Self-Audit Questionnaire for Consumers

Citizens State Bank is concerned about your privacy and security regarding your confidential financial information. This worksheet is being provided as a tool to evaluate the risks and security issues related to certain activities or behavior in your daily life. All the answers should be "Yes" and any "No" answers indicate that you may be at greater risk for an attempted or successful fraud attack. If you have any questions about the security of your accounts at the bank, please contact any of our Customer Service Representatives at 979-885-3571 Ext 256

Yes	No	
□	□	Your computers have anti-virus, spyware and malware protection software that is updated regularly with scheduled scans performed at least on a weekly basis. Your operating systems and web-browsers are also updated with the latest patches and you have activated your personal firewall. [If No, install and update these critical software tools regularly from legitimate sources.]
□	□	When using social media, you do not include personal information such as your physical address, phone number or date of birth including the year. Additionally, you do not list any additional confidential information such as the city you were born, Mother's Maiden Name or Social Security Number on websites or comments. [If No, remove this information from your profiles or comments.]
□	□	You use different passwords for your various banking sites which do not include easy guessable words or identifiable traits such as your birthday, name of family member or pet. Your passwords are not less than 5 characters and at least 2 of the characters are a number, special symbol and/or Capital letter. [If No, change your passwords. We recommend that you change them every 90 days.]
□	□	When using email, you never include confidential information about your financial accounts or other information that could provide access to your banking accounts. This would include your account numbers, bank name, login IDs, passwords and other confidential information. You do not click on links in emails unless you are sure they are from a legitimate or trusted source. [If No, stop including this information – email is insecure and can be intercepted.]
□	□	When discarding statements or other documents that contain confidential information, you always shred the document or destroy the information that is confidential. This information typically is the account number, name, address, bank or other identifying data that could be used to allow unauthorized access to your account. [If No, start shredding or masking data – dumpster diving is a big ID theft threat.]
□	□	You reconcile your monthly statements and report any discrepancy or suspicious activity immediately. You receive e-Statements to reduce the risk of mail theft. [If No, review transactions and balance statements monthly; request e-Statements.]
□	□	You have transaction alerts via email set up on your debit card or deposit alerts via email when your balance changes significantly. [If No, contact your institution to set up alerts as necessary to monitor activity.]

Answering "Yes" to all these questions will not guarantee that you will not be a victim of fraud, but it should lower your exposure to many of the common threats and risks in the marketplace.