Citizens 1st BANK

Fraud Education & Prevention

It's that time of year again when you might be using your debit or credit card more than normal. We at Citizens 1st BANK wanted to share with you a few things to watch for that might help protect you and your account from being a victim of a scam.

SEASONAL AND HOLIDAY CHARITY AND TRAVEL SCAMS

- A legitimate charity will welcome your donation whenever you choose to make it; whereas fraudsters will "pressure" you to make it right then
- You should never send donations in the form of gift cards or wire transfers.
- Watch for travel deals that seem too good to be true, and know who you are booking your travel through.

TWO-FACTOR AUTHENTICATION SCAMS

As fraud controls get smarter, fraudsters are shifting their attack patterns to bypass controls. Fraudsters have been using automated phone calls to try to steal consumers' two-factor authentication codes and hack into banking, merchant, and third-party payment accounts. These include Apple, Amazon, PayPal, and bank accounts. An example of these calls state: "In order to secure your account, please enter the code we have sent your mobile device now." Financial institutions and valid merchants will ask cardholders to enter this code on their website or app, not via text or automated phone call. A communication like this indicates the fraudster has tried to access an account and has run into a two-factor challenge from the merchant or institution. This call is an attempt to secure the code sent to a phone number or email on file at the merchant or institution. Usually something like the enter code that had has popped up on your phone. Once entered the automated message will say: "Thank you, your account has been secured and this request has been blocked." Sometimes the call will say don't worry about any payments or fees, we will refund it and then state, "you may now hang up." Scams like these require a hacker to already know several details about a cardholder, such as email address, phone number, and passwords. Personal data like this is often found on the dark web, collected from previous breaches and hacks, sold by POS merchants to marketers, or given out by cardholders themselves.

PHISHING/SMISHING ATTACKS

Phishing and smishing (phishing by SMS texts) are attempts to trick cardholders into providing sensitive confidential information in order to perpetrate fraud. Its variants, and frequency, continue to be on the rise. Phishing schemes such as “spear-phishing,” which is more targeted and difficult to identify, are becoming even more sophisticated than in the past. Instead of using only suspicious links in poorly designed emails, phishing emails are mimicking websites and appearing to be legitimate and credible. The use of web address shortening tools, such as TinyURL, make detection of suspicious links more difficult, even by savvy online users.
It is important to safeguard your financial data and your online banking credentials against criminals trying to harvest them. It is also a good idea to avoid clicking on links that appear in random emails and instant messages. Some phishing emails will start with “Dear Customer,” so your cardholders should be on the alert when they come across these emails. When in doubt, you should go directly to the source rather than clicking on a potentially dangerous link.
In general, you should never give out full card numbers, passwords (either to bank or merchant accounts), full social security numbers, or other sensitive information over the phone.

SECURING DIGITAL DEVICES

You should avoid storing confidential card information in unencrypted format on digital devices unless it is stored using a Digital Wallet or secure password management application. Security concerns include:

- Unencrypted card information on digital devices is susceptible to malware attacks.
- Sensitive information, such as PIN, Social Security number, or answers to security questions can also be stolen by way of malware and remote access applications downloaded to a digital device.
- Choose *reputable* and *secure* applications to store passwords and other sensitive data on digital devices. Avoid installing applications from alternative online “stores” that are not reviewed for security prior to being published.