Safe Surfing

Keep your Internet Banking Safe

When it comes to protecting your internet banking you can never be too careful. With the advancement of technology and the increase in internet banking users it is important to make sure you take the necessary precautions to prevent fraud.

There are simple practices that you can utilize when you do your banking online that will help decrease your chances of becoming a fraud victim.

General Internet use practices include:

DO NOT

Conduct banking transactions while multiple browsers are open on your computer
Use public or unsecured computers for logging into personal accounts
Share your account information with third party providers
Leave a computer unattended while logged in

DO

Be aware of your surroundings, make sure no one is shoulder surfing (watching and recording your key strokes)
Take care to properly store any documents that you use while internet banking, such as statements and invoices

Password guidelines include:

DO NOT

Share your password information with anyone
Use account login features that store your information
Use Social Security Numbers, driver's license, birthdates, family names, school, pets or workplaces for passwords
Use a pattern when changing your password
Use the same password for multiple accounts

DO

Use at least 8 characters
Include special characters, numbers and capital letters
Change your password frequently

Monitoring your account practices include:

DO NOT

Assume that fraud will not happen to you

DO

Check the last login date/time every time you login to make sure it was you

Review account balances and detail transactions regularly to confirm payment and other transaction data

Immediately report any suspicious transactions to your financial institution

View transfer history and confirm that there are no unauthorized transfers

Protecting your computer practices include:

DO NOT

Open mails from unknown sources

Click on links embedded in suspicious emails

Download attachments in suspicious emails or attachments that you were not expecting

Allow unauthorized access to your computer

DO

Install and maintain anti-virus, anti-malware, and anti-spyware software on your computer

Check your browser security settings and select at least a medium level of security

Clear the browser cache before online banking (this includes history, cookies and any copies of web pages that have been stored on the hard drive

Monitor and clear your cookies as necessary

Wireless Network protection practices include:

DO

Change the network password from a default to a complex and unique password

Disable remote administration for the wireless network hardware

Enable WPA encryption when possible

Disable broadcasting the network SSID

Social Networking practices include:

DO NOT

Download free applications from unknown users

Share user names, passwords or the information you use for authentication of your internet service with others

DO

Be aware of how much information you publish and who is able to view it

Treat downloads and applications like suspicious email until you can confirm the known trusted source

Some signs that your computer may be infected include:

You computer will run slower than normal

Continued or repeated Error messages

It will not shut down or restart

Displays a lot of pop-up ads when you are not connected to the internet

Computer sends emails that you did not write

A downloaded email appears with two different extensions (i.e jpg,exe or pdf, bll)

Repeatedly being asked to enter your user name or passwords

Being asked challenge questions if your computer was previously registered

Central Savings Bank
Consumer eBanking Tips:

Central Savings Bank will never send you an email asking to confirm your personal information.

Consumer eBanking:

DOES NOT

Use pop up windows to display login messages or errors

Use error messages that include an amount of time to wait before trying to login again

By incorporating these practices in your internet banking use you will be taking precautions to protect yourself from fraud. If you have any questions or would like more information on practices for protecting your internet banking please contact:

Central Savings Bank
511 Bingham Ave.
Sault Ste. Marie MI, 49783

906-635-6250

www.centralsavingsbank.com