Protecting Your Finances

INFORMATION YOU SHOULD KNOW TO PROTECT YOUR FINANCIAL WELL-BEING

Phishing: an email sent requesting sensitive financial information such as usernames, passwords and credit card information. You may be instructed to click on a link embedded in the email which will appear to take you to an official looking bank website. It will be here that the thief attempts to steal your username and password. **Prior to clicking on any link, confirm the link by sliding and holding the mouse pointer over the link and viewing the URL address, this will identify the true address of where the link will take you.**

Smishing: utilizes Short Message Service (SMS) systems to send bogus text messages via cell phones. Smishing is received in the form of a text message requesting your credit card number. They will claim you are about to be charged for a service you did not request unless you cancel it. You will be encouraged to provide credit card details or passwords as part of the cancelation process.
No legitimate agency requires you to enter your credit card number for a cancelation.

Vishing: involves automatic dialers who use fake caller IDs to obtain your financial information. These calls may be automated or by a live person. They will claim your account or card has been compromised and ask that you enter your account number and PIN. **DO NOT provide this information!** Confirm the accuracy of any call by using the contact information provided by the institution on your monthly statement.

Pharming: Much like Phishing, pharming is a hacker's attempt to redirect website traffic to a bogus site. The site instructs one to enter access credentials, such as username and password. Most online banking sites allow the capability to modify backgrounds, colors or recognizable words. This creates a unique customized site for you that is easily recognized when altered.

Malware: (Malicious software) is designed to interrupt computer operations, collect sensitive information, or obtain unauthorized access to computer systems. You may have heard of them: viruses, Trojan Horses, worms, spyware and adware. Malware is hidden inside free offers and applications, be careful of websites you visit and free offers available online.

Passwords: It is important, when choosing a password for Online Banking or making on-line purchases, to make the password unique. Never use this password for other sites and avoid using common words or phrases. Bypass using things like your date of birth, mother's maiden name, or your pet's name. To strengthen your password use upper and lower case letter combinations that are not found in the dictionary and insert numbers and special characters to create a multifaceted password. **Never share your password(s) with anyone or write them down!** If you have used a public computer network, be sure to update your password once you return to your personal computer network. **Do not use public computers to login to Online Banking.**

PIN: (personal identification numbers) Choosing the right Debit or ATM Card PIN number is important, but protecting it is more important. Never record your PIN near the card it is attached to. To help you remember your PIN, create a word then use your dial pad to transfer the word into a four digit number. You can also create a fictitious friend in your cell phone's directory incorporating your PIN in part of the phone number.

Anti-virus Software: Protect your computer(s) with anti-virus software as well as anti-spyware and firewalls. Keep up with their expiration dates so not to allow a lapse in protection. Configure the software to scan your e-mail as it is received. Don't forget to install these safety features on your smart phones too!

Screen Lock Smart Phones: This is your phone's capability to lock after a predetermined amount of time. Most smart phones use a pattern, PIN or password to unlock. This prevents someone from stealing your personal information. Your phone service provider can help you set these safety features.

Telephone Safety: When you contact us, know that we will ask a few questions to confirm we are speaking with the owner of an account(s). Likewise know that we would not contact you and solicit your personal information, such as social security number, date of birth etc., as you would have already provided that information at account opening. This would also not occur through mail or via email.

Guard Your Mail: You may think your home mailbox is a safe receptacle for outgoing mail, think again. Thieves use mailboxes to gather your personal information on checking accounts as well as credit cards. Take mail containing payments with checks to Post Office collection boxes. Always gather your mail daily and if you will be gone, have the Post Office hold your mail. If routine bills do not arrive at normal intervals, contact the creditor; a thief may have falsely changed your address to divert your information.

Lost or Stolen Debit or Credit Cards: Record the toll-free numbers in a secure place of all credit cards you carry in your wallet. If your card(s) become lost or stolen, immediately notify the creditor(s) so they can cancel your card(s) and issue new ones. You would then need to file a police report.

Public use of Personal Laptops: Establishing personal firewalls on your PC will help protect you when using your laptop on public networks. In addition you should routinely update your security software and applications. Avoid using public networks to access your financial accounts. Rogue networks are looking to deceive you into using their network, where they can capture your financial information. If you must get on a public network, always verify the network address is legitimate with staff of the facility. Make sure to logout each time you finish and close the browser as well.

ATM Safety: ATMs are a convenient way for you to transact banking. Here are several tips to help make your ATM experience a safe one. Prepare your deposit slips, envelopes, and calculations prior to approaching the Automatic Teller Machine. Scan the area to make sure it is well lit and that there is no one lurking. When possible, use drive-up ATMs so you do not have to get out of your vehicle. Be aware of your surroundings and remember to take your card prior to leaving.

Credit Review: You should review your credit once a year. The law requires that major consumer reporting agencies provide you a free copy of your credit report annually. You can visit annualcreditreport.com for your copy. Indications that something may be wrong with your credit: a bill does not arrive as expected, you receive a denial of credit that you did not apply for, or you receive calls or letters about purchases you did not make. Your best safe guard is routinely checking your credit.

Shred: Thieves are always searching for ways to steal your identity. You must be vigilant when it comes to protecting your personal information. They will steal your mail and even dumpster dive to obtain your identity. Make sure you shred all documents that contain account numbers, social security numbers and all other personal information. (Cross shredders are more thorough.)

Windows Updates: Microsoft regularly offers important updates to Windows that can help protect your computer against new viruses and other security threats. To ensure that you receive these updates as quickly as possible, turn on automatic updating; you won't have to worry if a critical fix for Windows has been applied.

fsbbank.net

Where you're always First

12/13