Office of the Comptroller of the Currency

SAFE MONEY

GUARDING AGAINST FINANCIAL FRAUDS & SCAMS

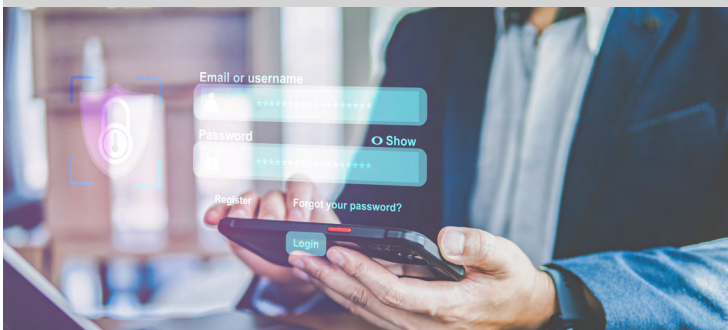
IMPOSTER SCAMS

Imposter scams involve fraudsters pretending to be someone you trust, such as a government official, family member, or a company representative, to steal your money or personal information.

The imposter uses this trust to deceive victims into sending money or sharing personal information.

RED FLAGS

- **Calls, emails, or texts** claiming to be government officials, law enforcement, or company representatives asking for immediate payments or personal information.
- **High-pressure tactics** demanding urgent payments, threatening arrest, legal action, or fines.
- **Untraceable payment requests** such as wire transfer, gift cards, or cryptocurrency.
- **Unusual grammar, awkward phrasing,** or language inconsistencies.
- **Unsolicited contacts** claiming money owed or needing to confirm personal details.
- **Fake websites** with poor design, low-quality images, or outdated logos. Be cautious if the site looks unprofessional or has obvious mistakes.



SAFE MONEY is a series of informational sheets developed by the Office of the Comptroller of the Currency (OCC) to help consumers recognize and avoid common financial frauds and scams.

COMMON METHODS

- **Business/Bank Imposters:** Pose as bank, credit card company, or business representatives asking for account information or money.
- **Charity Scams:** Pretend to represent charities, especially after disasters or during the holiday season, asking for donations that go directly into their pockets.
- **Family/Grandparent Scams:** Pretend to be family, often a grandchild, in distress and needing money urgently.
- **Government Imposters:** Pose as IRS agents or Social Security officials to extort payments or personal details.
- **Person-to-Person Payment Scams:** Trick you into sending money through payment apps.
- **Romance Scams:** Build emotional connections with victims online and then ask for money.
- **Tech Support Scams:** Impersonate tech companies and claim computer has a virus, attempt to gain access to system or charge for unnecessary services.

AVOID SCAMS

Verify the Source

- If someone claims to be a government official, independently verify their identity by directly contacting the agency through official channels.
- Before donating to a charity, use the IRS's tool to confirm charity is legitimate.

Don't Send Money or Personal Details

- Be wary of unsolicited calls, emails, or texts asking for money, Social Security numbers, bank details, or passwords. Avoid links or attachments provided in these communications. Never share personal information.

Hang Up on Robocalls and Pressure Tactics

- Hang up on automated calls from those you don't know. Legitimate agencies or companies won't demand immediate payments or personal information under the threat of consequences.

Monitor Accounts Regularly

- Set up account alerts for all transactions and review statements frequently for unauthorized charges or unusual and suspicious activity. Obtain free credit reports from AnnualCreditReport.com.

Stay Informed

- Subscribe to FTC Consumer Alerts to stay informed about common and new types of scams.

REPORT FRAUD

Taking swift and decisive actions when encountering an imposter scam can help protect your identity and financial well-being. Stay vigilant and always verify the authenticity of communications from an unknown source.

Alert Financial Institution

- If financial information was shared or payments were made, contact the financial institution immediately. Report the potential fraud and request a stop payment on any charges and monitoring of accounts for unauthorized transactions.

Place Fraud Alert on Credit Report

- Request a fraud alert or credit freeze on credit reports by contacting one of the three major credit bureaus. The first bureau contact will inform the other two.
- Fraud alerts – which last for one year and can be extended – make it hard for identity thieves to illegally open accounts in your name.
- Equifax: 800-525-6285; www.equifax.com
- Experian: 888-397-3742; www.experian.com
- TransUnion: 800-680-7289; www.transunion.com

Notify Relevant Agencies & Companies

- Visit FTC's ReportFraud.ftc.gov or call 877-FTC-HELP.
- Internet scams: Contact Internet Crime Complaint Center (IC3), a division of the FBI, at www.ic3.gov.
- IRS Imposters: Visit IRS Report Phishing.
- Social Security scams: Visit SSA Fraud Hotline or call 800-269-0271.
- Charity scams: Report to the actual charity and to the local State Attorney General. Find local State Consumer Protection Office.
- Tech support scams: Report to the actual tech company referenced by the scam.
- Romance scams: Report to the platform or social media site used for initial contact. Most have a "Report" or "Flag" button.
- Person-to-person scams: Report to the payment provider. Most offer a way to report fradulent activity directly through app or platform.

File a Police Report

- Contact or visit local police department to file a report with all the relevant information and documentation.

Office of the Comptroller of the Currency

Promoting a Safe, Sound, and Fair Federal Banking System

The Office of the Comptroller of the Currency's (OCC) mission is to ensure that national banks and federal savings associations operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.