



Office of the  
Comptroller of the Currency

# SAFE MONEY

GUARDING AGAINST FINANCIAL FRAUDS & SCAMS






## ONLINE & DIGITAL SCAMS

**Online and digital scams** occur via the internet, often through deceptive emails, websites, or messages that trick people into providing personal information or money.

These scams often come in the form of phishing emails, fake websites, or fraudulent online shopping schemes.

*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.*

## RED FLAGS

-  **Unsolicited texts, emails, and fake websites** that appear legitimate but are designed to steal personal or financial information. Misspellings, generic greetings, and old logos can be indicators.
-  **Online shopping scams** with non-existent goods or services after payment.
-  **Investment and loan scams** promising high returns or favorable loans that are fraudulent.
-  **Too good to be true offers**, such as winning a prize or getting products at significantly low prices.
-  **Unusual message from a friend** or contact, potentially indicating a hacked account.
-  **Remote access requests** often under the guise of fixing a computer problem.
-  **False receipts via email** of software purchase, such as anti-virus software, luring you to contact them.
-  **Ransomware/malware software** cutting off access to data or device and demanding a ransom to regain access.



## FRAUD METHODS

- Fake E-commerce Sites:** Fraudsters set up fake websites to sell products that are never delivered after payment is made.
- Phishing:** Emails or text messages that look like they're from legitimate companies, asking victims to click a link and enter sensitive information.
- Tech Support Scams:** Fraudsters pose as tech support representatives, claiming a computer virus needs immediate fixing, often gaining access to the victim's device.

## AVOID FRAUD

### Avoid Suspicious Links

- Do not click on links or download attachments from unknown sources, especially in unsolicited emails or texts.

### Use Strong Security Software

- Ensure devices are protected by up-to-date antivirus and anti-malware software.

### Verify Before Providing Information

- Always verify the legitimacy of websites and emails before entering sensitive information.

### Enable Two-Factor Authentication

- Use two-factor authentication (2FA) on all online accounts to add an extra layer of protection.

### Monitor Credit Reports

- Regularly review credit reports for any unauthorized inquiries or accounts, suspicious activities, or errors.
- Obtain free credit report from [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com).

## REPORT FRAUD

Online and digital fraud includes phishing, tech support scams, and fake e-commerce sites designed to steal personal information or money.

Always remain vigilant and proactive in protecting your financial information.

### Report to the Federal Trade Commission

- Visit FTC's [ReportFraud.ftc.gov](http://ReportFraud.ftc.gov) to report the fraud, providing as many details as possible. Or call 877-FTC-HELP (877-438-4338).

### Contact the Internet Crime Complaint Center

- Submit a complaint to the IC3, a division of the FBI, at [www.ic3.gov](http://www.ic3.gov).

### File a Police Report

- Contact or visit local law enforcement agency to file a report with all relevant information and documentation.
- Some law enforcement agencies have specialized cybercrime units.

### Notify Federal Agencies

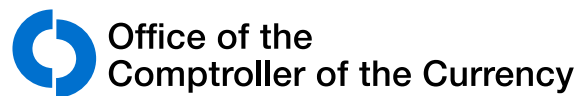
- Investment fraud: Securities and Exchange Commission: [www.sec.gov](http://www.sec.gov); 800-SEC-0330
- Telecommunication scams: Federal Communications Commission: [www.fcc.gov/complaints](http://www.fcc.gov/complaints); 888-225-5322
- Mail scams: U.S. Postal Inspection Service, [www.uspis.gov](http://www.uspis.gov); 877-876-2455

### Report to Social Media & Online Platforms

- Report fraudulent activities to social media platform.
- Contact customer service or website reporting tools.
- Report immediately to payment service provider customer support.

### Alert Financial Institutions

- Notify your bank, credit card companies, or other financial institutions involved.
- Cancel any affected cards and monitor accounts for unauthorized transactions.



## 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.