Identifying Scam Calls

Facilitation Guide

Help learners to identify and avoid scam calls.

Overview

This module introduces to learners to best practices for identifying and avoiding different types of scam calls.

For more information, be sure to watch Series 3 training videos from NYC Digital Safety.

Outcomes

By the end of this module, participants will be able to:

- Describe scam calls
- Name different types of scam calls
- Use best practices for identifying and avoiding scam calls

Format + Time Frame

This module provides an information overview of scam calls, including how they work and the forms they take, and a how-to guide for identifying and avoiding scam calls.

This module will take approximately 35 minutes to complete. You can combine this module with others for a longer learning experience.

Materials

- Slide deck
- Facilitation guide

- Handouts
    - Identifying Scam Calls
    - Spoofed Numbers

Lesson Plan

Activity	Materials	Time Needed
Introduction and welcome Greet learners and review the plan for this module.	Slides 1 and 2	2 minutes
Defining and discussing scam calls Start by introducing a definition of scam calls. Then, open a discussion and have your learners share their own experiences with scam calls.	Slides 3 and 4	7 minutes
Scam calls, how they work, and key features and traits of scam calls Review the slides that provide an overview of scam calls, including types of scam calls and how they work. Pause to see if anyone has additional examples to share or any thoughts or questions.	Slides 5 through 9	12 minutes
Ways to avoid scam calls Begin by distinguishing between scam calls and scam emails and then review the list of ways to avoid scam calls.	Slides 10 through 12	10 minutes

Pause to see if people have other suggestions to add.		
Wrap up, final tips, and final questions Review the closing thoughts and share the suggested resources. See if anyone has any final questions.	Slides 13 through 16, Handout	5 minutes

Considerations

Scam calls are a sort of universally shared nuisance at this point, so you might consider leaving time for your learners to share their own experiences with and examples of scam calls here. For an additional activity, you could even ask some of your learners to share a recent scam voicemail they've received or an example of a spoofed or scam caller from their phone's call history. Feel free to customize and include examples from your own learners for this module.

Options and Variations

This module pairs well with other modules on phones, particularly the module on handling spam calls, as well as modules on phishing schemes and scams more generally. You could run a combined workshop or you could offer a workshop series that focuses on various scams and schemes over email, phone, and text.

You can also provide this information and content to patrons via a service point by sharing the handout form this module with them, as well as the handout on handling spam calls.

Assessment

The following are some suggested assessment questions that you can use and adapt for your own purposes. These questions can help you assess various things, including knowledge retention, personal views and preferences, and concept application.

You might consider asking these as a pre or post test, or you can have learners answer these as part of an exit survey or a follow-up survey. Keep reading for suggested questions and an answer key with further details and explanations.

Questions for Participants

What is a spoofed number?

A. Another way of referring to spam calls
B. An unknown number
C. When a caller deliberately falsifies the number you see in your caller ID to disguise their identity
D. When a scammer calls you with multiple numbers to avoid being blocked

Which of the following are examples of common scam calls? Select all that apply.

A. Calls saying you owe money to the IRS
B. Calls saying you've won a prize
C. Calls claiming to be from your workplace wanting you to perform a task
D. Calls telling you to reset your password

What is a sign of a possible scam call?

A. A robotic voice
B. A recorded message asking you yes or no questions
C. Calls from an unknown source
D. All of the above

What should you not do if you receive a scam call?

A. Block numbers from scammers
B. Report scam calls to places like the FCC
C. Screen your calls with voicemail or screening tools
D. Just hang up if you answer one

E. Confront the scammer

Answer Key

What is a spoofed number?

Answer: C, When a caller deliberately falsifies the number you see in your caller ID to disguise their identity

Spoofed numbers are fake numbers essentially. A caller will deliberately conceal and falsify their number on your caller ID, in order to look like another number. Often callers will make it look as if they are using a local number in order to get you to answer.

Which of the following are examples of common scam calls? Select all that apply.

Answer: A, Calls saying you owe money to the IRS; B, Calls saying you've won a prize

Most scam calls are centered around money, such as money you allegedly owe or money you've allegedly won. The latter two answers here are examples of common phishing schemes you might receive over email, which tend to have a somewhat wider range of topics included and often focus around your online accounts.

What is a sign of a possible scam call?

Answer: D, all of the above

Robotic or recorded calls, automatic menus, and unknown numbers can all be signs of a potential scam call. Increasingly, these are recorded calls and an actual human isn't the one doing the calling.

What should you not do if you receive a scam call?

Answer: E, confront the scammer

Answers A-D are all good potential ways to deal with a scam call. The main thing to not do is to try to engage directly with the call, whether that's calling back, asking questions, replying to menu prompts in order to talk to someone, etc.

Connections to Other Modules

This module connects to many other modules. The following suggestions provide opportunities for exploration, connection, and potential programming. However, feel free to explore and make connections between other modules not listed here as well!

1.1 Phishing Schemes

1.3 Social Media Account Hacks

3.1 Handling Spam Calls
3.1 Spoofed Numbers

3.2. Identifying Email and Text Spam
3.2 Dealing with Scammers
3.2 Managing SMS Settings

These and other modules can be found at this project's website, nycdigitalsafety.org.

About This Project

These materials were released in October 2022 as part of NYC Digital Safety: Privacy & Security.

NYC Digital Safety: Privacy & Security is a partnership between New York City's three library systems — Brooklyn Public Library, The New York Public Library, and Queens Library — and METRO Library Council. With support from the New York City Office of Technology and Innovation, this project ensures that NYC residents can rely on public libraries for their questions about internet privacy and security.

Visit nycdigitalsafety.org for more information.