Tips for Conducting Online Transactions

Your online passwords are the key to your personal information. If criminals know your password, they can use it to steal from you or pose as you in online transactions. The following are some simple tips to make your online experience safer:

DO

Install a reputable antivirus software program on all computers and keep them current.

Use trustworthy computers – Shared public computers, such as those in airport lounges, internet cafes, public libraries or hotel lobbies, could be connected to keystroke loggers or infected with password-stealing viruses. Don't use them to access websites containing personal or confidential information.

Make your password as long and complex as possible – Try to use a combination of upper and lower case characters as well as numbers so your password will be easy to remember, but hard to guess.

Use more than one password – Use a generic password for low-risk websites where there is little risk to you if someone figures it out. Not every website warrants the same level of protection as those containing personal or confidential information.

Periodically change your password – Changing your password every ninety (90) days is standard practice and reduces the risk of a criminal obtaining your information.

Safeguard your user name and password information – If you must record your user name or password, be sure to put it in a safe place or use password protected software to house all passwords.

Monitor your accounts – Review your account activity regularly and report any suspicious or fraudulent activity immediately.

Log off the system when you are finished conducting business – Simply closing the page or clicking "X" is not sufficient. In order to ensure the safety of your information, you should log out of the system prior to closing the window.

DON'T

Never email your password to anyone – Email travels the internet in much the same way a postcard travels through the U.S. mail. There is no "envelope" to protect the contents from prying eyes. There is no reason for anyone to know your password.

Avoid predictable sequences of characters or obvious passwords – Passwords such as "Password," "1234," or "abcd" are not secure choices and are easily discerned by criminals, leaving your information at risk.

Do not respond to an emailed request for your password or other confidential information – First Metro Bank and all other reputable companies will never ask you to provide confidential information in an email.

Business Owners

In addition to the tips listed above, here are a few additional steps for businesses:

1. Initiate a policy and process to discontinue online access to former employees upon termination;
2. Segregate duties among two or more employees so no one person has too much access or control;
3. Use firewalls to protect your business from outside intrusion or hackers; and,
4. Encourage your employees to refrain from writing down passwords and leaving them in obvious places.

FIRST METRO BANK
Member FDIC