Cyber Fraud Resources

Common tactics used to steal login credentials

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the investor protection checklist are intended to help you and your family better protect yourselves against such activity.

Malware

Using malicious software (hence, the prefix "mal" in malware), criminals gain access to corporate and private computer systems and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.

How it works: While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email attachment.

Phishing

Phishing is a popular tactic used by cyber criminals to steal account information or login credentials. It is essentially a fake electronic message designed to trick you into divulging information and/or granting access that you shouldn't. This is often accomplished with the help of a fake website that strongly resembles a real site.

How it works: Masquerading as a known entity, or one with which the victim may have a financial relationship (e.g., a bank, credit card company, brokerage company), the criminals lure victims into opening email links or attachments. Doing so may direct victims to provide sensitive information on a fake website, or it may install malware to capture login and account information.

Credential Replay

It's common practice for people to use one password on many sites. However, doing so leaves people vulnerable to credential replay attacks.

How it works: Attacks occur when a criminal obtains the password for one compromised account and then tries to use it to log in to other accounts. The more a password is reused, the more chances there are for that password to be compromised or stolen.

Investor protection checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Manage your devices.	• Install the most up-to-date antivirus and antispyware programs on all devices and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device. • Access sensitive data only through a trusted device and secure Internet connection; avoid use of public Internet connections other than through a Virtual Private Network (VPN). • If you have children, set up a separate computer they can use for games and other online activities. • Keep operating systems and software up to date (PCs, laptops, tablets, smartphones). Many updates are made to resolve recently identified security risks. • Do not install pirated software. It often contains security exploits. • Frequently back up your data in case of ransomware attacks.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.

Fidelity INVESTMENTS

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Protect all passwords.	• Avoid storing passwords in email folders or un-encrypted files on your computer. Consider using a password manager program instead. These programs help generate and manage complicated passwords. • Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity. • Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships, and avoid using a single password across multiple sites. • Utilize multi-factor authentication, especially for financial and email accounts.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Surf the web safely.	Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly, without the proper protection of a secure VPN connection.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect information on social media.	Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that criminals will use to learn critical facts about people.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect your email accounts.	• Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account. • Use secure data storage programs to archive critical data and documents. • Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action. • Establish separate email accounts for personal correspondence and financial transactions. • Choose a unique password and utilize multi-factor authentication. • Review all emails carefully before clicking on links or attachments.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Safeguard you financial accounts.	• Consider contacting the three major credit bureaus to add a "security freeze" and prevent new accounts being opened in your name: – **Equifax:** 800-685-1111 – **Experian:** 888-397-3742 – **Transunion:** 888-909-8872 • Lock down personal credit reports with Experian®, TransUnion®, and Equifax®. Proactively enroll in an identity theft protection service to protect personal data. • Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held. • Never send account information or personally identifiable information over email, chat, or any other unsecured channel. • Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website's URL into the browser yourself. • Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.

Information provided in this document is for informational and educational purposes only. To the extent any investment information in this material is deemed to be a recommendation, it is not meant to be impartial investment advice or advice in a fiduciary capacity and is not intended to be used as a primary basis for you or your client's investment decisions. Fidelity and its representatives may have a conflict of interest in the products or services mentioned in this material because they have a financial interest in, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services including Fidelity funds, certain third-party funds and products, and certain investment services.

Fidelity Institutional Asset Management® (FIAM®) provides registered investment products via Fidelity Distributors Company LLC, and institutional asset management services through FIAM LLC or Fidelity Institutional Asset Management Trust Company.

Fidelity Clearing & Custody Solutions® provides clearing, custody, or other brokerage services through National Financial Services LLC or Fidelity Brokerage Services LLC, Members NYSE, SIPC.

934224.1.0 1.9899622.100