Security Education

Protect Yourself Online

- What You Should Know About "Social Engineering"

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. Also "Social engineering is described as the art of using weaknesses in human behavior to gather information to breach security without the victim noticing that they have been tricked".

How Does Social Engineering Work

A social engineer will commonly use the phone, internet, engage in dumpster diving or psychological persuasion to trick people into revealing sensitive information or getting them to do something against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.

Social Engineering by Phone

The most common form of social engineering is conducted by phone. The attacker calls pretending to be someone important for the company or an outside consultant working for the company. Many times the attacker will have several scripts that he/she has rehearsed (known as pretext calling). The attacker gains customers’ trust and extracts important pieces of information from each customer. If the customer has no idea what information he/she can or cannot disperse, then the attacker can also play on the customer’s unawareness with respect to the disclosure of information.

Social Engineering by Internet

Online social engineering can take many forms. Many times the would-be attacker can send a customer an e-mail directly requesting the customer’s password or the attacker can send the customer an attachment. The attachment can be a “Trojan Horse” which records the customer’s keystrokes and sends them automatically to the attacker via e-mail. Furthermore, the attachment can install a pop-up window that looks like a legitimate network request for the customers to re-enter their username and password. When the customers re-enter this information the hacker captures the login information.

Social Engineering by Dumpster Diving

Another less glamorous form of social engineering is called dumpster diving. Here the attacker collects information about the customer or company from the trash that the customer or the company throws away. The customer or company dumpster can be a gold mine for the attacker, providing him/her with enough information to launch another form of social engineering attack, such as by phone.

Social Engineering by Psychological Persuasion

Psychological persuasion can be used in any of the other categories of social engineering discussed previously. Many times, the attacker uses persuasion to gain the customer's trust. This method is very useful in pretext calling.

Best Defense is to Protect Yourself…

Always be on the alert for suspicious questions and behaviors.

- Fraud... What should you do if you suspect you are a victim of fraud?

  The best detector of fraud and identity theft is you. Through proactive monitoring, you can look for unusual activities and act fast before damage occurs.

  Banking online gives you quick access to your accounts, so fraudulent activities can be detected sooner. Additionally, by taking advantage of online bill pay and good old fashioned paper shredding, you can contribute to your own online safety.

  How to detect fraud:

  Monitor your accounts regularly

  Plus International Bank recommends frequently reviewing your account online for any unusual activity.

  Recognize fraud and identity theft

  Fraud is an act that occurs when someone uses your account to make unauthorized purchases, usually when the account number or card has been stolen.

  It's important to learn how to recognize activities that may indicate possible fraud or identity theft.

  The following may be signs of fraud:

  •If you did not receive an expected bill or statement by mail

  •If unexpected charges occurred on your account

  •If there are charges on your account from unrecognized vendors

  •If posted checks appear on your account significantly out of sequence

Identity theft happens when a thief steals information such as your name, birth date or Social Security number to open credit cards, mortgages, and other accounts without your knowledge.

Check your credit report annually

By monitoring your credit report, you can make sure that no one has opened bank accounts or applied and been approved for loans in your name using stolen information.

Nationwide consumer reporting companies will provide you with a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com or by calling 1 877 322-8228

You can also get an explanation of your rights from the Federal Trade Commission (FTC), the nation's consumer protection agency.

- What should you do if you suspect your computer has been compromised?

A Compromised Computer is defined as any computing resource whose confidentiality, integrity or availability has been adversely impacted, either intentionally or unintentionally, by an untrusted source. Here are a few clues that may indicate your computer has been compromised.

If your computer begins to exhibit:

•A sudden reduction or unresponsiveness in the computer's performance

•Unusual behaviors, such as windows briefly popping up and closing down

•Application programs terminating and restarting again or programs running that you are unfamiliar with

•Sporadic failed logins, even though you are certain you entered the password accurately

•If you own a business: An e-mail bounces back, you are unable to receive e-mails or traffic to your site or employee's password doesn't work.

Your computer may have had malicious software installed by a hacker that can capture sensitive information (including passwords), alter data or disrupt your service.

The following steps should be taken in response to an actual or suspected compromised computer:

•Disconnect the computer - Disconnecting the computer from the Internet or the network as soon as possible prevents a potentially untrustworthy source from taking further actions on the compromised computer

•Back-up or image the computer's hard drive

•Perform a clean installation of Microsoft Windows - A format of the drive “should” be completed.

•Immediately update that installation with all of the latest patches.

