INTERNET FRAUD

- Legitimate businesses will never ask for confidential information such as account numbers, passwords, PIN numbers, credit card numbers, SIN numbers, bank accounts or social security numbers over the internet or by phone. Do not respond to such requests.
- Delete unsolicited emails that ask for personal information. If you suspect you have provided confidential information to a fraudulent site, contact the customer service number on the back of your card or from your account statement.
- Never send payment information via email. Information that travels over the Internet through email is not fully protected. Reputable merchants have encryption technology to protect your information. It is identifiable by a padlock icon.
- Use anti-virus software, spyware filters, email filters and firewall programs to help ensure information safety for your computer. Keep your software updated.
- Keep all your passwords and user names secret.

Alberta Government

Slave Lake Victim Services

Slave Lake Victim Services |
1005 - 6th Avenue
Slave Lake, Alberta
T0G 2A3
Phone: (780) 849-6884
Fax: 780-849-2133
www.slavelakevictimservices.com

"Victim Services Working in Partnership with the R.C.M.P."

Internet Fraud

Credit Card Fraud

IDENTITY THEFT/PHISHING

- Identify theft occurs when someone appropriates your personal information to open credit card accounts. They run up charges on the account and have them sent to a new address so that you may not immediately know there is a problem. They can establish cell phone services, open bank accounts, and write bad cheques.
- They can make major purchases in your name.
- Phishing is a term used for fraudsters looking to commit identity theft. It is the creation of email messages and web pages that are replicas of existing legitimate sites and business. The term includes emails that notify you that an account will be immediately shut down unless you reconfirm your billing information. They upset you in hopes of getting an immediate reaction.
- Report phishing to reportphishing@antiphishing.org . If fraudulent activity has resulting from a phishing email, contact the police.
- Report suspected fraud to Phonebusters – call 1-888-495-8501 or www.recol.ca

Slave Lake Victim Services

BANKING

- Routinely check your monthly credit card and bank statements.
- Never disclose your PIN number to anyone. No seemingly trusted source including the financial institution, the police or a merchant should ask you for your PIN.
- Shield your PIN entry with your body or your free hand.
- Keep a record of transactions, write down confirmation numbers and review on statements thoroughly
- Shred all personal and financial information such as credit card offers, ATM receipts, bank statements, before you dispose of them.
- Pay attention to billing cycles, or to a lack of mail being delivered to your address. It is possible the mail is being intercepted.
- On your checks only put your initial and your last name
- Put your work phone on your checks instead of your home phone

CREDIT CARDS

- Report lost or stolen cards immediately.
- Keep on eye on your credit card when it is processed to make sure it is not copied through a skimming device (a second card reader).
- Ensure you get your card back immediately, that way criminals have less chance to copy the information. Check to make sure it is your card.
- If the cashier wants to swipe your card twice, always ask why.
- Never leave your cards unattended at work. There are more credit cards thefts in the workplace than anywhere.
- Minimize the number of credit cards you carry in your wallet or purse.
- Do not leave your credit cards in the glove compartment of your car. Many credit card thefts are from glove compartments.
- Treat your cards as if they were cash; don't leave them in places where criminals can access them.
- Never lend your credit card to anyone.
- Sign the back of your new card right away. Destroy old cards.
- Make a list of all your cards and their numbers and keep in a safe place.
- A Credit Bureau report alerts you to sudden changes in your credit card balances. A variety of services are available for a fee.
- Check with your credit card company for specialized protection programs.
- Photocopy all your cards and passport both sides
- If your credit card is stolen could call a national credit reporting agency:
  - Equifax 1-800-465-7166
  - TransUnion 1-877-525-3823