Protect Yourself from Impersonation Scams

ASK WHY. VERIFY.

A consumer education campaign brought to you by:

INSTITUTE for MARKETPLACE TRUST℠ | amazon

What is an impersonation scam?

Impersonation scams occur when a scammer pretends to be a trustworthy organization or person to steal your money or personal information.

How impersonation scams work

Impersonation scams are perpetrated in a wide variety of ways—by phone, email, text, or by messaging you on social media. Scammers seek to get you to make a payment of some kind, share personal information, or give them access to your computer by pretending to be a well-known organization with whom you've likely engaged in some manner.

Business impersonation scams were the category most frequently reported to BBB Scam Tracker℠. Below are a few examples, but please remember that scammers are creative and shift their tactics constantly. *This list is NOT comprehensive of all scammer tactics.*

Account integrity. You're told that hackers have gotten access to your account — and the only way to protect it is to buy gift cards and share the gift card number and PIN on the back.

Tech support. A scammer posing as a tech support representative calls you at home and offers to fix a technical bug that you haven't even noticed, or a popup warning appears on your screen instructing you to dial a number for help. Scammers pose as tech support employees of well-known companies and hassle victims into paying for their "support." They may ask to get access to your computer to steal information or install ransomware or malware.

Rewards or prizes. Scammers may promise to provide money or prizes for testing and/or reviewing products for a well-known company. They will ask you to fill out a form via a malicious link to steal your personal information.

QR Codes. Be cautious if you receive an unsolicited message with a Quick Response (QR) code. Legitimate companies and businesses may use QR codes to point people to their websites, encourage app downloads or display menus, among other uses. But scammers can use QR codes to steal your personal information.

Order confirmation. You aren't expecting any packages, but you receive a phone call or text message saying that they cannot deliver the package. It urges you to click a link or call them back to verify address immediately.

Surveys. You receive a message asking you to fill out a survey. It looks like it came from a trusted brand but is really a scammer trying to get you to click on a malicious link or steal your information.

How to protect yourself from impersonation scams

Know how to spot an impersonation scam. Scammers will try to steal your personal information or money by:

Reaching out unsolicited to ask for personal information or payment for something.

Pressuring you to act immediately.

Asking you to wire money or send gift cards (untraceable forms of payment).

Threatening you in some way (for example, penalties or jail time).

Offering something that is "too good to be true."

Asking to access to your computer to assist you with your account.

If you're targeted by a scammer:

- **Stay calm.** If you are contacted by a possible impersonation scam, resist the urge to act immediately, no matter how dramatic the story is or how threatening or intimidating the caller sounds.
- **Don't reply directly**. Don't respond to the call, text, or email. Instead, call the company or person directly to verify the message or the phone call you received.
- **Go to the source or get help.** When in doubt, call your local BBB® to ask for a second opinion. If you made a purchase, always verify it and track it using company's app or website. Legitimate purchases will appear in your order history.
- **Never feel pressured to give personal information (SSN, account numbers/passwords, license number, etc.)** over the phone, especially if the call was unexpected. Scammers may impersonate a company's customer service, even spoofing a number. If you're unsure, end the call/chat and reach out directly to the company's customer service phone number or website.
- **Never pay over the phone, especially if the call was unsolicited.** To make a payment, you should be able to go directly to the organization's website.
- **Never allow remote access to your computer if somebody offers tech support.** Shut down your computer immediately and seek support directly from your service provider.
- **Search BBB Scam Tracker.** If you're suspicious about the situation, search BBB Scam Tracker to see if anyone else has reported a similar situation. The NEW BBB Scam Tracker enables you to search by email, URL, phone number, and more.
- **Check the email address or URL more closely.** Scammers use similar website addresses or emails to appear legitimate, but if you look closely, you may find one letter or number that is off.

ASK WHY. VERIFY.

Report scams to BBB Scam Tracker **(BBB.org/ScamTracker)**