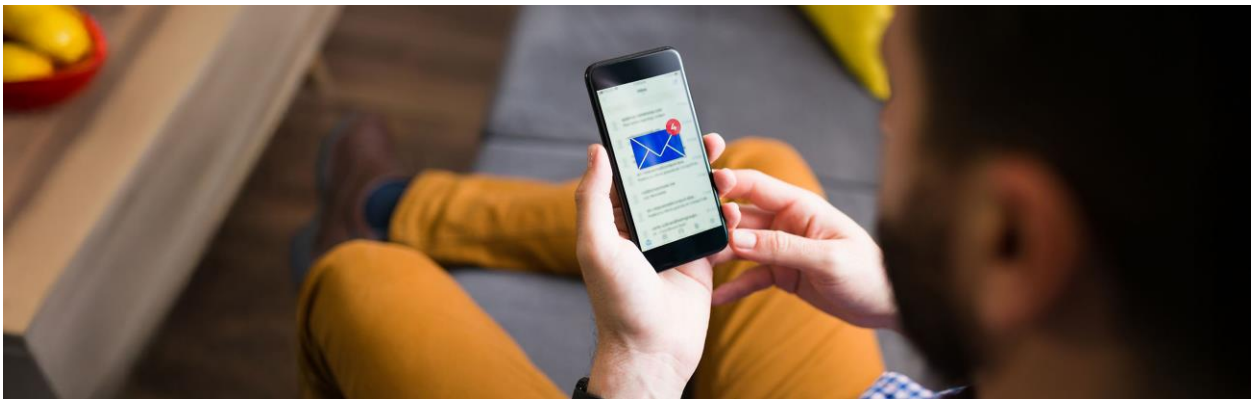

Top Scams to Watch Out For

Learn about the top scams and tactics fraudsters use to trick victims.

Key Takeaways

- Cybercriminals use sophisticated tactics to impersonate trusted sources and create a false sense of urgency.
- Avoid clicking on links or opening attachments in unsolicited emails or text messages and never grant remote access to your electronic devices.
- Even if you receive a call from a number you recognize, don't provide the caller with sensitive personal data. Instead, hang up and call back using a verified phone number.

Cybercriminal activity continues to evolve as fraudsters develop more sophisticated tactics to trick unsuspecting individuals.

Many of the latest scams utilize social engineering or the use of false pretenses to try and convince victims to share personal information. The initial request may seem innocuous, but the information you give up could be deviously deployed later to initiate an attack against you.

Watch Out for These Common Scams

1. Investment Scams

You receive a lucrative offer from a financial expert to invest in the financial markets with the promise of quickly making money at no risk. All you need to do is hand over your funds and your investments will grow in no time. Sounds great, right?

In this type of scam, fraudsters often leverage social media platforms and group chats to impersonate legitimate financial industry professionals. They promise free financial guidance, but once they have your money, they disappear, along with your funds.

Security tips: Morgan Stanley leadership and personnel will never reach out to you via social media or group chat to conduct business. If you receive outreach about an investment opportunity offered by or affiliated with Morgan Stanley via these channels, you should treat it as fraudulent and immediately reach out to your Morgan Stanley Financial Advisor or contact us at 888-454-3965.

2. Tax Scams

Scammers may impersonate the Internal Revenue Service (IRS) by calling you and saying you owe back taxes. They may even threaten you with a lawsuit or jail time if you don't immediately pay the debt with a wire transfer, prepaid card or gift card.

What's wrong with this scenario? If you owe taxes, the IRS won't call you. Instead, the agency will contact you by mail. In addition, the IRS will never ask for money using those payment options or threaten to arrest or sue you.

Security tips: If you receive a call like this, hang up immediately without providing any personal or financial information. Then report the call to the Treasury Inspector General for Tax Administration(opens in a new tab) (TIGTA) or Federal Trade Commission(opens in a new tab) (FTC).

3. Computer Tech Scams

Have you ever received a call from someone telling you there's a serious problem with your computer? It's likely a fraudster seeking remote access to your device in order to "fix" the issue. Instead, they'll infect your computer with malicious software, aka malware.

