



Business Impersonator Scams

Here's how they work:



You get a call, email, text, or message on social media that looks like it's from a business you know. It says there's a problem with your account, or you won a prize. It tells you to call a number or click a link.

But the message isn't really from a familiar business, it's from a scammer. If you call, they'll tell you to send payment or give personal information. They'll insist you can only pay with gift cards or cryptocurrency, or by wiring money or using a payment app, which no honest business will do. Or they'll ask for your Social Security number or access to your computer.

But it was never really that business contacting you, there wasn't a problem, and there was never a prize.

Here's what to do:

- 1. Stop.** If you get an unexpected call, email, text, or message on social media — even if it looks like it's from a business you know — don't click any links. And don't call phone numbers they give you. These are often scams.
- 2. Pass this information on to a friend.** You may not have gotten one of these messages, but chances are, you know someone who has.



Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...*Pass* it ON

Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Go online: **ReportFraud.ftc.gov**
- Call the FTC at 1-877-FTC-HELP (1-877-382-4357)
or TTY 1-866-653-4261

Your report can help protect other people. By reporting fraud, you can help alert law enforcers across the country who investigate and bring cases against scammers. Your report makes a difference.



**FEDERAL TRADE
COMMISSION**

August 2023

ftc.gov/PassItOn