MASSPIRG Education Fund

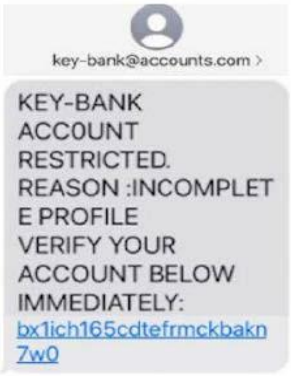
Tips to avoid robocalls, robotexts and scams

Unexpected means trouble. **Unexpected calls, texts or emails** are a red flag.

Two easy ways to protect yourself from scams:

1. Never give personal information to anyone who contacts you unexpectedly, no matter who they say they are. Not your name, your ZIP code, your shoe size … Nothing.

If you think a call, text or email could be legit, call the bank or the relative or the company or government office, using contact information you look up independently and know is correct. Call the number on the back of your bank card, or the number on your internet provider's statement, for example. Log into your credit card or Amazon account. Said another way: Assume every unexpected call, text or email has bad intentions. (The text to the right is fake.)



2. Never pay for something you weren't expecting to pay for with gift card numbers or money through Zelle, Venmo, CashApp or another instant option.

In general, you shouldn't send money through Zelle, Venmo, etc. to anyone who isn't a close relative or friend. Don't be fooled by an urgent request to supposedly pay back taxes or bail your grandchild out of jail or avoid a utility shutoff or claim your sweepstakes prize.

Real companies and government offices don't ask for gift cards or person-to-person payments. Remember this: Gift cards are for gifts, not debts.

WARNING WORDS

If a caller says any of these things, hang up. Call a friend or your bank.

- "This is urgent."
- "Don't tell anyone."
- "Your account has been hacked."
- "Don't hang up."
- "You must go withdraw cash now."
- "You need to go buy gift cards."
- "You have unpaid taxes."
- "We will have you arrested."
- "Your computer has a virus."
- "Pornography was found on your computer."
- "Go put cash into an ATM." (It's likely converting your cash to crypto currency, which you cannot recover.)

TOLD TO ACT IMMEDIATELY? THAT'S A RED FLAG

Legitimate companies and government offices will never threaten you and tell you to act that exact minute. Hang up if you are:

- Asked to provide a code sent to you by someone trying to confirm your identity.
- Accused of a crime.
- Told your computer has a virus.
- Asked to open another bank account.
- Threatened that something bad will happen if you don't comply.
- Told you won a contest you don't remember entering.
- Asked to pay money in any way besides a credit card.
- Told a loved one is in danger.
- Told you missed jury duty.
- Told you have a deadline to act.

OTHER TIPS

1. If a call or text urges you to provide information, pay money or buy gift cards immediately, take a breath. Call a trusted relative or friend to help you sort out what's going on. Sometimes just saying it out loud helps someone recalibrate.

2. Vow to do more to protect your friends and relatives, especially the most vulnerable. We should strike up conversations with loved ones about scams that are out there and make sure they know they can talk to us if there's ever a question about a call or text message they received.

3. We should never belittle people who fall for scams. We need to eliminate the stigma so people feel free to reach out for help.

4. 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 who has spoofed the number.

MASSPIRG Education Fund

In the past, you presumably would recognize someone impersonating a loved one or co-worker. That's not even a sure thing these days with artificial intelligence technology that can clone our voices easily.

5. Be careful when looking up phone numbers. Bad guys create lots of fraudulent customer service numbers to trick us. Yes, scams happen this way. See our guide: How to avoid imposter phone numbers, emails and more

6. 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 has been exposed in the parade of data breaches, including the massive breach involving National Public Data this year and the whopper involving the credit bureau Equifax in 2017.

7. 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.

On your *home phone/landline*, you can get a free call filtering service. Nomorobo and YouMail are ones to consider.
On your *cellphone*, the FTC recommends checking with the CTIA, the wireless industry's trade association. Here are options to find 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

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

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

10. 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.

11. Report illegal or unwanted robocalls and texts:
● Contact the Federal Trade Commission at 1-877-382-4357 (1-877-FTC-HELP) or file a complaint online at ftc.gov/complaint
● Contact 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.
● Contact your state attorney general. The contact information for the attorneys general for every state is here.

12. 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.

13. 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 about $50. This is a particularly good idea for older folks who like to answer all calls and may be more trusting.
Here are two to consider. (This writer actually bought the first one for an elderly relative; these kinds of phones work great:)
● AT&T cordless phone - caller ID announcing, call-blocking (with 2 handsets and answering machine)
● Panasonic cordless phone - robocall blocking (blocks calls from computers,) caller ID announcing, call blocking (with 1 handset and answering machine)

ADDITIONAL WARNING SIGNS FOR ROBOTEXTS

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 Trade Commission and the Massachusetts Attorney General's office, 617-727-8400 or file an on-line complaint here: https://www.mass.gov/how-to/file-a-consumer-complaint.

7. If you regularly get texts you want from your pharmacy or airline or your bank or your doctor, add them as a named contact on your phone. That will help you spot imposters.

MASSPIRG Education Fund
March 2025