Security tips: Never grant access to your device when you receive this type of call. Don't provide the caller with any personal, account or computer-related information. Instead, ask the caller for their name, as well as the name of their company. Then hang up and call back using the company's official phone number.

4. Online Dating or Romance Scams

Be leery of people you've met online – often through dating or social media sites – who initially seem romantically interested in you, but, as time goes on, ask for money (usually by wire transfer, gift card or cryptocurrency) to pay for a medical emergency, the cost of travel to visit you or some other reason.

Security tips: Avoid sending money or gifts to someone you've never met in person. Ask anyone you meet online plenty of questions and look for discrepancies in their answers. If you feel someone is trying to scam you, stop all contact with the perpetrator immediately.

5. Advance Fee and Lottery Scams

While the details of these schemes vary, they all involve a fraudster asking you to pay a small fee upfront in exchange for a larger return later. The payout you're promised may be connected with a lottery winning or special gift. After paying the fee, you'll receive little or nothing of value in return.

Security tips: Don't conduct business with someone you haven't researched on your own to confirm their authenticity. Also, don't sign any non-disclosure or non-circumvention agreement that's designed to prevent you from independently verifying the credentials of the person offering the opportunity.

Check with your local police, contact the Better Business Bureau or speak to your Financial Advisor or lawyer for additional guidance.

6. Charity Scams

Using the name of an organization that's similar to a well-known, reputable charity, fraudsters employ high-pressure tactics (usually during the holidays) to encourage you to donate on the spot.

Security tips: Ask for detailed information about the organization and take the time to confirm it's one worthy of your support. Don't feel the need to give money right away on the phone. You can always donate later through the charity's official website once you've done your homework. You may want to consult a charity watchdog site to help with your research.

How Do Fraudsters Pull Off a Scam?

Let's start by examining three tools used to perpetrate scams: phishing, vishing and SMiShing.

1. Phishing:

Phishing starts with an email that often looks like it's from a trusted or legitimate source. The email will ask you to do something – usually click on a link or download an attachment.

The link typically takes you to a website that seeks to steal your information or attempts to download malware onto your computer. Meanwhile, opening the attachment may infect your computer with malware.

Once the malware invades your computer, a hacker can use it to look at personal documents saved on your computer. They can also capture the keystrokes on your computer (or take screenshots of sites you visit) to harvest your logins, passwords and other sensitive information. After hackers steal your information, they'll often try to access your bank accounts or contacts or sell your data to other cybercriminals.

Security tips: Never click on a link or open an attachment from unsolicited sources, and don't provide personal information when responding to an email request.

2. Vishing:

With this phone scam, a fraudster calls you and poses as a representative from a reputable organization, often times your bank or financial institution, to obtain your personal information. Vishing calls usually have a sense of urgency or panic to make you more likely to share the requested data.

Security tips: Only answer phone calls from numbers you recognize. You should not give out your personal information over the phone when you receive an unsolicited inbound call. Before you respond, make sure the person asking for the information is from a legitimate organization and is who they claim to be. You can always hang up and call the organization back using a phone number found through a trusted source – such as the company's mobile application, official web site or a financial statement.

3. SMiShing:

Short for "SMS phishing," this occurs when a cyberthief tries to fool you into providing them with your personal information via a text message or attempts to get you to click on a link in the text. The fraudster may also try to download malware onto your mobile device.

Security tips: Just like with phishing emails, never click on unknown links embedded in a text message, especially from a sender you don't recognize. If you have any doubt about the authenticity of the sender, don't respond. Instead, do research to verify the validity of the sender.

Designating a Trusted Contact to Help Prevent Fraud

With scams on the rise, protecting your assets and personal information remains our top priority. One way to help protect yourself or your loved ones' accounts from fraud and financial scams is to **add a trusted contact**. A **trusted contact** is a person you designate to be contacted if we are unable to reach you or if there are concerns regarding your well-being or potential financial exploitation. It is important to note that a trusted contact does not have permission to access account details, make decisions or perform any actions on your behalf. This individual serves as an additional layer of defense in case issues arise.