WSB WINCHESTER SAVINGS BANK

STRENGTH. SERVICE. COMMUNITY.

COMMON SOCIAL ENGINEERING ATTACKS & HELPFUL TIPS TO AVOID THEM

COMMON SOCIAL ENGINEERING ATTACKS

- **Bogus Email from a Friend.** It is a common social engineering tactic used to extract information from a large network of people. In this case, criminals only infiltrate one email account and use the contact list to send spyware-ridden email to others in an address book.

In most cases, the attacker using a hacked account sends you an email address claiming that your 'friend' is stuck in a foreign country after being mugged. They request money for a return ticket and promise to refund the money once they are back. Usually, the email has instructions on how to send the money to your 'stranded friend' abroad.

Don't be fooled into trusting an email attachment or a link sent 'supposedly' by a known friend.

- **Phishing Attacks.** Most **phishing attacks** are created through bogus emails allegedly from trusted service providers such as banks, schools, software companies or government security agencies. (e.g. FBI, Better Business Bureau, IRS)

An online fraudster sends an email posing as one of your trusted merchants (i.e. credit card or utility company).They request that you urgently update your account details or upgrade your current software through given links**.** Most phishing emails require you to do something urgently or risk some consequences. Clicking on the embedded links directs you to spoofed websites designed to steal your login credentials.

Another common trick used by phishing masters is to send you an email claiming that you've won a lottery or certain promotion goodies. You are required to give your banking details in order receive your lottery winnings. In other cases, the scammer poses as the FBI saying they have recovered your 'stolen money' and are requesting that you send your bank details to get your money back.

- **Unsolicited Tech Support.** In some instances, criminals pose as tech support teams from popular companies such as Microsoft, claiming they are responding to ''your request'' to resolve a tech problem. Although you never requested help, you could be tempted to take advantage of a free service because you could be having a tech problem with your Microsoft product. This scam can be attempted by phone or email.

Responding to a suspicious email may result in an interaction with the criminal who may request more specific details about your computer system in order to help you out. In some cases the criminals may request you to log on to "their company systems," or they might give you a bogus command to run on your system. Such commands are only intended to give the attacker greater access to your computer system.

Never allow anyone who ***contacts you*** to access your computer system.

HELPFUL TIPS TO AVOID SOCIAL ENGINEERING ATTACKS

- **Be wary** of unsolicited emails, instant messages and phone calls from people such as service providers. Verify the source of the message before giving out any information.
- **Go slowly** and pay keen attention to fine details in emails and messages. Never let the urgency in an attacker's message cloud your judgment.
- **Educate yourself**. Information is the most powerful tool in preventing social engineering attacks. Research facts on how to identify and ward off online criminals.
- **Never click on embedded links** in emails from unknown senders. If necessary use a search engine to search for suggested websites, or manually enter the website URL.
- **Never download email attachments from unknown senders**.
- **Reject requests** for online tech support from strangers, no matter how legitimate they may appear.
- **Secure your computer space** with a strong firewall and up-to-date antivirus software. Set your spam filters high.
- **Patch up software and operating systems** for zero-day vulnerabilities. Follow up on patch releases form your software providers and patch-up as soon as humanly possible.
- **Pay attention to website URLs**. Sometimes online fraudsters make slight changes to URLs in order to direct traffic to their own spoofed sites.
- **Avoid being greedy on the web**. If you never participated in a lottery, it goes without saying that you can never be the winner. If you never lost money, why would you accept a refund from the FBI?
- **Analyze each and every situation** before giving out any personal, sensitive or computer-related information.

ACTION STEPS FOR SOCIAL ENGINEERING VICTIMS

Due to the nature of social engineering attacks, **most victims don't know they've been hacked,** and it may take months to identify a security breach. If you suspect that you've been a victim of social engineering,

- **Create** a new strong password for all your accounts. Ensure that your new password cannot be linked to you or your family.
- **Contact** your bank, and carefully review your financial statements.
- **Report** the incident to law enforcement agencies to avoid liability in cases of identity theft and impersonation in criminal activities.

Preventing social engineering attacks requires knowing when and whom to trust on the web.