

Invoices, Emails, and Calls That Aren't What They Seem

Business Imposter Scams

In business imposter scams, criminals pose as legitimate companies, utilities, banks, or service providers. They may claim there is a billing problem, overdue balance, or account issue that requires immediate payment. The scammer often uses official-sounding language, logos, or invoices to appear legitimate. The goal is to collect money or financial information before the victim can verify the request.

RED FLAGS

- Unexpected demands for immediate payment to avoid service shutoff or penalties.
- Requests for payment through gift cards, wire transfers, or cryptocurrency.
- Emails or calls that pressure you not to contact the company directly.

BE SCAM SMART

- Contact the company using a phone number from a bill or official website, not the message you received.
- Do not make payments based on unsolicited calls, emails, or texts.
- Take time to review bills carefully and consult a trusted person if unsure.

Tech Support Scams

In tech support scams, fraudsters pretend to be representatives from well-known technology companies or internet providers. They claim your computer, phone, or internet service has a serious problem such as a virus or security breach. The scammer pressures you to act quickly and may ask for remote access to your device. Their goal is to steal money, install malware, or gain access to personal information.

RED FLAGS

- Unsolicited calls or pop-up messages claiming your device is infected or compromised.
- Requests to download software or allow remote access to your computer or phone.
- Demands for payment to fix a problem you did not notice.

BE SCAM SMART

- Do not trust unsolicited tech support calls or pop-ups—hang up or close the message.
- Never give remote access to your device unless you initiated the support request.
- If concerned, contact your technology provider directly using a trusted source.



Where to Report a Suspected Scam

- FBI Internet Crime Complaint Center (IC3): complaint.ic3.gov
- General fraud (FTC): reportfraud.ftc.gov
- National Elder Fraud Hotline: **833-FRAUD-11** (833-372-8311)
- Florida Office of Inspector General: **1-866-9-NO-SCAM** legacy.myfloridalegal.com/contact.nsf/contact?Open&Section=Citizen_Services
- The U.S Department of Health and Human Services Office of Inspector General: **1-800-447-8477** oig.hhs.gov/fraud/report-fraud

