Don't get hooked: Know warning signs of a phishing scam

(BPT) - Half of the world's 7 billion inhabitants use email, generating 269 billion emails per day in 2017, according to technology market research firm The Radicati Group. Email is so commonly used in business and personal interactions that it's also become a prime avenue for scammers to attempt to trick people and companies into voluntarily giving up money and valuable information, like credit card or Social Security numbers.

The act of using email, text or copycat websites to commit fraud is called "phishing," and scammers use the tactic to steal money, information and identities, the Federal Trade Commission warns. Phishing is so successful — and so common — that the average business-user probably receives at least one risky email per day, according to the 2017 Spear Phishing Report by GreatHorn, a cybersecurity firm.

Spotting phishing emails

While October is National Cybersecurity Awareness month, consumers need to be vigilant against phishing attacks year-round, Western Union advises. The money transfer business cites common phishing email characteristics that you should watch for:

* Emails that are poorly written, with misspellings and incorrect grammar. For example, a familiar company name might be misspelled.

* Your name isn't included in the email's "to" line, indicating that the same email may have been sent to thousands of people. Emails that begin "Dear Valued Customer," "To Whom it May Concern," or even just "Hello" could be a scam.

* A URL that is suspicious or fake. To view a URL without clicking, just hover your mouse cursor over the "click here" or "take action now" hyperlinks in the email. If the URL doesn't

appear to be associated with a legitimate company website or appears suspicious in any other way, don't click it.

* You receive an email informing you of a security breach with one of your online accounts. The email threatens that your account will be suspended if you don't take immediate action. The email may ask you to go to a website or respond to the email with personal information, such as your account number, password, credit card number or Social Security number.

What to do

If you receive a suspicious email, Western Union advises these steps:

* Don't open the email or any attachments. Instead, delete it or, if your email service permits, report the email as phishing.

* Never follow links in a suspicious, unsolicited email, even if it's to "unsubscribe" from the sender.

* If an email appears to be from a company you actually do business with, claiming a problem with your account, instead of clicking on a link in the email or replying to the email, contact the company through other channels — by phone or the customer service link on the company's actual website. Ask customer service to verify whether there really is a problem with your account.

* Remember, if an organization is legitimately one you do business with, they shouldn't need you to tell them your account number — they should already have it. Nor should they need your password or other personal information. For example, Western Union does not send emails asking for your ID, password or personal information. If you're not sure whether an email is from Western Union or not, don't open any links, click on any attachments or provide any passwords or user IDs. Forward the original email to spoof@westernunion.com and then delete it.

* Likewise, be wary of emails claiming to be from government agencies such as the IRS. The IRS says it "never sends out unsolicited emails, and under no circumstances, requests immediate payments by money transfer, credit card information or pin numbers through email."

To learn more about phishing and other types of fraud, visit wu.com/fraudawareness. To report money transfer fraud using Western Union, call 1-800-448-1492 to file a formal fraud complaint.