

## Keeping Your Money Safe: Phishing

*Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.*

*Denise Owens, CFE,  
SVP, Fraud  
Department Manager*

Phishing (pronounced "fishing") is one of the most common scams on the Internet. According to [Verizon's 2019 Data Breach Investigations Report](#), nearly one-third of all data breaches in 2018 involved phishing. Not only are these types of attacks increasing as time goes on and our lives and data get stored online, but they're evolving.

### How Does the Scam Work?

Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information that is then used to commit identity theft or other types of fraud. This is usually done by including a link that will appear to take you to the company's website to fill in your username, password, account number, personal identification number (PIN), Social Security number, or other personal information — but the website is a clever fake and the information you provide goes straight to the scammers.

The term "phishing" is a spin on the word fishing, because criminals are dangling a fake "lure"—the email and website that look legitimate—hoping users will "bite" by providing the information the criminals have requested.

Scammers will try to entice you with lucrative offers and eye-catching statements. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. When you come across these kinds of emails, it's best to just ignore them.

### How to Prevent Phishing

Though hackers are constantly coming up with new techniques, there are some things that you can do to protect yourself and your organization from phishing attempts:

- **Think before you click.** If you aren't 100 percent sure about where a link leads, it behooves you to hesitate and think about it before clicking. One tactic you can use is to hover over the link, which usually displays the link's destination, and check for odd-looking URLs such as misspellings. If there is any doubt in your mind, opt to navigate directly to the website rather than clicking a potentially dangerous link.
- **Verify a site's security.** If you're on a website where you expect to share personal confidential or financial

information, you should verify the site's security. Make sure the site's URL begins with "https" and there is a closed lock icon near the address bar. Additionally, if you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites.

- **Keep your browser up to date.** Security patches are released for popular browsers like Chrome and Internet Explorer all the time. They are released to counteract security loopholes that phishers inevitably discover and exploit. If you typically ignore messages about updating your browsers, you're putting yourself and your system at extreme risk. The minute an update is available, download and install it.
- **Be suspicious of pop-ups.** Pop-up windows often seem to be legitimate components of a website. However, they are often phishing attempts. One common tactic is an appeal to an impulse or emotion, such as a "75% off today only!" offer, in an attempt to get you to click on the pop-up. Most browsers allow you to block pop-ups so you don't have to be subjected to this type of phishing attempt. However, if one manages to slip through the cracks, don't click on the "cancel" button because these also often lead to phishing sites. Instead, click the small "x" in the upper corner of the window. Likewise, if you receive a pop-up advising you to click the link to have your antivirus software run a check on your computer, cancel out and access your antivirus software to request a scan.
- **Never give out personal information.** As a general rule, you should never share personal or financially sensitive information over the Internet. When in doubt, visit the main website of the company in question, get their number, and give them a call. Legitimate entities like banks and the IRS don't ask you for financial or personal information in an email. Most phishing emails will direct you to pages where entries for financial or personal information are required. As a rule of thumb, you should never make confidential entries through the links provided in the emails. Additionally, you should never send an email with sensitive information to anyone.
- **Use antivirus software.** This is one of the basic defenses for your system and your information. Like with your browser, it's imperative to keep your antivirus software up to date. Some legitimate websites could unknowingly contain malware and by viewing a post or recipe on the website, a scammer could attempt to load malware onto your computer. If your antivirus software is up to date, it will block this malware. In addition, antivirus software scans every file that comes through the Internet to your computer, helping to prevent damage to your system.

## Keeping Your Money Safe

Being consistently vigilant and careful will help you prevent phishing attacks and reduce your chances of being attacked by malicious actors. It is also beneficial to partner with a financial institution that takes fraud prevention seriously.

PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, [visit our fraud resources page](#).