



# VASSEY

## Financial Planning & Investments



### **5 Ways to Spot a Phishing E-Mail**

*Presented by Alex Vassey, CFP®*

Did you know that phishing (i.e., scam) e-mails account for about [91 percent of all cyberattacks](#)? In other words, nearly every cybersecurity issue you could think of—from viruses, to ransomware, to full-blown data breaches—starts with users accidentally clicking malicious links in e-mails.

On the technology end, spam filters and antivirus scanners combat the threat of phishing e-mails. But these security features aren't perfect. Inevitably, you'll find phishing e-mails in your inbox, and the only true "patch" is awareness. To help you protect your sensitive information against cyberthreats, let's review five telltale signs of a phishing e-mail and what to do when you've spotted a phish.

#### **1) Unexpected request**

You probably recognize the sender or the content of most e-mails you receive. But with phishing scams, victims are often faced with an unexpected request. A common ploy is the e-mail from a "friend" stranded in a foreign country. He or she just needs a one-time wire transfer of a few thousand dollars to make it home safely. How often does this scenario actually take place in real life? Requests like this one are unusual for a reason—they aren't legitimate.

#### **2) Urgent!!**

Most phishing e-mails prompt recipients for action ASAP; that way, there isn't time to process what you're reading and doubt its veracity. But think about it: How many times have you sent an e-mail that was really urgent? Typically, urgent requests are made by phone or in person, not via e-mail. This is one of the biggest signs of a scam.

#### **3) Poor grammar, spelling, or syntax**

Keep an eye out for typos and strange syntax, which are common features of malicious e-mails. Most phishing e-mails are sent from foreign countries, where computer crime laws may not be as strict as they are in the U.S. Even if U.S. law enforcement tracks down an attacker, the country in which the attacker resides may not cooperate. Scammers are much safer attacking us from abroad. Fortunately, their language can be a dead giveaway.

#### **4) Suspicious hover-over link**

Attackers want to convince you that you're going to a legitimate website, when instead they're sending you to a malicious one that could install malware on your computer or trick you into revealing your password. If you hover over a link within an e-mail and the URL doesn't match the description of the link, it might be a phishing site. When the URL doesn't look familiar, don't take



# VASSEY

## Financial Planning & Investments

a chance. If the e-mail regards an online account that you log into regularly, simply open up a new browser window and log in as you normally do. (Don't click that link!)

### 5) Asks for sensitive information

Phishing e-mails often ask you to "verify" your credit card number, social security number, or account password—something legitimate services wouldn't do. Never share sensitive information through e-mail.

### Don't take the bait!


Now that you know the signs of a phishing e-mail, what should you do if you spot one? It's simple: Just delete it! Many users feel compelled to report phishing e-mails to someone else—whether it's a coworker or the e-mail service provider—but if a suspicious e-mail is forwarded, it's more likely that the malicious link will be clicked. If we all get in the habit of recognizing and deleting suspicious e-mails, phishing will become a weaker threat altogether.

Sometimes, detecting phishing e-mails can be tough, even when you've seen a million before. Here are two recommendations to keep in mind:

1. **If you're unsure, press delete.** If an e-mail is causing you to hesitate, it's probably because something is "phishy." Trust your gut. In the event that you accidentally delete a legitimate e-mail, the sender will get in touch with you again, at which point you'll have more information to work with.
2. **Verify with the sender "out of band."** In other words, simply call the sender. Don't use a number provided from the e-mail, because it could be fake. If you don't have the actual number on hand, try researching the official website of the business or individual.

Many phishing e-mails tempt recipients with irresistible offers, but here's a legitimate deal: Keep these five signs in mind when checking your e-mails, and you'll be taking a major step toward ensuring that cyberattacks can't reach your networks.

###

*Alex Vassey is a CERTIFIED FINANCIAL PLANNER™ professional, a Registered Investment Advisor, and a Chartered Retirement Plans Specialist® with [Vassey Financial Planning & Investments](#), located at 140 Bountyland Road, Seneca, SC 29672. He offers securities and advisory services as a Registered Representative of Commonwealth Financial Network®, Member [FINRA](#) / [SIPC](#). Fixed Insurance products and services offered through CES Insurance Agency. He can be reached (864) 718-0600 or [alex@vasseyfpi.com](mailto:alex@vasseyfpi.com). [Certified Financial Planner Board of Standards Inc.](#) owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™ and  in the U.S.A.*