Common types of Computer Fraud – Financial Institutions

Several financial institutions have discovered attempts by criminals to gain banking log-on and/or credit/debit card details from their customers by getting them to reveal their personal and banking security details.

PHISHING E-MAILS

This is the name given to e-mails that claim to be from your bank or other financial organizations but are actually sent to you by fraudsters. These e-mails typically urge you to click on a link that takes you to a fake website which is often identical to the one you would expect to see. You are then asked to verify or update your personal security information. The fraudster who has created the fake website will then have your security and other personal information. A genuine organization will never send you this type of e-mail.

These e-mails aren't normally addressed to you by name; they are sent to millions of recipients in the hope that some will respond. The aim of the e-mail is to trick you into providing your details. This practice is likely to be an increasing menace and you are advised to:

Not go to any website and input any password or other banking details as a direct result of an e-mail request; banking details includes credit/debit card and PIN numbers requested via e-mail. Your financial institution will never send you e-mails asking you to update your security; it will never ask you to confirm your log-in or security password information by clicking on a link in an e-mail, or visiting a website.

We will never ask you to verify information such as validating or updating an account, or confirming your security details i.e. password, card number, pin number, by e-mail, phone or text.

If you receive any e-mails claiming to be from your financial institution asking for security details, delete them immediately without responding.

TROJANS

Trojans are usually received in e-mails that may contain files, pages or attachments to open. Once opened, they can secretly install a program that can monitor your online activity, down to what keys you're pushing on your keyboard.

This could mean the next time you enter your credit/debit card details on your favorite on line shop, the fraudsters would be alerted. This is one of the reasons why it is important that your computer security is kept up to date.

MONEY MULE/ADDITIONAL INCOME E-MAIL SCAM

One of the many scams around involves someone offering, via an e-mail or website; to pay funds into your account on the understanding you then transfer them overseas. In return, you supposedly get a commission. Some of these want an up front deposit; once you have paid, you will never hear anything again and more likely than not have lost your money.

Many of these scams also involve the proceeds of fraud and you should ignore the request. Any customer that participates may well become involved in a police investigation and we could close any account involved in this scam. The golden rule for all of these e-mails is that if it looks too good to be true, it probably is a con.

COMPUTER FRAUD WEBSITES

- http://www.fbi.gov/scams-safety/fraud – FBI Website with information on general fraud schemes. Some of the described schemes are not computer specific but are often presented via the internet websites and e-mail.
- http://www.fbi.gov/scams-safety/fraud/seniors/seniors#target – A linked area on the FBI website above regarding schemes that are more likely directed at senior citizens.
- http://www.fbi.gov/scams-safety/fraud/internet_fraud – A linked area on the FBI website that is specific to fraud on the internet.
- http://www.ic3.gov/default.aspx – How to report internet fraud and scams. This is a partnership website that includes the FBI, National White Collar Crime Center, and the Bureau of Justice Assistance.
- http://krebsonsecurity.com/ - Brian Krebs is a former IT writer for the Washington Post. Most of his writing is a bit technical and more related to computer security, but he is current on what is going on in the cybercrime world.

Tips to Prevent Computer Fraud

Email Precautions:

- If you receive emails from senders you don't know, delete them immediately without opening them and do not reply to unsubscribe as this can tip off phishers that they have reached a valid email address.
- If you get any type of unsolicited email or pop-up message that asks for any type of personal information, don't respond to it and notify your Internet Service Provider (ISP) immediately.
- Never send personal or sensitive business information via unsecured email. Any information sent through unsecured email messages may be intercepted and stolen.

Online Precautions:

- Install and keep anti-virus/anti-spyware software on your computer updated.
- Do business only with reputable online firms.
- Don't keep personal or business information, passwords or account numbers online or on websites.
- If you are conducting any type of business online, make sure you are doing so on a secure web connection. If you see the characters https:// in the web page address in your browser, you are visiting a secure website that uses encryption to protect your identity and your information. If you only see http://, don't enter any personal information because the page in not a protected web site and could be intercepted during transmission.
- Know who you are dealing with online. Don't complete forms that ask for personal information if you don't know exactly where they are going and what they will be used for. Review the Web site privacy policies of sites with which you deal.
- If you bank online, make sure you stay at your computer for the entire transaction, and then be sure you sign off completely when you are done.
- Ask to have your account and credit card statements sent to you online directly from your bank or credit card company.

Most banks have a secure e-mail or contact method that one can use after logging into the account. Always use that method for sending sensitive information to your bank.