Keeping Your Money Safe: Holiday Phishing Scams

Ashlie Hagemann, Fraud Supervisor

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.

With the holiday season upon us in the midst of the COVID-19 pandemic, even more shoppers are expected to conduct their gift buying and shipping online. In fact, Deloitte forecasts that e-commerce sales will grow by 25 percent to 35 percent during the 2020-2021 holiday season. Don't forget, that also means cybercriminals are ramping up their efforts to steal your money or confidential information using phishing scams.

What is the Scam?

A phishing scam generally starts with an email in which the cybercriminal impersonates a well-known brand, product, government organization, or other entity. Their goal is to trick you into believing that the email is legitimate. But if you click on a link or file attachment in a phishing email, you will often be routed to a fraudulent site and asked to enter account credentials or provide your financial information. While phishing attempts can take a variety of forms, there are four main types of holiday scams to watch out for during this time: fraudulent shipping notifications, charity frauds, gift card scams, and travel phishing scams. In each of these scenarios, your attentiveness and preparation are critical to thwart the phishing attempt.

- **Fraudulent shipping notifications** alert you there is a package or gift to collect, but in order to receive it, you are prompted to click on a link for the shipping details or to find out where you can pick up your package.
- **Charity frauds** play on your sense of generosity during the holiday season and maliciously attempt to get you to donate funds or share your confidential information.
- **Gift card scams** usually involve a cybercriminal posing as a government agent or bill collector and attempting to persuade you to submit a payment by buying a gift card and then sending them the account number and other information.
- **Travel phishing scams** offer you a deal to purchase a vacation package, followed by a message that your trip has been canceled. In order to receive a refund, you are asked to click a link or visit a site.

How to Avoid Holiday Phishing Scams

The fact that cybercriminals ramp up their efforts during the holiday season should reinforce the importance of practicing safety and common sense when it comes to identifying phishing scams. The

following tips are ways you can make sure you avoid becoming a victim:

1. Don't open attachments from suspicious email addresses – Always check the ID and the address of an email sent to you. Cyber criminals often will create a "dummy" Gmail or Yahoo! account (e.g., Amazon123@gmail.com). At initial glance, it might seem legit but if you look closely, you can see why a legitimate company like Amazon would not send you an email from anything but amazon.com.

2. Pay by credit card – Credit cards, unlike debit cards, give you more protection in case you complete a transaction only to later discover it was fraudulent. You have the ability to dispute the charges with a credit card, whereas a debit card transaction immediately transfers the funds out of your account. Recovering those funds is almost impossible.

3. Buy gift cards for gifting only – Gift cards are a quick and convenient holiday present that has become more popular recently. Remember that no legitimate organization or entity will ask you to pay with a gift card. Cybercriminals will instruct you to buy gift cards from various stores (usually Walmart, Target, Walgreens, or CVS), then ask you to provide the gift card number and PIN. Once you do so, they have access to the entire amount you put on the gift card and you have virtually no recourse in recouping your money.

Stay Safe This Holiday Season

As always, the "Keeping Your Money Safe" fraud prevention series is designed to help you thwart cyber criminals trying to acquire your personal information or infiltrate your devices. The key to protecting yourself is education and awareness. 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.