How safe is your online information?

CALGARY, ALBERTA - MARCH 17th, 2016 - With nearly 30 million active Facebook and Twitter users across Canada combined*, social media giants are often celebrated for bringing people together through the gift of instant communication. However, social media has also brought scammers closer to consumers BBB is helping social media users spot cyber criminals.

The third week of National Fraud Prevention Month is all about cyber security and how to protect yourself against the dangers of everyday digital practices.

So what are the risks of using social media?

- Your personal information and identity could be stolen
- Cyber criminals can use your identity to make fraudulent purchases or engage in other illegal activity under your name
- Depending on what kind of information you include on social media profiles, it could tip off burglars looking for empty homes and easy targets
- If you add friends or followers you don't know, you could be inviting scammers who are phishing for your personal information into your social network
- Hackers could gain access to your social media profiles and pose as you as they send out spam and malware to your friends and other contacts

"Identity theft and phishing aren't new scams, but the tricks that scammers are using to lure their victims are new," says Sandra Crozier-McKee, president and CEO of BBB Serving Southern Alberta and East Kootenay. "Social media has become a regular part of every day life, so people think nothing of "Liking" or sharing posts. It is crucial for consumers to understand the responsibility that comes with using social media and educate themselves about the risks of misuse."

<u>Do you recognize any of these? Check out these popular social media scams:</u>

- Fake friend requests: Leaving your profile wide-open to the public allows you to receive friend requests from anyone and everyone, including scammers. If you readily accept friend requests without verifying that person's identity, you can unknowingly grant scammers access to your account. He or she creates a new account under your name and fills it with your photos, interests and status updates. With 1 billion active daily Facebook users worldwide , you are unlikely to spot the impersonator.
- Like farming: Soliciting "Likes" and shares of popular photos that tug at the heartstrings such as children cancer patients, animal abuse, countries that are victims of natural disasters etc... Scammers are actually hiding behind some of these pictures. "Liking" these images or pages that belong to malicious Facebook apps are phishing tools to access info for identity theft and other illegal activity.
- Viral videos: More than just a wildly popular video, these videos actually contain viruses. Celebrity scandals or bogus news stories that spark your interest will prompt you to update your video player in order to view the video. If you activate the updating software, a virus or other malware will be downloaded to your device and the scam will be automatically shared with all of your friends.

- Hidden URLs: Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer. Instead, hover your mouse over the link and its true destination will appear at the bottom left corner of your screen.
- Gossip, scandals and other entertainment "news": Scandalous photos of your favourite celebrities or sensationalized news items concocted by scammers to pique your curiosity. If you want to view the photo or read the bogus article, you will be prompted to activate or download a third party application. These apps will request your profile information and be able to post content on your behalf, install malware on your device without your knowledge and ultimately leave the gateway to identity theft and other types of fraud wide open.
- Hidden Charges: "What type of Friends character are you? Find out with our quiz! " If you enter your info and cell number, as instructed, after a few minutes, a text turns up. It turns out you're more of a Rachel than a Monica. Well, that's interesting ... but not as much as your next month's cell bill will be. You've also just unwittingly subscribed to some dubious service that charges your mobile phone account every month. As it turns out, that "free, fun service" is neither. Be wary of these bait-and-switch games.
- Free items/giveaways/lottery/sweepstakes: Congratulations! You've won a free trip to a tropical destination, or a luxury car or a large cash prize. However, in all of these instances, in order to collect your winnings you are asked to wire money and provide other personal information. Be wary of unsolicited, free contest prizes and never wire money to a stranger.
- Condolence scams: Users will get a Facebook or Twitter post supposedly from a family member or friend that has fallen on hard times and needs your help. Or you receive a notification of the death of a loved one stating you are the beneficiary of the deceased's estate. In either instance, you are asked to wire money to help your friend or to claim your inheritance. If you're suspicious, contact your family and friends directly to verify their circumstances.
- Chain Letters: You've likely seen this one before. It may appear in the form of, "Copy and paste this Facebook status and Mark Zuckerberg will donate $4.5 million to the first 1,000 users!" This was later declared a hoax, but why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.
- Phishing email: Receiving an email that appears to be from Facebook, Twitter or another social media outlet addressing you by name may seem legitimate. The message could claim there is a problem with your account prompting users to click on a link that leads to foreign domain installing malware on your computer, or provide personal information to verify your account. Either way, you are granting scammers access to your personal data and opening the window for identity theft and other types of fraudulent activity.