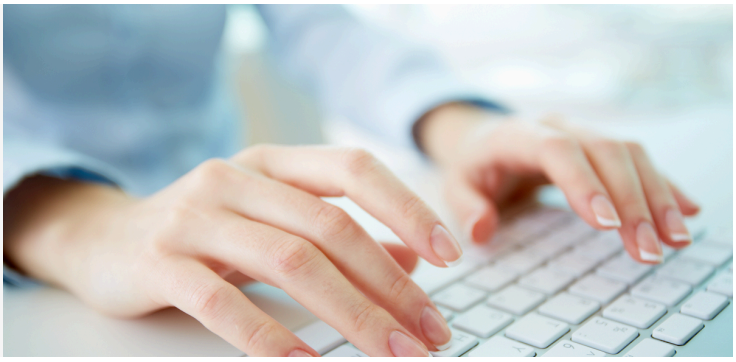
Prevent Phishing Attacks

DATA & CYBERSECURITY

Phishing scams are growing more sophisticated. Here is a checklist of things to do to recognize and avoid these scams so you can protect both your identity and your assets.



According to the Financial Industry Regulatory Authority (FINRA), typical phishing attempts now use the names of real people or organizations, including financial institutions, credit card companies, electronic payment services, mail delivery services, and other familiar providers, and can originate from email addresses that appear to legitimately belong to those entities.*

Take a Breath Before You Act

☐ **Hold off acting on "urgent" messages.** Before you respond to a call or email demanding your attention about an urgent situation, take a breath instead of giving in to the instinct to act.

☐ **Don't respond to any email requests for personal or financial information.** Financial institutions as a practice don't ask you to provide sensitive information, such as your Social Security Number or account numbers, in response to emails.

☐ **Think before you click.** Emails "phishing" for your data often include infected attachments or links to fake websites. Even if you know the sender, clicking a link in an email or instant message is generally not recommended.

Look Out for These Tells

☐ **Watch out for emails with "invoice" in the subject line.** Scammers often send suspicious emails that contain PDF attachments claiming to be an invoice paid, locked PDF asking you to enter a user name and password to unlock.

☐ **Beware of unexpected messages.** While misspelled company names and jumbled website URLs were a clear tipoff to phishing ploys in the past, scammers have evolved their tactics and are now using ChatGPT and AI to make their phishing emails appear even more realistic.

☐ **Be wary of offers that are "too good to be true."** If you've learned by email that someone in Tasmania will give you a share of the $5 million settlement if you front $100 or that you'll receive a an inheritance from your great-aunt Martha (who you never knew you had) as soon as you provide your Social Security Number, just pass.

Use the Web Wisely

☐ **Use your own device.** If possible, avoid using public computers or devices that aren't yours to access your financial accounts.

☐ **Use only secure networks to access your financial accounts.** Consider enabling multi-factor authentication (MFA), if available, and be sure to create strong passwords for your accounts and any financial apps you use.

☐ **Look for the HTTPS lock.** Legitimate websites use Secure Sockets Layer (SSL) to encrypt data before it's transmitted across the web. The secure areas, where you might provide your sensitive information, are marked with a lock icon, which generally appears next to the website address, also called a uniform resource locator or more commonly a URL. If you double-click on the icon, you'll also see details about the site's security.

☐ **Regularly review your account statements and activity for any unrecognized transactions.** Immediately report any suspicious activity to your financial institution. Check your credit report annually as well, looking for accounts you didn't open and any unexplained activity

Reach the Right Place

☐ **Verify the claim by independently logging on to the company's main website.** Alternatively, call using a telephone number obtained from a separate source. For instance, type the URL found on a legitimate account statement directly into your browser, check the account using the associated app on your mobile device or call the phone number found on the back of your credit card.

Working With Janney

Depending on your financial needs and personal preferences, you may opt to engage in a brokerage relationship, an advisory relationship or a combination of both. Each time you open an account, we will make recommendations on which type of relationship is in your best interest based on the information you provide when you complete or update your client profile.

If you engage in a brokerage relationship, you will buy and sell securities on a transaction basis and pay a commission for these services. Our recommendations for the purchase and sale of securities will be based on what is in your best interest and reflect reasonably available alternatives at that time.

If you engage in an advisory relationship, you will pay an asset-based fee, which encompasses, among other things, a defined investment strategy, ongoing monitoring, and performance reporting. Your Financial Advisor will serve in a fiduciary capacity for your advisory relationships.

For more information about Janney, please see Janney's Relationship Summary (Form CRS) on www.janney.com/crs which details all material facts about the scope and terms of our relationship with you and any potential conflicts of interest.

Get the benefit of convenient, timely access to your accounts with Janney Online Access.

Checking your portfolio and financial plan progress is easy when you use Online Access. Transfer funds, store documents including wills and power-of-attorney permissions in a central Document Vault, and manage your eDelivery notice preferences.

---

* Phishing Scams: Stay Clear of the Bait, FINRA, April 2023, https://www.finra.org/investors/insights/phishing-scams