Great outcomes. Done well.

BAIRD

Gone Phishing

Wealth Management Insights | April 2019

Phishing – the fraudulent practice of using seemingly reputable emails to con recipients out of personal or financial information – is a big business, costing U.S. companies and consumers more than $500 million every year.[1] Yet you can keep your private information private – it just takes a little detective work and due diligence when reviewing your inbox. In this month's Wealth Management Insights, we look at the most common red flags that an email you received is actually an attempt to steal your personal information.

According to a recent McAfee survey, 97 percent of consumers were unable to correctly distinguish between legitimate emails and attempts at phishing.

What you should know:

Who is it from?

- You don't recognize the sender or their email address.
- You recognize the sender, but the email is unusual or out of character for this person.
- The sender's email address is from a suspicious or unfamiliar domain. (An email address's domain is everything after the @, like "rwbaird.com.")

Who is it addressed to?

- You were cc:ed on an email yet don't recognize the other recipients.
- The email was sent to an unusual mix of people, such as those whose last names start with the same letter.
- The list of email recipients looks like it's from someone's personal contacts.

When was it sent?

- It was sent at an unusual time, such as business correspondence emailed at 3 a.m.

What is the subject line?

- The subject line begins with "RE:" yet is not a response to something you sent or requested.
- The subject line does not relate to the content of the message.

Are there attachments?

- The email includes an attachment you're not familiar with or weren't expecting. (Email attachments are a common avenue for malware or viruses to compromise your computer.)

- The attachment is a .DOC, .XLS, .PDF or .ZIP file. While these file types are commonly used in everyday life, they're also frequently used to transmit malicious code.

What is the email about?

- The sender wants you to perform some electronic action (i.e., open an attachment or click a link) to either avoid a negative consequence or to gain something of value.
- You're unexpectedly being asked to sign in to an account (i.e., provide your user name and password).
- The electronic action you're asked to complete seems illogical or poorly defined.
- The email contains conspicuous spelling and grammatical errors.
- You have an uncomfortable feeling about the sender's requests.

Are there any hyperlinks?

- When you hover your mouse pointer over a hyperlink, it displays a link-to address for an unexpected website.
- The link-to address seems legitimate but begins with unexpected coding like "data:text/html" instead of "http:" or "https:".
- The email contains long hyperlinks with no further information.
- The hyperlink has a misspelling of a known website, like "rwbalrd.com" instead of "rwbaird.com."

What you should do now:

If you're unsure if an email you received is legitimate, the best course of action is to contact the sender offline, using a phone number you already have or can find through an online search. Avoid using a phone number included in the phishing email, as that could be part of the scam.

All of us at Baird take your financial security seriously. Contact your Baird Financial Advisor for information on how we keep your private information secure. Not a Baird client? **Find a Baird Financial Advisor.** ■

[1]Forbes.com, May 5, 2017