Current Types of Fraud

Social Engineering

The art of manipulating people into performing actions or divulging confidential information. A form of trickery or deception for the purpose of information gathering, fraud, or computer system access.

Phishing scams

Fraudsters attempt to acquire information such as usernames, passwords, and credit card details by disguising themselves as a trustworthy entity in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging.

Spoofing scams

Website Spoofing – Fraudsters attempt to direct users to a fake website whose look and feel is almost identical to the legitimate one. This allows them to capture information such as usernames, passwords and credit card data.

Email Spoofing

Fraudsters spoof email address and header information to make an email appear to be from a legitimate entity. It is very easy to impersonate and forge emails. Email spoofing is commonly used in spam and phishing emails.

Vishing

Criminal practice of using social engineering over the telephone system (VoIP or Voice over IP), to gain access to private personal and financial information from the victim for purpose of financial reward. The term is a combination of voice and phishing. This is the main reason it is important for you to initiate any call before divulging personal or financial information.

Malware

(Malicious Software) is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. It's used to describe any kind of software or code specifically designed to exploit a computer, or the data it contains, without consent. Malware includes viruses, worms, trojan horses, spyware, dishonest adware and root kits.

Spyware

A type of malicious software installed on computers that collect information about users without their knowledge. Its presence is typically hidden from the user and can be difficult to detect.

Keyloggers

The action of tracking (or logging) the key strokes performed on a keyboard, typically in a covert manner to gather sensitive information.

Tabnabbing

A phishing attack that takes advantage of user trust and inattention to detail in regards to tabs open in an internet browser session. Fraudsters will load a fake page in one of the open tabs in your browser. This tab will have a spoofed copy of your banks website and in most cases appear that your login has timed out. When the user attempts to reenter login credentials they are captured by the fraudster.

Fake Mobile Banking Apps

Fraudsters may develop and publish fake mobile banking apps in an attempt to steal your online banking credentials.

SMShing

Criminal activity using social engineering techniques over SMS texting. Fraudsters will attempt to gain personal and financial information by spoofing your banks name and number in a text message.

Whaling

Phishing attacks targeted at high profile senior executives

Man-in-the middle (MIM) or Man-in-the browser (MIB)

Fraudsters insert themselves between the customer and the financial institution and hijack the online session. The fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account or direct the customer to a fraudulent website that is a mirror image of the banks website where they capture the customer's login credentials.

Money Mules

A money mule is a person who transfers stolen money or merchandise from one country to another, either in person, through a courier service or electronically. It is typically online scams that prey on victims who are unaware that the money or merchandise they are transferring is stolen. A scammer will employ a mule to relay the money or goods to the scammer.