PEOPLES STATE BANK OF COLFAX

PARTNERING FOR ONLINE SECURITY

Safe online banking depends on continuing and strengthening our partnership.

The bank has security measures to protect your account information, but they can't be effective without your help and cooperation. Many of the fraudulent activities come from a result of hacking into individual user accounts and from there electronically breaking into your information and security codes.

Some common sense and easily implemented precautions can help you safeguard your personal information:

- **Strong passwords** - It is advisable to have a strong password that cannot be compromised, while an easy password is easy to remember, a more complex password is more secure. Use a multi-character password if possible and avoid using obvious characters such as personal name and address. Never share online banking details such as log in and passwords with family or friends.

- **Anti-Virus Protections** - Make sure the anti-virus software on your computer is current and scans your email as it is received.
- **Email Safety** - Email is generally not encrypted, so be very careful when sending any sensitive information such as account numbers or other personal information. Never click on link's within emails that are from an unknown source. Many virus' are launched through email messages to unsuspecting victims.
- **Sign Off and Log Off** - Never leave your computer unattended when logged into Internet banking. Always log off by following the bank's secured area exit procedures.
- **Don't get Phished** - Crooks are always trying to get your personal information and they know of many ingenious methods. Do **not** respond to any unusual email requests for personal information.
- **Monitor your accounts** - Check your accounts regularly. Let us know immediately if you encounter anything that does not seem right.

ONLINE AND MOBILE THREATS: Understanding how criminals try to trap you is your first line of defense:

- **Phishing** - This is the criminal attempt to steal your personal information through fraudulent emails or smart-phone texts. They are often very believable, luring the victim to a site that asks them to provide (or "verify") personal financial details such as your account number and/or social security number. Heritage State Bank will never ask you for personal information through email correspondence. If you are ever in doubt, pick up the phone and call us immediately before releasing personal information.
- **Card Skimming** - This is a criminal's attempt to gain a victim's personal information by tampering with ATM machines. Fraudsters set up a device that can capture stripe and keypad information such as PINs and accounts numbers. Use ATMs you know and trust-as well as examine the machine closely if something does not look right-DON'T use it.
- **Spyware** - This is the term used for criminal software that a victim unknowingly loads on a personal computer. Once there, the spyware collects personal information and sends it to the criminal. Up-to-date security software is the best defense.

HELPFUL HINTS:

- Cyber-criminals often prey on those who are most vulnerable, such as senior citizens or young adults, who may not be as aware of the technical aspects of the threats. Make sure you alert any friends or family members who might be in this category.
- Those who monitor their accounts online often detect fraud earlier than those who rely solely on paper statements.

Let's work together to secure your personal information. If you feel you may have become a victim of any of the above-mentioned compromises, please contact a banking representative at either of our branch locations immediately.