CLARITY POINT
FINANCIAL PARTNERS

A Hightower Company

How to Protect Yourself from Online Scams and Digital Fraud

Online scams continue to rise, with the FBI reporting losses over $16 billion in 2024.[1] The true number is likely higher, as many incidents go unreported. While tactics are becoming more sophisticated—especially with the use of AI—most scams still rely on the same core tactics, which are urgency, impersonation, and deception.

The good news: once you know what to look for, many scams are easier to recognize and avoid. Below are common scams to be aware of this year.

Common Scams to Watch For

EMAIL PHISHING

Scammers send emails that appear to come from trusted organizations you use, such as banks, advisory practices, retailers, and service providers. They attempt to get your information by asking you to click a link or provide personal information.

watch for:

- Unexpected emails requesting action
- Links that take you to login pages
- Slight misspellings in email addresses

TEXT MESSAGE SCAMS (SMISHING)

Fraudulent texts about deliveries, unpaid tolls, DMV notices, account alerts, or refunds.

watch for:

- Messages asking you to click a link or "fix" an issue
- Unknown numbers creating urgency
- Requests for personal or payment information

IMPERSONATION & AI VOICE SCAMS

Scammers may pose as a financial institution, colleague, or even a family member using AI–generated voices or messages.

watch for:

- Urgent requests for money or sensitive information
- Requests to keep the situation confidential
- Unusual communication methods or tone

QR CODE SCAMS

Fraudulent QR codes may appear in emails, packages, or public places and direct you to malicious websites.

watch for:

- Unexpected QR codes asking you to log in or provide information
- Codes from unknown or unverified sources

TECH SUPPORT SCAMS

Pop-ups or calls claiming your device is compromised and urging immediate action.

watch for:

- Unsolicited warnings about viruses or security issues
- Requests for remote access or payment

IDENTITY THEFT & ACCOUNT TAKEOVER

Scammers use stolen personal information to access accounts or open new ones.

watch for:

- Unexpected account alerts
- Unrecognized transactions
- Missing bills or statements

KEY RED FLAGS

If you notice any of the below, take a moment to stop and ask yourself:

- Is this message unexpected?
- Does it create a sense of urgency or pressure?
- Is it asking for money, login credentials, or security codes?
- Does it include a link, attachment, or QR code?
- Is it asking me to keep the request confidential?

How to Protect Yourself

These simple habits can help reduce your risk:

- Going directly to trusted websites or apps instead of clicking links
- Using multi-factor authentication (MFA) wherever available
- Keeping devices and apps updated
- Avoiding accessing sensitive information on public Wi-Fi
- Limiting what you share on social media
- Monitoring financial accounts regularly

Note: If something doesn't feel right, don't click on any links, reply or engage in any way. Instead, you should report suspicious messages both with your email provider and to the organization that is being impersonated. When contacting the organization that is being impersonated, make sure you reach out to them via a known, trusted number or website. It is also a good rule of thumb to routinely monitor your accounts for any unusual activity.

a note to our clients

We continue to strengthen our systems and processes to help protect your information and accounts. However, many scams rely on direct interaction with individuals.

If you ever receive a message that appears suspicious or references your financial accounts, please contact us. We are always here to help you verify and stay protected.

CLARITY POINT FINANCIAL PARTNERS

A Hightower Company

FIVE GREENTREE CENTRE

525 ROUTE 73 NORTH, SUITE 306

MARLTON, NJ 08053

(856) 291-9300

CLARITYPOINT.HIGHTOWERADVISORS.COM

[1] *FBI releases annual internet crime report. (2025, April 24). Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report*