



ConnectHome Nation Webinar

Tips from the FCC on Handling Robocalls and Internet Scams

2/25/2020



Agenda

1. FCC's Consumer Connections: What You Should Know About Robocalls and Scams

Lyle Ishida, Director of Consumer Affairs and Outreach Division

2. Q&A

[Agenda](#)

Topic #1

Q&A

Lyle Ishida

**Chief of Consumer Affairs and Outreach Division
Consumer and Governmental Affairs Bureau
Federal Communications Commission**



What are Robocalls?

Robocalls are unsolicited pre-recorded telemarketing calls to landlines and all autodialed or pre-recorded calls or text messages to wireless numbers, emergency numbers and patient rooms at healthcare facilities.





FCC | CONSUMER CONNECTIONS

Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofers may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

Here are some good ways to avoid being spoofed:

- Don't answer calls from unknown numbers.
- If you answer and it's not who you expected, don't hang on, hang up.
- If a caller asks you to hit a button to stop getting calls, just hang up.
- Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- Use extreme caution if you are being pressured for immediate payment.
- Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- Report spoofing scams to law enforcement, the FCC and the FTC.



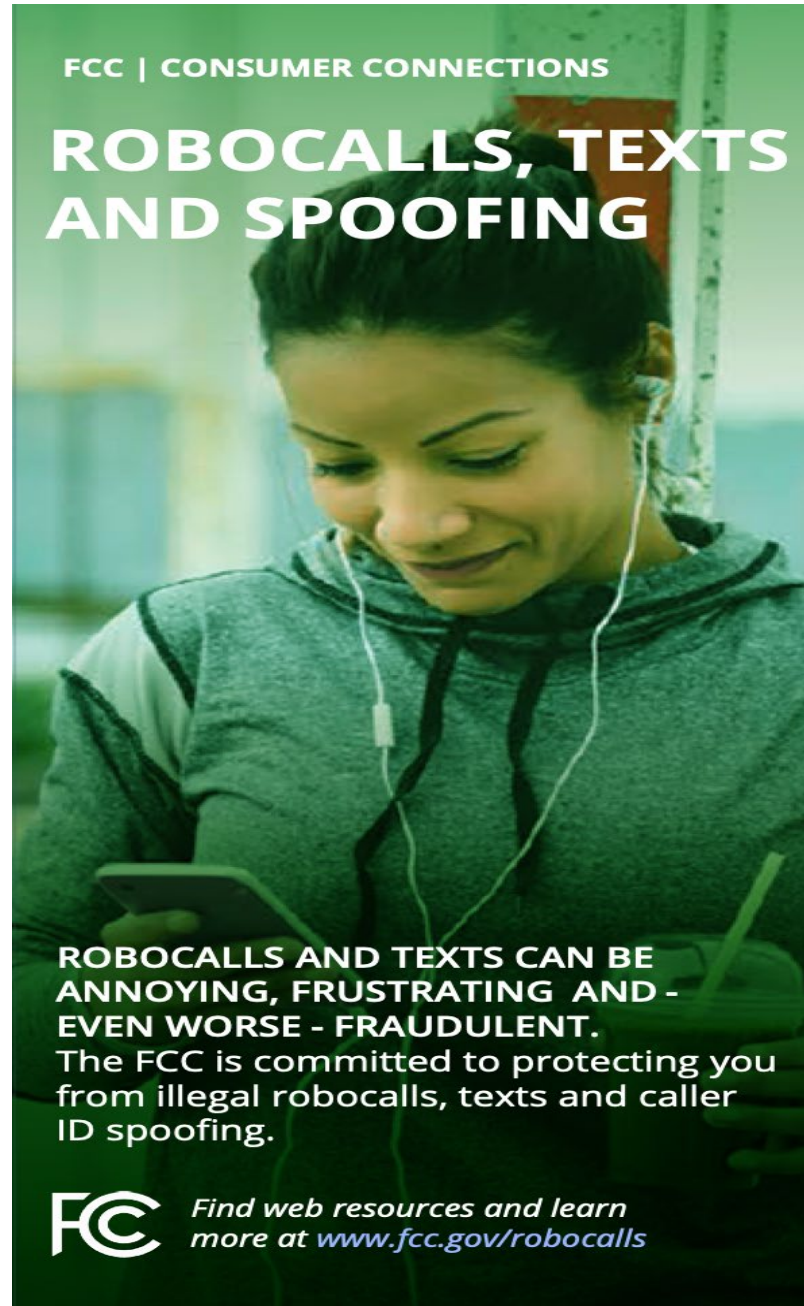
Learn more at fcc.gov/spoofing

Caller ID Spoofing

- Caller ID Spoofing is when a caller purposely falsifies the information transmitted to your caller ID display to disguise their identity.
- There are legitimate legal uses for spoofing. These include when a doctor calls a patient from her personal mobile device and the call displays the office number or when a business displays its toll-free number as a call back number.

Texts and Emails


- Calls are not the only form of scamming
- Scams can also come via email and text messages



FCC | CONSUMER CONNECTIONS

ROBOCALLS, TEXTS AND SPOOFING

ROBOCALLS AND TEXTS CAN BE ANNOYING, FRUSTRATING AND - EVEN WORSE - FRAUDULENT. The FCC is committed to protecting you from illegal robocalls, texts and caller ID spoofing.

