PIRG CONSUMER WATCHDOG

TIPS TO PROTECT YOURSELF FROM ROBOCALLS AND ROBOTEXTS

We frequently get asked: How can you identify a scam text, call or email? You really can't. The bad guys are better at this than we are. You should assume that any request is a scam if it's unexpected, and if you're asked to provide or confirm any information or to pay money or buy gift cards. Here are some robocall and robotext rules to live by and share with vulnerable loved ones.

On robocalls, the first two are most important, if you do nothing else:

1. Never confirm or provide personal information to any caller you weren't expecting, or pay something you weren't expecting to pay, no matter who they say they are. Don't provide your name, account log-in code, your address, your shoe size … Nothing. If someone calls and claims to be with a government office or company you do business with and you think the call may be legitimate, hang up and call them back at a phone number you look up independently.

2. Don't ever pay bills or debts with gift cards. Period. Full stop. Gift cards are for gifts or to make a purchase for yourself. No legitimate operation accepts gift cards to pay for an obligation — not the Internal Revenue Service or a jail or a bank.

3. If you get some kind of call that you're supposedly a victim of fraud or you're behind on taxes or your grandchild is in jail, call someone you trust before you do anything — maybe a friend, a trusted relative or a neighbor. Just saying what's going on out loud can help you realize it's a scam.

4. If any caller wants you to take action immediately or pressures you not to tell anyone about the call, hang up and contact a trusted relative or friend.

5. On your outbound voicemail message, don't provide your full name. There's no sense giving potential scammers information they may not already have.

6. Don't trust your caller ID. A call appearing to be from a neighbor or a government agency could be coming from a con-artist halfway around the world. A scammer could even potentially spoof a number in your contacts list. In the past, you presumably would recognize if the voice was unfamiliar. That's not even a sure thing these days given the rise of artificial intelligence technology that can spoof your voice.

7. Don't be fooled if a caller knows your name, address, family members' names or even your Social Security number. All of this and more was exposed for half of the adult population in the Equifax data breach of 2017 and numerous other breaches in recent years.

8. If you have a voicemail box with your phone line, set up a password. Some voicemail services give access to messages if you call from your own phone number. But if an identity thief spoofs your number

and there's no password, they potentially could access your messages and personal information.

9. Don't give your phone number to anyone who doesn't really need to reach you immediately, especially if they're going to put your number in a database. Instead, opt for email notifications from retailers, pharmacies, etc., particularly if you get your email on your cell phone.

10. For those times when you need to give a business a phone number, consider getting a free phone number to link to your phone, such as a Google Voice number. You can set it up to require callers to state their name before you decide whether to answer or let the call to voicemail. Using this number to make phone calls also prevents businesses from automatically capturing your real cellphone number when you call a toll-free number.

11. Use multiple robocall filters. Each one offers an opportunity to catch something that slips through the previous filter. You can route calls that are flagged straight to your voicemail. Start by asking your phone company what robocall filters it offers at no charge. For more information on call blockers, the FTC recommends consulting with the CTIA, the wireless industry's trade association.

Here are lists of reputable robocall filtering software for cell phones. Some are free; some cost money.
For Apple (iOS):
https://www.ctia.org/consumer-resources/how-to-stop-robocalls/ios-robocall-blocking/
For Androids:
https://www.ctia.org/consumer-resources/how-to-stop-robocalls/android-robocalls-blocking

12. Never respond in the affirmative to unknown callers who ask something like, "Can you hear me?"

13. If you answer an unwanted call, never press a button to be removed from the call list or call a number back to get off their list. It doesn't work; it just lets the caller know there's a live person at this phone number. Just hang up. Never call back.

14. If you don't want to receive sales calls, register your phone number with the federal Do Not Call Registry. Legitimate businesses will honor your request because it's the law. Registering with the Do Not Call Registry also gives you more legal rights to file complaints.

15. Report illegal/unwanted robocalls and texts:
** Call the FTC at 1-877-382-4357 or file a complaint online at ftc.gov/complaint
** Report scam robocalls or texts to the Federal Communications Commission.
** Report Do Not Call List violations to the Federal Trade Commission. (Or sign up if you haven't.)

You should note the number on your Caller ID and any number left on the message that you're supposed to call back. You should also report illegal or unwanted calls to your state attorney general. See the contact information for the attorneys general in every state here.

16. If you continue to get more than a few illegal robocalls a week, complain to your phone company and ask what more it can do to help protect your privacy. Companies are allowed to block spoofed and known scam calls, provide on-screen warnings of suspicious calls, offer to let customers divert calls with the caller ID blocked to voicemail, etc.

17. Consumers whose landline providers don't do a good enough job of filtering robocalls may consider buying a phone that requires the caller to announce their name or else the call won't ring. They're available for $50 or less. This is a particularly good idea for older folks who like to answer all calls and may be more trusting.

18. Vow to do more to protect your friends and relatives, especially the most vulnerable. We should occasionally strike up conversations with loved ones about scams that are out there and make sure those we care about know they can talk to us if there's ever a question about a call or text message they received. And we should never belittle people who fall for scams. We need to eliminate the stigma so people feel free to reach out for help.

On robotexts, there are some additional warning signs and advice:

1. If you get a text message from an entity that you never agreed to get texts from, the message is almost surely an attempt to defraud you. Entities that send robotexts are required to get upfront consent before sending any messages.

2. If you get a text you weren't expecting or from a company you've never exchanged texts with before, watch out.

3. If a text is urging you to act immediately, don't do it. Scammers trick us by causing us to think we have to do something right now — pay a debt, buy gift cards, stop fraud —or else bad things will happen. Scammers hope people won't take a moment to think through the request.

4. If a text contains awkward language or spelling or grammatical errors, it's likely not coming from the entity it claims to be from: a bank, a government office, FedEx, Amazon, etc.

5. If the text appears to be from an email address instead of a phone number or five-or six-digit sender, it's more likely to be a scam.

6. If you get a suspicious text and you've already opened it, send it to your carrier by forwarding it to 7726 (SPAM). And report it to the Federal Communications Commission.