Financial Fraud: *Phishing*

Phishing is the fraudulent attempt to obtain sensitive information or data by disguising oneself as a trustworthy entity. Phishing attempts generally ask you to take a particular action, such as logging into your account or contacting the sender back in order to provide more information.

Email Phishing – emails that appear to be from a trusted organization. Be wary of emails that request account or personal information, emails that do not address you by name or do not include contact information for the sender, emails that contain spelling or grammatical errors or suspicious links, or emails sent from email addresses that do not match the organization.

Website Phishing – a website that may look legitimate but is spoofed and run by a scammer. These sites can be provided to the victim via email or by clicking a link from a web search. Be wary of web pages that are slightly off in URL or appearance, contain misspellings or grammatical errors, or with pop-ups requesting account information.

Vishing – phishing over the phone. Scammers pose as a financial institution or credit card representative to trick unwary consumers into providing sensitive information.

Smishing – phishing via text or SMS message. Be cautious of text messages asking for account information or requestion you to log into your account, or messages containing links, as the links can be malicious or direct you to spoofed sites.

Fraud Prevention Recommendations

- **Use cybersecurity best practices**, including enabling anti-phishing protection on your web browser, adding multi-factor authentication to account log ins, using unique, strong passwords for different accounts, and not clicking on unsolicited links.
- **Contact your bank directly** by using the phone number or website listed on the back of your card, rather than following guidance from an email, phone call, or text message you received.
- **Never provide a one-time-passcode to a caller**, or via email or SMS text message, and never install Remote Access software unless instructed by a trusted system support provider.
- **Review bills, bank statements, and credit reports** to identify unauthorized charges, and sign up for purchase alerts with your card issuer to notify you of suspicious activity.

To learn more about protecting yourself from financial fraud, visit:
https://usa.visa.com/visa-everywhere/blog.html

VISA
everywhere you want to be