Financial Wellness

Four tips for protecting yourself from email scams

Fraudulent emails try to fool you into revealing personal information. Here are some tips to protect yourself.

2-minute read

1. Check the address and domain of all emails

If you notice the slightest discrepancy in the entity name or address, delete the email immediately, without clicking on any links or opening any attachments.

2. Consider calling the sender

If you are unsure of the legitimacy of an email, contact the sender by phone to confirm.

3. Be cautious of unusual requests, even those that appear to come from a trusted source

Even if an email appears to come from a trusted source, never click on links or open attachments that you were not expecting. Never respond to emails asking you to change your password or to provide your personal information, including your credit card number.

4. Keep your software up to date

Ensure that your computer's operating system, your web browser, and your anti-virus software have the most recent updates.

Email scams on the rise

Seasonal scams: You may start to receive fraudulent tax related emails during tax season. If you receive a threatening email that appears to come from the Internal Revenue Service (IRS), do not click on it. The IRS will never make initial contact with a taxpayer by email or phone. They will also never make threats of arrest to obtain payment of taxes.

Mortgage closing costs scams: If you receive an email with new wire instructions for your closing costs, confirm the instructions with your attorney. Fraudsters may have stolen your information by hacking into the database of other entities involved in the transaction, such as title companies.