Imposter Scams FAQs

What are imposter scams?

Cybercriminals often try to scam you by posing as somebody else, such as government officials, friends, family, and others. The cybercriminal's goal is usually to get money or your personal information.

What are the cybercriminals' tactics?

In imposter scams, cybercriminals may pose as anybody you might trust or fear and contact you via email, telephone, or text message. **Their common tactics include:**

- Threatening messages unless you pay a fee or fine
- Requiring you to "confirm" your account or personal information
- Offering a great product, service, or investment at a too-good-to-be-true price
- Pretending they urgently need money because of some dire event, like a family member getting arrested, hurt, or having their money stolen while on vacation

What are the types of imposter scams?

There are many different types of imposter scams, as listed below.

Business/job opportunity imposter scams — These involve cybercriminals advertising fake job openings and business opportunities on legitimate sites. The criminal may request a fee for job placement or your personal and/or financial information "for security purposes" or to "start the employment paperwork and set up direct deposit."

Charity imposter scams — These involve cybercriminals impersonating a legitimate or fake charitable organization to steal money and/or personal information.

Debt collection imposter scams — These involve cybercriminals pretending to be legitimate collection agents to trick or pressure you into paying money for debts that may have been paid, canceled, or don't even exist.

Education/scholarship imposter scams — These involve cybercriminals posing as school or university representatives and asking for "upfront fees" to ensure enrollment or to offer fraudulent "scholarship" assistance.

Family/friends imposter scams — These involve cybercriminals posing as a relative or friend, calling or sending messages requesting urgent financial help, such as for fees to get out of jail, pay a hospital bill, or leave a foreign country.

Government/military imposter scams — These involve cybercriminals posing as a government or military representative calling or sending messages urgently requesting you provide personal information and/or pay a fee or fine. The cybercriminals may also threaten to deny you services, arrest or deport you, or take other legal action if you don't comply.

Imposter Scams FAQs

Investment imposter scams —These involve cybercriminals promoting a high-paying investment opportunity and persuading you to "invest" in the fraudulent opportunity.

Prize/lottery/sweepstakes imposter scams — These involve cybercriminals claiming that you won a large amount of cash or other prizes and must provide a small claim fee, tax fee, or personal information to get the prize.

Romance imposter scams — These involve cybercriminals pretending to have a romantic interest in you, gaining your affection, and then using that goodwill to commit fraud.

Technical support imposter scams — These involve cybercriminals posing as a vendor or technical support representative claiming that your device needs to be scanned or repaired. A similar message may pop up on your computer or device screen. The cybercriminal's goal is to get paid for performing the service, plant malicious software on your device, and/or get your personal information.

What should I do if I'm targeted in an imposter scam?

- Be suspicious of sensational, too-good-to-be-true, upsetting, or threatening statements. Cybercriminals want you to react immediately without thinking.
- Verify the identity of the sender and ignore fraudulent commands and requests for action.
- Delete an unusual, unexpected email or text message and hang up on a telephone caller.
- Get the caller's name and (business) phone number, then call the organization / company using their phone number published on their website to verify a caller's identity and request.
- Do not click on any unexpected links or attachments as they may lead to malicious websites or contain malicious software.
- Never respond to a text message or email unless you know the sender is legitimate, as that tells the cybercriminal that they reached a real person (and increases the likelihood you'll get more fake messages).
- Never give credit card or personal information to an unsolicited phone caller.
- Never wire money or send gift cards to a stranger.

How do I learn more and report an imposter scam?

Learn more about imposter scams and where to report at: www.fightcybercrime.org/imposter-scams/