Common Forms of Online Fraud

The following glossary of terms provides a look at some of the tools fraudsters use to facilitate fraud online.

Phishing

Phishing is an email scam in which fraudsters send messages to try to gather personal and financial information by pretending to be a well-known company. These email messages claim to be from a real business or organization and ask you to update or confirm your account information. They direct you to web sites that look legitimate, but are not. Although they can be difficult to spot, they generally ask you to click a link back to a 'spoof web site'. Never respond to these emails, click on the links, copy and paste a link from the message into your web browser, nor enter personal information. Even if you don't provide what they ask for, simply clicking the link could subject you to background installations of malware (key logging software or viruses). Park Bank will never send you an email asking for confidential personal and banking account information.

Malware

Malware includes computer viruses, Trojan horses, spyware, adware and other malicious or unwanted software. Through malware, fraudsters have the ability to take control of your computer or monitor your activity without your knowledge. When this occurs, they can steal sensitive information and conduct banking transactions such as ACH and wire transfers to an offshore account. This has been the most common form of fraud that Park Bank's clients have experienced recently. It occurs when a company's employees either open a fraudulent or SPAM email, browse an infected website, download files via peer-to-peer file sharing, 'catch it' from other infected computers within the company's internal network or use an unprotected home PC to conduct business transactions.

How malware works:

- Fraudsters are able to watch keystroke logs to get a hold of passwords and account numbers. Sometimes they even intentionally lock out accounts to make the user re-renter passwords or security question answers.
- Using the passwords they've captured, fraudsters log into web services like email and online banking to steal more information or initiate banking transactions.
- It is common for fraudsters to initiate large wire or ACH transfers to themselves if they gain access to online banking accounts. Many times, the transfers go to offshore accounts or bounce through a network of 'mules' who quickly forward the funds out of reach, leaving the business unable to recover any funds. In most cases, the funds are gone within the first day and before the fraud is even discovered.

Corporate Account Takeover (CATO)

A form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts they control.

PARK BANK
first IN LASTING RELATIONSHIPS®

Active Trojans (Man-in-the-Middle Trojan)

Installs malware on the user's computer that interacts with a financial institution's genuine website on his/her behalf. As the Trojan interacts with the site through the computer, it allows the fraudster to imitate the user. Because the Trojan is on the user's computer, it appears to be transacting from his/her IP address and machine.

Botnet

A series of networked computers that have been compromised with malicious software and are used to send spam or malware to other computers. Users are often unaware that their computers are infected.

Keystroke logger

A program that can record what a user types on his/her computer. Details of what the user typed is sent to a "drop zone" (an e-mail account or a server) for the fraudster to retrieve and use for fraudulent activity.

Man-in-the-Middle Attacks

The fraudster acts as the "middle man" by tricking a user into unknowingly entering sensitive information (such as user IDs, passwords, Social Security and account numbers) on a website that appears to be the financial institution's site. The fraudster then simultaneously feeds that information to the financial institution's genuine website and performs fraudulent transactions.

Page-in-the-Middle Attack

Similar to a man-in-the-middle attack, but in this case, the fraudster will wait until a user logs in to a financial institution's website to redirect him/her to a fake page to collect sensitive information (such as user IDs, passwords, Social Security and account numbers), and then redirects the user back to the genuine website.

Screen scrapers

A program that captures tiny images of on-screen selections (for targeting financial institutions that use virtual keyboards at log in). Details of the screen capture is sent to a "drop zone" (an email account or a server) for the fraudster to retrieve and use for fraudulent activity.

Spyware

A type of malware that can secretly monitor or control a user's computer activity.

Trojans

A type of malware that allows a fraudster to gain unauthorized access to a user's computer.

Virus

A computer program that, when installed on a user's machine, can make copies of itself. Viruses are usually sent via e-mail attachments.

These terms have been collected from various industry sources. **For more information, please visit www.ftc.gov and www.onguardonline.gov.**