•Use the latest anti-spyware or anti-virus detection to scan and clean any data that you want to recover from the backup

•Notify users of the computer (if any) of a temporary service interruption

•If the compromised computer provides some type of service, it is likely that users of this service will be impacted by the interruption brought on by disconnecting the computer from the network.

•Preserve any log-in information not resident on the compromised computer - All log files, pertaining to a compromised computer, that are stored on a secondary computer or on some type of external media should be preserved immediately.

•Contact your Company’s Help Desk for assistance (as applicable) - Contact your Help Desk for assistance in tracking down changes made by the hacker. They will determine the best course of action for the compromised computer.

- Why you should protect your computer?

Your computer is a popular target for intruders. Why? Because intruders want what you have stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money or credit to buy themselves goods and services.

How do intruders break into your computer? In some cases, they send you an e-mail with a virus. Reading that e-mail activates the virus, creating an opening that intruders use to enter or access your computer. In other cases, they take advantage of a flaw or weakness in one of your computer’s programs – a vulnerability – to gain access.

Once they’re in your computer, they often install new programs that let them continue to use your computer – even after you plug the holes they used to get onto your computer in the first place. These backdoors are usually cleverly disguised so that they blend in with the other programs running on your computer.

Whether your computer runs Microsoft Windows, Apple’s Mac OS, LINUX, or something else, the issues are the same and will remain so as new versions of your system are released. The key is to understand the security-related problems to think about the solutions.

Here is the list of tasks you need to do to secure your home computer:

•Install and Use Anti-Virus Programs

•Keep Your System Patched

•Use Care When Reading E-mail with Attachments

•Install and Use a Firewall Program

•Make Backups of Important Files and Folders

•Use Strong Passwords

•Use Care When Downloading and Installing Programs

•Install and Use a Hardware Firewall

- Your consumer protection under Regulation E

  Regulation E provides rules for error resolution and unauthorized transactions for electronic fund transfers affecting your consumer deposit accounts. These electronic fund transfers include most transactions processed online. In addition, it establishes limits to your financial liability for unauthorized electronic fund transfers. These limits, however, are directly related to the timeliness of your detection and reporting of issues to Plus International Bank. It is for this reason that we encourage you to immediately review your periodic account statements and to regularly monitor your account activity online.

  In general, the protections and deadlines included in Regulation E are extended to consumers transacting business on consumer accounts.

  The "Electronic Fund Transfers" disclosure provided to you at the time of account opening provides detailed information. You may also contact us to request a free printed copy of this disclosure at (305) 375-0590.

- Password Security: What are the best practices to follow?

  Passwords are very important for maintaining your online identity, because they ensure that no one else can access your accounts and do things you wouldn't do. As such, you should make sure that your online passwords are as strong as possible.

The following best practices for password and account security focus on variety, length and complexity:

•Avoid dictionary words or simple to guess words, phrases, names or significant dates when generating a password.

•Variety is important. Don’t use the same password for multiple sites or accounts.

•Select strong passwords with ten or more characters, randomly adding capital letters, punctuation or symbols (if permitted).

•Substitute numbers for letters that look similar.

•Think of a meaningful song or quote and turn it into a complex password using the first letter of each word.

•Keep your passwords secure and do not share your passwords with others.

•Do not store passwords and/or user IDs on your computer, laptop or mobile device.

•Do not use public computers, such as those at hotels or libraries, to log into a bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes.

•Only log in to your bank accounts on trusted computers or mobile devices you control.

- E-mail Security: What are the best practices to follow?

Here is some important information we want you to know about e-mail security:

•Plus International Bank will never ask you to provide confidential information such as account numbers, Social Security numbers or passwords via the internet or e-mail.

•Forged e-mail purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal/sensitive information for fraud. Do not respond to e-mails with questions about your accounts and do not include any personal information. You may use secure messaging within Online Banking to ask us account-related questions.

•Plus International Bank is committed to protecting your privacy and adheres to its privacy policy for sharing information.

•Never open or respond to SPAM (unsolicited bulk email messages). Delete all SPAM without opening it. Responding to SPAM only confirms your e-mail address to the spammer, which can actually intensify the problem.

•Never click on links within an e-mail. It is safer to retype the Web address than to click on it from within the body of the email.

•Never give out your email address to unknown Web sites. If you don’t know the reputation of a Web site, don’t assume trust. Many Web sites sell email addresses or may be careless with your personal information.

