Phishing Scams: Protecting yourself and your information

Online fraud takes many forms, but fraud scams known as phishing remain most prevalent. Phishing scams most often utilize emails or automated phone calls in an attempt to prompt a consumer into providing personal or account information that is then used by the perpetrators to commit fraud. The term “phishing” is used to describe these scams as the fraud perpetrators are fishing to obtain personal and account information from individuals who may fall prey.

These emails can take on an air of legitimacy by using financial institution logos or even the names of employees, but in fact are fraudulent. These e-mails may be readily identified by a lack of using the cardholder name and/or by urging a response within a short time frame such as 48 hours “in order to prevent your account from being suspended,” or some other negative action. These communications will typically request the reader to click on a link to update or confirm account information, possibly due to an alleged security update, system maintenance, or an update in technology.

Financial institutions will never send unsolicited e-mails requesting anyone to provide, update or verify account or personal information, such as passwords, Social Security numbers, PINs, credit or check card numbers, or other confidential information. To protect sensitive information, never respond to such requests. It’s important to remember that this type of scam can also come in the form of text messages or phone calls.

Consumers can protect themselves by deleting and reporting the potential phishing attempt to their financial institution.

Email phishing:

- Typically the cardholder name is not used. (i.e., “Dear Cardholder”)
- Any emails that request you to change your e-mail addresses or passwords
- E-mails requesting that you update personal or account information due to system, security or technology updates at your financial institution
- Do not click on any links in these e-mails or respond in any way

Phone and SMS phishing:

- The financial institution name may or may not be correct
- The customer name will commonly not be used, (i.e. “Dear Cardholder”)
- Requests for full account/card number, PIN, expiration, and/or other personal information
- Messages often urge action to prevent negative impact

Legitimate calls from a financial institution will frequently require two pieces of information to authenticate the cardholder’s identity, but will typically will be the last four digits of social security number (NOT the full number), and/ or address.