Community 1st Bank

Helping You Do the Right Thing to Protect Your Financial Identity

IDENTITY THEFT

Did you know identity theft is one of the fastest growing frauds? Someone could steal your financial identity with as little information as your social security number. Identity theft is when someone assumes your identity to open up new credit accounts, spends the available balances and does not pay the creditors, all in your name.

Steps to protect yourself:

1. Review your credit report annually for accuracy by contacting the Annual Credit Report Service at http://www.annualcreditreport.com, which provides one free report per year. You may also contact the individual credit reporting agencies.
2. Review your statement to ensure all activity was initiated by you. If you do not have a secure mailbox, electronic statements may be a good option to avoid physical theft.
3. Protect your bank account information and do write confidential information on checks or carry your Social Security number or other confidential information with you.
4. Unless you initiated the call, never provide confidential information over the phone. Criminals may initiate a call to inform you of a prize you have won or to inform you of a job offer that you happened to be "just the right person" for in order to obtain confidential banking or personal information. If it seems to be too good to be true, it most likely is.

CYBER CRIME

Criminals are becoming increasingly savvy with electronic frauds as they become more sophisticated. The attack on your personal information can come from anywhere in the world.

Tips to prevent a cyber attack:

1. Install anti-virus, anti-malware, anti-spyware software and make sure it is up to date. This is the first line of defense and critical in our current technology environment. These threats have the ability to steal and transmit confidential information to the Fraudsters. See below for definitions
2. Use a strong password which should have at least 8 characters and be a combination of uppercase, lowercase, numerical, and special characters, which is changed often (about every 90 days). It should not be a word in the dictionary or family names, something that is easy to remember and hard to guess.
3. Before inputting confidential information or login credentials, verify internet session is secure by looking for the "s" in the web address, i.e. https://
4. Avoid having your computer "remember" the log-in information, the risk far outweighs potential time savings.
5. View your account frequently online from a secure computer to ensure all activity is proper.
6. Never access your online banking or other sites with confidential information from a public computer (hotel, library, school, etc.).
7. Be suspicious of an unexpected email representing it is from a known company or government agency. If there is a phone number, call to ensure it is valid as crooks often pose as a legitimate operation. Be wary of emails sent to you or to a business which may include invalid emails such as service@xyzcompany.com or accounting@abccompany.com.

CYBER CRIME (CONT.)

8. Employment requiring the use of a personal bank account is suspect. Positions such as payment processor, tax management, mystery shopper, etc. requiring usage are not legitimate.
    a. No legitimate business would require you to move funds through your personal account.
    b. Report any such schemes to law enforcement immediately.
9. Commercial customers are not covered by consumer protection laws such as Regulation E and are responsible for implementation of additional security measures such as transaction verification and providing view only access where appropriate to mitigate risk. It is prudent to perform a risk assessment and review internal controls based on changes within the organization at least annually.
10. **Contact a representative at Community 1st Bank immediately if you believe any of your account information has been compromised.**

Computer Threat Examples:

Malware- software used by hackers to gather sensitive information or gain access to private computer systems. 'Malware' is the general term used for all hostile or invasive software.

Phishing- Techniques used by crooks to acquire sensitive information through social engineering. Phishing appears to be a legitimate website, message or other communication.

Spyware- Malicious software designed to steal sensitive personal information such as user IDs, passwords, answers to security questions, etc. without the user knowing it.

Keylogger/Sniffer- Captures information by tracking and logging keystrokes, capturing screen shots or recording histories and information copied to "clipboards".

Virus- Computer program that can replicate itself and make unauthorized changes to your computer.

Adware- Bombards your computer with unwanted ads sometimes to the point it is unusable.

Rootkit- A stealthy type of malware which hides the existence of certain processes or programs from normal detective methods. Removal may be practically impossible and can be very complicated.

Trojan- Malware that appears to be a legitimate file and allows hacker unauthorized remote access to your computer.

Please remember, if you are suspicious about an activity as it relates to your personal information as requested by someone you don't know, contact us immediately at Community 1st Bank so we can assist you in determining if a fraudulent act is in process.

Post Falls Office: (208) 457-6310

Coeur d'Alene Office: (208) 635-7171

Like us on facebook to receive additional information on protecting your identity and confidential information as well as other valuable updates and news or visit our website, http://com1stbankid.com for additional information.