the 'My Personal Response Plan' worksheet (page 50). In this activity, participants imagine that they have been scammed through an online recruitment site, and then work through the steps that they would actually take in response, encouraging a combination of both immediate action and longer-term behavior change.

Where possible, trainers urge participants to implement one to three concrete actions while in the room (e.g. save the emergency/scam reporting phone number of their primary financial institution, bookmark a resource like www.scam.org, save the phone number/contact information of local cybercrime authorities, etc.)

Logistics:

- **Format:** Individual activity
- **Materials needed:** Printed copies of the 'My Personal Response Plan' worksheet (page 50), one copy per participant

Content and Resources:

Instructions: Print copies of the 'My Personal Response Plan' worksheet, one copy per participant

My Personal Response Plan

Worksheet

Imagine you realize you've been scammed through an online recruitment site. You were offered a lucrative job by a 'recruiter' on a popular job website. They asked you to share personal information, and you even paid a 'processing fee' to get the job offer. It turns out that the job and the recruiter were fake. They now have your money and sensitive information.

Work through the steps below based on what you would actually do:

1. **Stop the damage:** What is the first action you would take in the next five minutes?

---

2. **Activate your support network:** Who is the first person you would contact (friend, family member, colleague)? Why them?

---

3. **Report the scam:** Which platforms, organizations, or authorities in your country would you report this to? (Examples: the platform where it occurred, your bank, consumer protection agencies, or reporting sites like scam reporting portals)

4. **Preserve evidence:** What specific information would you save or document before taking further action? (e.g., messages, email addresses, transaction records, screenshots)

5. **Secure your accounts:** What steps would you take to protect your accounts and identity immediately after?

---

6. **Change future behavior:** What is one habit or rule you would adopt to reduce your risk moving forward?

Module 5: Support

5.1 Presentation and Discussion

Time: 30 minutes

Description: Trainers deliver a short, interactive presentation that introduces ways to support victims and build Scam Strong communities. The trainer pauses regularly with questions to prompt discussion. Trainers can use the content and discussion questions from the 'Content and Resources' section included below to develop their presentations.

Logistics:

- **Format:** Instructor-led, whole group (25 participants)
- **Materials needed:** Slides (including prompt questions for group discussion)

Content and Resources:

Presentation Part 5.1.1 Support Victims

Help stop ongoing harm

- **Help stop all contact with the scammer.** Scammers often continue communication to request more money or information. Helping victims block phone numbers, messaging accounts, or email addresses can help prevent further manipulation.
- **Help review recent financial activity.** Offer to look together at bank statements, payment app histories, or credit card activity to identify unfamiliar transactions. Early detection can help financial institutions respond more quickly.
- **Assist with securing accounts and devices.** Offer to help change passwords, enable multi-factor authentication, or check device security settings. If the victim downloaded malware or suspicious apps, disconnect the device and seek technical support.

Support effective and timely reporting

- **Assist with gathering documentation and evidence.** Help to find and organize evidence, including messages, transaction records, account details, screenshots, and links that may all be helpful when reporting the incident.
- **Help contact banks, payment services, or authorities.** Financial institutions often have dedicated fraud teams that can guide next steps. If the victim feels stressed or uncertain, offering to sit with them during the call can make the process easier.
- **Help identify and reach victim support services.** Finding and connecting the victim with consumer protection agencies, hotlines, or relevant nonprofit organizations can help them get the services they need, including guidance on financial recovery, identity protection, and emotional support.

Watch for continued risk

- **Be alert for follow-up scams.** Victims may receive messages from people claiming they can recover the lost money, investigate the crime, or represent law enforcement. These "recovery scams" often ask for additional fees or personal information. Make sure the victim is on the lookout for these kinds of follow-up scams.
- **Encourage ongoing monitoring of accounts and communications.** Remind victims to regularly check financial accounts, credit reports, and messages. This can help detect further suspicious activity early. Help them close any unused accounts that may also be subject to future hacks.
- **Reinforce preventative habits without reinforcing a victim's sense of fear or shame.** Rather than emphasizing blame or fear, focus on practical steps that build back a victim's confidence, such as verifying requests, pausing before sending money, and using strong account security.

Approach with care and respect

- **Start conversations without blame or judgment.** Avoid questions or comments that suggest the person should have 'known better.' Instead, simple statements like "I'm glad you told me" or "Let's figure out the next steps together" can help the person feel supported.
- **Acknowledge that scams are sophisticated and target many people.** Modern scams are carefully designed to exploit trust, urgency, or emotions. Reminding someone that scams affect people from all backgrounds can reduce shame and encourage them to take action.
- **Create a safe space for the person to share what happened.** Give them time to explain the situation in their own words. Avoid interrupting or rushing to conclusions. Instead, focus on listening. Understanding the full story can help identify what information or accounts might be at risk.



Discussion Questions:

- If a family member or friend told you they had been a victim of a scam, what would you say? What would you have to stop yourself from saying?
- What's most helpful in the moment—advice, action, or emotional support? Why? How would that differ for different people in your life?

