

Alert: Due to the prevalence of email "phishing" and "pharming" scams, Citizens State Bank- Princeton (CSB) would like to remind our customers to take the proper precautions while navigating the web. Never provide your Social Security number, passwords, card, pin or account numbers in response to an unsolicited request. Please remember, if you did not initiate the communication, you should not provide any information.

Learn how to Protect Yourself From Internet Fraud: Recently, millions of credit cards were compromised nationwide by a computer system breach of a company that processes Credit Card transactions. CSB continuously works hard to make sure your account and information are safe. Here are some relatively simple steps you can take to help reduce your susceptibility. We also recommend that you visit these sites, which include a short, informative video:

<http://anon.vodium.com.edgesuite.net/anon.vodium/fdic/identitytheft/index.html>

<http://www.treas.gov/press/releases/js3083.htm>

General;

Carry only necessities on a daily basis. Items like a Social Security card should be stored safely at home.

Do not provide your Social Security number unless absolutely necessary. When a Social Security number is requested to sign up for a service, confirm that it is actually needed rather than some other identifier.

Do not sign the back of your credit cards. Instead, write "PHOTO ID REQUIRED". Make photocopies of the vital contents of your wallet. For example: copy both sides of your license, credit cards, etc. In the event of a theft, you will know what you had in your wallet and all of the account numbers and phone number to call and cancel.

Limit the use of paper statements. A paperless environment helps reduce the chance of identity theft. The fewer personal documents sent through the mail, the less chance there is for possible fraud.

Shred documents containing personal or financial information before discarding. Most fraud and identity theft incidences happen as a result of mail and garbage theft.

Review your credit report. Look over your credit report regularly - at least once a year -for any inaccuracies. You can get a free credit report once a year from each of the three major credit bureaus at <http://www.annualcreditreport.com> . For a small fee you can obtain a copy at any time directly from the credit bureaus:

Equifax: 1-800-685-1111 or <http://www.equifax.com>

Experian: 1-888-397-3742 or <http://www.experian.com>

TransUnion: 1-800-916-8800 or <http://www.transunion.com>

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Pharming is a technique used by individuals and companies to obtain important personal and financial information without your knowledge. It is similar to Phishing, except the information is collected without you needing to click a link in an email.

Steps to Keep You Safe:

Be wary of suspicious emails. An email requesting your account information and password should be scrutinized carefully, particularly if the information is needed to "award a prize" or "verify a statement." Avoid opening any questionable emails. If you have opened an email, do not open any attachments or links it may contain, and delete it. Please notify us immediately if you receive a suspect email claiming to

come from CSB. Protect your passwords. Memorize your passwords. Do not write them down or share them with anyone.

Change them regularly and use combinations of letters and numbers. Do not use your Social Security number as a username or password. Keep your computer and online experience safe. We encourage you to consider installing a firewall, anti-virus software, and a pop-up blocker, which can help keep your computer and personal information secure when you conduct online transactions. Keep your computer operating system up to date. If your computer is more than five years old, its operating system (e.g. Windows 98, OS 7, etc.) may not offer the same level of protection as newer systems. System manufacturers provide frequent updates to help make your system more secure. Some manufacturers supply updates automatically through email or via your Internet connection. You may also check their Web sites, including:

<http://www.microsoft.com/security/>

<http://info.apple.com/>

Use a current Web browser. To provide our customers with the most secure online access to their accounts, CSB continually upgrades our online services. In certain cases, the software you use to connect to the Internet (i.e. your Web browser) may eventually become unsuitable for sensitive transactions such as Internet Banking. In order to maintain a high level of security, CSB does not allow access to CSB Internet Banking or Corporate Cash Management using browsers that do not meet our security criteria. Install a personal firewall. Though most office networks include firewall protection, your home computer may benefit from this added level of security. Check to see if your operating system already includes a firewall prior to purchasing a separate one. Install and update anti-virus software.

