NYC Digital Safety

Privacy & Security

Identifying Scam Calls

Learn how to identify and deal with scam calls.

1. What Are Scam Calls and How Do They Work?

Scam calls are similar to phishing schemes. These calls try to trick you into revealing personal information or giving someone access to your financial accounts.

While an online phishing scheme might seek to gain access to your online accounts,, scam calls often try to convince you to reveal your financial information in order to pay a phony bill or take advantage of some alleged financial opportunity.

Here are some tactics that scam calls use to fool or trick you:

- **False sense of urgency:** Scam calls often pressure you into revealing your information. They might claim that you owe money or that there's a "limited time offer" for you to refinance something
- Instilling fear: Likewise, scam calls often try to scare you into revealing your information. For example, scammers might pretend to be from the IRS
- **Tempting you with an opportunity:** These scam calls often try to convince you that you've won something or that you can take advantage of a limited or "special" opportunity
- Appeals to kindness: Some scammers will impersonate a charity and trick you into donating money to what you think is a good cause

2. What Are Some Common Types of Scam Calls?

Scam calls often center around trying to get your money. Here are a few common scam calls that you might encounter:

• **Debt consolidation:** Scam calls often try to tempt you with offers to consolidate your debt, whether that is student loans, a mortgage refinance, or credit card debt

NYC Digital Safety

Privacy & Security

- **Help paying off loans:** A variation of the debt consolidation scams, these scams trick you by offering to help you pay off your loans
- **Health insurance:** These scams try to fool you into signing up for some sort of phony health insurance plan
- **IRS calls:** Fake IRS calls have become incredibly common. These scams scare you into thinking that you owe money to the IRS and that you're going to be in trouble if you don't pay them immediately
- **Fake fraud alerts:** These scammers try to impersonate your bank or a utility company and convince you that your account has been compromised to get you to reveal your information
- **Fake charities:** These scams dupe you into donating money to what you think is a good cause
- **Free cruise:** Another scam that is incredibly common. This scam tries to get your personal information by convincing you that you've won a free cruise
- **Tech support:** These are much more common over email, but they do crop up sometimes via the phone. With this scam, someone will call claiming to be from tech support to obtain your account information

3. How Can You Identify and Deal With Scam Calls?

Use the following strategies:

- Be wary of answering calls from unknown numbers. Consider sending those to voicemail as a way to screen them
- If you answer a call from an unknown source and get a robotic voice or an obvious recording, it could be a sign of a scam
- Save businesses or services that you use in your phone contacts so you can be sure of who is calling you
- Be wary of any call or voicemail that is trying to convince you or pressure you into giving away personal details or financial information
- Cut down on the amount of spam calls you get in general by using tools on your phone and from your wireless carrier to block and report spam. Search for options for your type of phone and your particular wireless carrier

NYC Digital Safety

Privacy & Security

- Use third-party applications to help you manage and block spam calls. These include applications like Robo-Killer or ones from wireless carriers like Verizon's Call Filter
- Sign up for the <u>Do Not Call</u> registry to stop getting calls from telemarketers
- Be cautious about where you give out your phone number online
- If you get a suspicious voicemail or call, run a search to see if you can learn more. You might find reports of a known scam
- Finally, you can report scams yourself to places like https://reportfraud.ftc.gov/#/