Presentation Part 5.1.2 Build Scam Strong Communities

- **Pay attention to signs that someone in your community may be at risk of a scam, staying alert and supportive of the people around you.** This community-oriented approach—also known as 'safeguarding'—can help prevent scam-related harms from escalating.
- **Watch for financial stress or unusual requests for money.** If a potential victim needs to urgently send money, withdraw savings, or transfer funds, this may be a sign that a scammer is pressuring them. Gently encourage the potential victim to pause before acting.
- **Notice secrecy around new online relationships or opportunities.** Pay attention if a potential victim becomes unusually private about a new online relationship, job offer, or investment opportunity. This may be a sign that a scammer is targeting them. Scammers often encourage secrecy to prevent victims from seeking outside advice.
- **Discreetly check in with others who know the person well.** Family members, friends, or trusted colleagues may have noticed similar warning signs, such as sudden financial pressure, secrecy about a new online relationship, or unusual requests for money. Sharing observations can help "connect the dots" and build a clearer picture of what might be happening. Always handle these conversations carefully and respectfully, with the goal of supporting the person and preventing harm, not spreading rumors or assigning blame.

Discussion Questions:

- What's the most difficult part of getting involved when you think someone in your community or family might be getting scammed?

5.2 Group Activity: How to Be a Scam Strong Champion

Time:

20-30 minutes

Description:

Set up four stations, each featuring one of the four Scam Strong Champions (Ravi, Daniela, Samuel, Amina). Divide into four groups (six to seven per group), each group rotates between two to three stations (~10 minutes per station). At each station, the group discusses the following questions:

- What did the Scam Strong Champion do well?
- What are additional actions they can take to help the scam victim?
- What might make it difficult to take these actions in real life?

Logistics:

Format: Four groups of six to seven

Materials needed: Printout of Scam Strong Champions (Ravi, Daniela, Samuel, Amina) for each station (pages 56-59), one copy each

Content and Resources:

Instructions: Print one copy each of the Scam Strong Champions, one per table



Scam Strong Champion Ravi

Ravi's grandmother received a call from someone claiming to be from her bank. The caller said her account had been compromised and urged her to transfer money immediately to keep it safe. Trusting the caller, she did.

When she later told Ravi, he stayed calm.

"Nani, these scams happen to many people—the caller sounded official on purpose. Let's focus on protecting your accounts first. We can call your bank together and explain what happened."

Together, they contacted the bank's fraud department, reviewed her transactions, saved the scam number as evidence, and strengthened her account security. Ravi also warned other family members to pause and verify similar calls.



Scam Strong Champion Daniela

Daniela began noticing that her friend was constantly talking about someone she had met online. The relationship had moved quickly, and soon her friend mentioned that the person needed financial help to deal with an unexpected emergency.

Instead of criticizing her, Daniela approached the conversation gently.

“I’m really glad you told me about him. Sometimes scammers build trust over time before asking for money. Would you mind if we took a closer look at the messages together?”

Together, they reviewed the profile and messages and started noticing warning signs that something might not be right. Daniela encouraged her friend to pause before sending any money and to verify the person’s identity. That conversation helped her friend step back and avoid what could have become a costly romance scam.



Scam Strong Champion Samuel

Samuel noticed that a co-worker seemed unusually stressed after talking about a new online investment opportunity that promised fast returns. Soon the colleague admitted that he had already sent money—and the person behind the investment had stopped responding.

Samuel focused on helping rather than blaming.

“I’m really glad you told me. These scams are designed to look convincing. Let’s look into some ways to report this scam to law enforcement together”

Together, they gathered screenshots of messages, transaction records, and account details. Samuel encouraged his colleague to contact his bank and report the incident to the appropriate authorities. Taking these steps helped protect the colleague from further losses and made it easier to warn others about similar scams.



Scam Strong Champion Amina

Amina is a nurse in a community health clinic. Over a few visits, she notices that one of her patients seems anxious and distracted, mentioning urgent phone calls about a “problem” with his bank account. The patient also says a relative has been helping him move money quickly to “fix” the issue.

Concerned, Amina gently reaches out to the patient’s daughter after getting permission to do so.

“I just wanted to check in—your father mentioned some urgent calls about his bank account. Sometimes scammers create pressure like this. It might be worth taking a moment to verify what’s happening together.”

The daughter thanks Amina and mentions that her father has been going to the bank frequently and she’s not sure why. She speaks with her father that evening. Together, they contact the bank, stop a pending transfer, and report the scam. By connecting the dots and involving a trusted family member, Amina helped prevent further harm. A well-connected community can protect those at risk.

5.3 Individual Activity: Who Can I Help?

Time: 15 minutes

Description: Participants complete the 'Who Can I Help?' worksheet (see page 61). In this activity, participants identify three people (or groups of people, e.g. grandparents) within their community who might be particularly vulnerable to scams, or who may not know much about the dangers of online scams (e.g., older relatives, students, colleagues under financial stress). Then identify one concrete action they can take to support each individual (e.g. talk to a parent about scams, share a checklist with coworkers, set up a family safe word)

Logistics:

- **Format:** Individual activity
- **Materials needed:** Printed copies (one copy per participant) of 'Who Can I Help?' worksheet (page 61)

Content and Resources:

Instructions: Print copies of the 'Who Can I Help?' worksheet, one copy per participant

Who Can I Help?

Worksheet

Identify three people within your community who might be particularly vulnerable to scams, or who may not know much about the dangers of online scams (e.g., older relatives, students, colleagues under financial stress). Then identify one concrete action you can take to support each individual (e.g. talk to a parent about scams, share a checklist with coworkers, set up a family safe word).

Name: ----------

What I can do to help: ----------

Name: ----------

What I can do to help: ----------

Name: ----------

What I can do to help: ----------

Resources



Internet Society

onlinesafety.internetsociety.org

With support from Google.org