Don’t take the bait: Here’s how taxpayers can avoid getting caught by a phishing scam

Data thieves don’t take a break during the holidays. In fact, the IRS warns taxpayers that the agency is seeing a large increase in bogus email schemes that seek to steal money or tax data.

The most common way for cybercriminals to steal money, bank account information, passwords, credit cards and Social Security numbers is to simply ask for them. Every day, people fall victim to phishing scams or phone scams that cost them their time and their cash.
Here are a few steps taxpayers can take to protect against phishing and other email scams. When reading emails, people should:

- **Be vigilant and skeptical.** Never open a link or attachment from an unknown or suspicious source. Even if the email is from a known source, the recipient should approach with caution. Cybercrooks are good at acting like trusted businesses, friends and family. This even includes the IRS and others in the tax business.
- **Double check the email address.** Thieves may have compromised a friend’s email address. They might also be spoofing the address with a slight change in text. For example, using narne@example.com instead of name@example.com. Merely changing the “m” to an “r” and “n” can trick people.
- **Remember that the IRS doesn't initiate spontaneous contact with taxpayers by email to ask for personal or financial information.** This includes asking for information via text messages and social media channels. The IRS does not call taxpayers with aggressive threats of lawsuits or arrests.
- **Not click on hyperlinks in suspicious emails.** When in doubt, users should not use hyperlinks and go directly to the source’s main web page. They should also remember that no legitimate business or organization will ask for sensitive financial information by email.
- **Use security software to protect against malware and viruses found in phishing emails.** Some security software can help identity suspicious websites that are used by cybercriminals.
- **Use strong passwords to protect online accounts.** Experts recommend the use of a passphrase, instead of a password, use a minimum of 10 digits, including letters, numbers and special characters.
- **Use multi-factor authentication when offered.** Two-factor authentication means that in addition to entering a username and password, the user must enter a security code This code is usually sent as a text to the user’s mobile phone. Even if a thief manages to steal usernames and passwords, it’s unlikely the crook would also have a victim’s phone.
- **Report phishing scams.** Taxpayers can forward suspicious emails to phishing@irs.gov