If you receive an e-mail that appears to be from Plus International Bank but seems suspicious in any way, do not respond or click on any links it contains. Report your concerns by calling Plus International Bank at (305) 375-0590.

Fraudulent E-mail

Criminals may send you an e-mail or pop-up message that looks as though it comes from a trusted source. These phony messages may ask you to provide personal account information at a website that looks legitimate. They might even warn you that your account could be suspended if you don't respond.

This is the most common type of online fraud, called "phishing" or "spoofing." Criminals send you these phony e-mail messages — or direct you to a fraudulent website — for one reason only: to steal your personal and financial information.

What can you do?

•Do not open attachments or download software from sources you don’t know, they could contain viruses. If you receive an e-mail or pop-up message that looks suspicious, delete it immediately. Do not reply or click on any links it provides.

•Be selective when providing your e-mail address.

•Do not use e-mail to transmit confidential information such as your Social Security number, account numbers, passwords, PINs, etc.

•Never provide personal information in response to an unsolicited request. Plus International Bank will never ask you to furnish confidential information via internet or e-mail.

•If you are a Plus International Bank Online Banking customer, you may use secure messaging within Online Banking to ask us account-related questions.

- Online identity protection

Online identity protection means following best practices to help you browse the Internet safely and securely.

Be selective about where you surf.

Not all Web sites are benign. Sites that are engaged in illegal or questionable activities often host damaging software and make user susceptible to aggressive computer attacks.

Use a secure browser.

Always use secure Web pages when you're conducting transaction online (a Web page is secure if there is a locked padlock in the lower left-hand corner of your browser).

Select a strong password.

Do not use birth dates, first names, pet names, addresses, phone numbers or Social Security numbers as your password. Instead, use a combination of letters, numbers and symbols. Be sure to change your passwords regularly and refrain from using the same password as used on other systems.

Don't choose "Remember My Password."

Do not use the "remember your password" feature for online banking or transactional Web sites.

Don't use public computers for sensitive transactions.

Similarly, do not use your personal computer to transact via a public/unsecure wi-fi connection. Always keep personal Wi-Fi network password protected. This will keep out potential hackers and other unauthorized users.

Detecting a rogue update or fraudulent message.

Do not click on links in e-mails you receive. Instead, type the URL directly into your browser. In Phishing scams, scammers send official-looking e-mails with links to fake sites in an attempt to gather personal information. Sometimes these e-mails can download malicious software (malware) onto your computer to steal personal data.

Be wary of e-mails that announce there is a problem with your account. Plus International Bank does not send these types of notifications.

What can you do?

•Update and strengthen the security of your online passwords.

•Change your password often.

•Keep your operating system, browser and anti- virus protection software up-to-date with the latest vendor provided updates.

•Use a secure browser and trusted computer for sensitive transactions.

•Log off when you're done using Web sites that require a user ID and password.

•Disconnect and shut down when you're not using your computer.

- Protecting your kids online

The key to protecting your children online is to educate them about the risks they may face. By understanding these dangers, you and your children will be able to work together better to defend against them. Here are some steps you can take.

•Education: The most important step you can take is education. No single technology or computer program is going to solve all the dangers you and your children face online.

•Dedicated Computer: Have a separate computer just for your children to ensure that if they do accidentally infect their computer, your online accounts are not affected or compromised.

•Rules: Create a document that identifies the rules you expect your children to follow when online. Also, consider posting how the rules will be enforced and possible consequences for violating the rules.

•Monitoring: Children are by nature trusting and curious. So monitor your children's activities; they simply do not realize how dangerous the world can be. Help them to identify issues and discuss these issues together so that they can build a safe online presence.

•Filtering: In addition, you may want to filter your children's online activities, such as restricting which websites they can visit. This is especially important for younger children, as it protects them from accidentally accessing dangerous or unwanted content.

- Trusteer Rapport Software Protects Against Malware

Trusteer Rapport is dedicated online banking security software to protect against financial malware and phishing attacks.

Developed by IBM and free to Online Banking and Online Cash Management customers, Rapport provides an extra layer of protection, working alongside your anti-virus software and firewall to help:

•Prevent malware and fraudulent websites from stealing your Online ID, Passcode and other sensitive information

•Shield your online bank account from prying eyes

•Keep your computer malware-free by blocking malware installation and removing existing infections

Free Trusteer Rapport Fraud Protection Software is highly recommended for Online Banking customers and a requirement for Online Cash Management for business customers.

Protect your computer. Protect your Banking online. Protect yourself!