Commercially available virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. These programs offer continuous upgrades in response to the latest threats. Some of the most popular programs are:

<http://us.mcafee.com>

<http://www.norton.com/>

Activate a pop-up blocker. Several free, publicly available programs exist that will block all popup windows from occurring while you are online. Perform an Internet search for "pop-up blocker" or look at the options provided by major search engines. You should confirm that these programs are from legitimate companies before downloading. Once you have installed a pop-up blocker, you should determine if it blocks information that you need to view or access. If this is the case, you should consider turning off the blocker when you are on Web sites you know use pop-windows to provide information you need or want to view. Scan your computer for spyware regularly. You can eliminate potentially risky pop-up windows by removing any spyware or adware installed on your computer. Spyware and adware are programs that look in on your Web viewing activity and potentially relay information to a disreputable source. Perform an Internet search for "spyware" or "adware" to find free spyware removal programs. You should confirm that these programs are from legitimate companies before downloading. As with a pop-up blocker, you will want to be sure that your removal program is not blocking, or removing, wanted items, and if it is, consider turning it off on some Web sites. Use secure Web sites for transactions and shopping. Be sure the Web page you are viewing offers encryption of your data. Often you will see a lock symbol in the lower right-hand corner of your browser window, or the Web address of the page you are viewing will begin with

"https://...". The "s" indicates "secured" and means the Web page uses encryption. csbprinceton.com, for instance, provides 128-bit encryption - the highest level commercially available today. Avoid downloading programs from unknown sources. Downloads from unfamiliar sources may contain hidden programs or viruses that can compromise your computer's security. Disconnect from the Internet when not in use. Dedicated services such as DSL or high-speed cable provide a constant connection between your computer and the Internet. When not in use, disconnect from the Internet to avoid unwanted access to the information on your computer. Even if you have a firewall installed, this is an additional step you can take to help protect yourself.

Online Fraud Q & A;

How do phishers get my email address?

Phishing emails are just like spam—they're largely sent at random. Spammers gather emails from all over the web: websites, newsgroups, legal and illegal mailing lists, etc. Sometimes it's simply guesswork. The email addresses aren't ever gathered from the companies that are spoofed in phishing, unless that information is somehow stolen.

Is it safe to use online banking and buy things from the Internet?

Online banking and ecommerce is generally safe and convenient. Still, you should never relax your guard online, and treat unsolicited emails as suspiciously—if not more—as you'd treat an unsolicited phone call or stranger knocking at your door.

How do I protect myself?

The golden rule to avoid being phished is to never hit "reply" or click the links within a suspicious email. If you can tell it's phishy, always delete the email immediately. The only reason you wouldn't delete an obvious spoof email right away is because you're "Where You Can Report Flushing" reporting it to the proper authorities. Once you've done that, and deleted the phishing email, empty the trash box in your email program as well. If you're not sure whether the email is legitimate or fake, be suspicious of any emails that request financial or personal information, especially ones that prey on fear or use pressure tactics. If you have reason to believe that a financial institution really does need personal information from you, call the company yourself - using the number in your phone book, not the one the email provides. Also, rather than just clicking on the link provided in the email, type the company's official web address into your web browser yourself, or use a bookmark you previously created. Even though a URL in an email may look like the real deal, fraudsters can mask the true destination.

How do I find more information on how to protect my personal and financial data?

Personal firewalls and security software packages protect a computer network from unauthorized access, making them a must-have if you engage in online financial transactions. Use anti-spam, anti-virus, and anti-spyware software, like Ad-Aware.

How do I report suspected phishing attempts?

If you receive a phishing email, immediately forward it to the company that is involved. You can also file complaints with the Federal Trade Commission and forward them the email as well, at spam@uce.gov . This will help everyone—you, other Internet users, companies, everyone—protect and fight against phishing attacks.

What should I do if I've responded to a phishing email or website?

If you've responded to a phishing email and think you may have compromised personal identification or financial information, don't panic - but you'll need to act immediately. Notify us at csbprinceton@csbprinceton.com, credit card issuers, and credit reporting agencies, and ask them to flag your account and watch for unusual activity.

Still have questions?

Please email us at csbprinceton@csbprinceton.com.

How Can Someone Steal Your Identity?

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. Identity theft is a serious crime. People whose identities have been stolen can spend months or years - and their hard-earned money - cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit. The Federal Trade Commission at <http://www.ftc.gov> has an excellent website explaining identity theft, tips on minimizing your risk, and actions to take if you become a victim of identity theft. We encourage you to visit the following Federal Trade Commission web sites to minimize your risk of this growing crime.

The hyperlinked sites reflected herein are for your convenience only and you access them at your own risk. The use of a hyperlink never constitutes an endorsement of a company, product, or opinion. The use of the hyperlink does not imply that Citizens State Bank of Princeton agrees with the content being linked to and provides no guarantee that the content contains accurate information. Additionally, the linked sites may provide less security and/or a dissimilar privacy policy than that of Citizens State Bank of Princeton, TX.