 Find web resources and learn more at www.fcc.gov/robocalls

FCC Response



Implementing new rules.



Ruling on issues addressed in comments and informal complaints.



Taking enforcement action.



Keeping consumers informed via presentations and materials distribution.

Common Questions

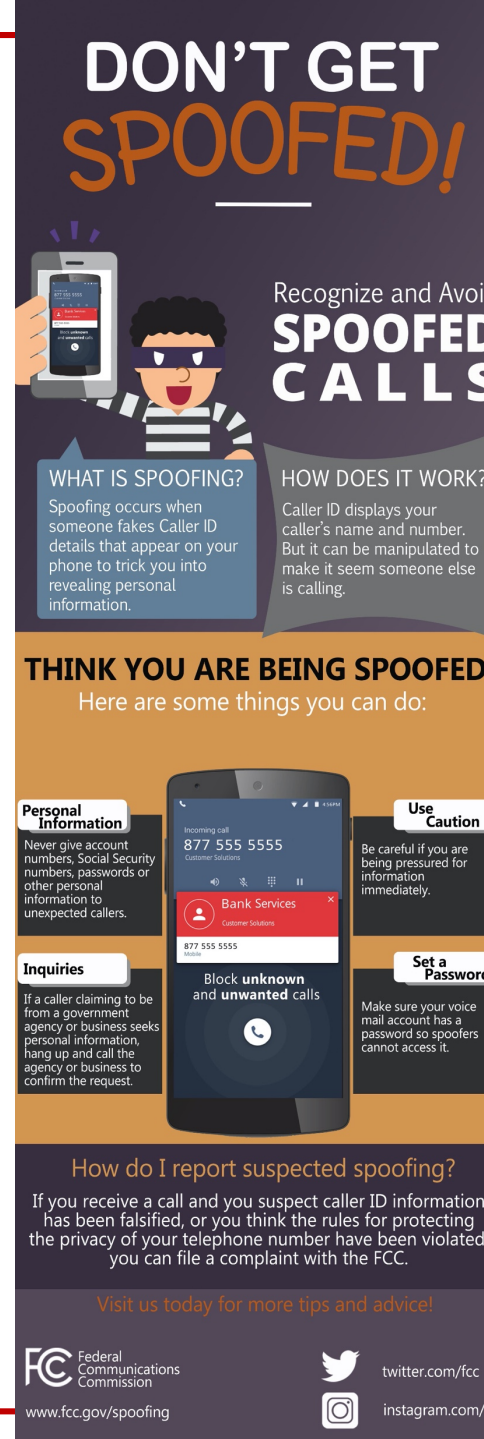
- How do you recognize potential scam?
- What do you do if you think you've been scammed?
- What you can do to lessen the number of unwanted robocalls, texts or emails you receive?

How can PHA staff help?

- Public Housing Authority staff and residents can benefit from knowing more about unwanted calls that can lead to scams.
 - Find additional info at:
 - www.fcc.gov/consumer
 - www.fcc.gov/outreach
- Important information to share with residents:
 1. During tax season, you might be the victim of a scam if you receive a call from someone saying they are with the IRS.
 1. They IRS will ALWAYS send you a letter if there is an issue with your taxes.
 2. Utility companies will never call requesting payment in the form of a gift card.

How can PHA staff help?

- Contact the FCC via outreach@fcc.gov, to:
 - Ask the FCC for materials to distribute to residents. The cards contain helpful tips.
 - “The Three Commandments”
 - Collect information and report attempted fraud..
 - Request that the FCC host topic-specific webinars for your residents.
 - Request a Train-the-Trainer Session on how to recognize and possibly decrease unwanted calls.
 - If local, request an in-person presentation.



DON'T GET SPOOFED!

Recognize and Avoid **SPOOFED CALLS**

WHAT IS SPOOFING?
Spoofing occurs when someone fakes Caller ID details that appear on your phone to trick you into revealing personal information.

HOW DOES IT WORK?
Caller ID displays your caller's name and number. But it can be manipulated to make it seem someone else is calling.


THINK YOU ARE BEING SPOOFED?
Here are some things you can do:


- Personal Information**
Never give account numbers, Social Security numbers, passwords or other personal information to unexpected callers.
- Use Caution**
Be careful if you are being pressured for information immediately.
- Inquiries**
If a caller claiming to be from a government agency or business seeks personal information, hang up and call the agency or business to confirm the request.
- Set a Password**
Make sure your voice mail account has a password so spoofers cannot access it.


Block unknown and unwanted calls

How do I report suspected spoofing?
If you receive a call and you suspect caller ID information has been falsified, or you think the rules for protecting the privacy of your telephone number have been violated, you can file a complaint with the FCC.

Visit us today for more tips and advice!

 Federal Communications Commission
www.fcc.gov/spoofing

 twitter.com/fcc

 [instagram.com/fcc](https://www.instagram.com/fcc)

Other Resources



Consumer Affairs and Outreach Division: outreach@fcc.gov and <http://www.fcc.gov/outreach>



Consumer Help Center: <http://www.fcc.gov/consumers>



Consumer Complaints Center: <https://consumercomplaints.fcc.gov/>



Scam Glossary: <https://www.fcc.gov/scam-glossary>



ConnectHome Nation Webinar

Q & A

