PREVENT PHISHING ATTACKS

Check it out: Everything is a little easier when you have a list of steps to help you accomplish your objective. Here are some things you can do to avoid being scammed through fraudulent emails.

✓ 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.
- ☐ **Look for typos.** While less a tell than in the past, some phishing emails and fake websites still have grammar and spelling errors, as well as missing trademark and copyright marks.
- ☐ **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 web browser pop-up blocker.** Hold off automatic pop-ups of malware that can divert a legitimate website visit to a fake one that simply looks good.
- ☐ **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.

✓ REACH THE RIGHT PLACE

- ☐ **Call the number on your account statement or credit card.** Rather than call a phone number provided in an email (or given to you by a caller you don't know), use one from a source you trust.

WORKING WITH JANNEY

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.