Top 10
Facebook Scams

1. 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 1.23 billion people on Facebook worldwide, you are unlikely to spot the impersonator.

2. 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.

3. 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.

4. Custom profiles
Another common scam offers to change your Facebook profile look or layout. A famous version was the Facebook Black scam. It supposedly gave you a slick, black color scheme. These scams try to trick you into installing a rogue Facebook application, which gives scammers access to your personal data. It will also spam your friends to try and trick them, too.

5. 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.

6. Find out who has been looking at your profile
Ever wonder who is checking you out? Again scammers are preying on your curiosity and solicit your account information through a third party application. Whether you're wondering if that cute guy or girl is checking you out, or if you have legitimate cyber-stalking concerns, there is no way to accurately find out who has been viewing your profile.

7. 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.

8. Condolence scams
Users will get a Facebook 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.

9. Current event scams
The recent missing Malaysia plane is the latest target of social media scams. Links to pages and videos claiming the plane has been found and that there are survivors have surfaced on Facebook. Clicking on the links will take users to websites pretending to be YouTube, CNN, the BBC or Facebook itself. There, they'll find videos promising exclusive information claiming to solve the mystery of flight MH370, but only in exchange for personal information.

10. Phishing email
Receiving an email that appears to be from Facebook 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.

More Social Media Scams

Jobseekers Linkedin to Employment Scams

How the scam works:

Job-seekers create a professional profile on Linkedin by uploading their resumes and experience in hopes of being contacted by an employer or recruiter with a potential employment opportunity. Scammers create fraudulent profiles posing as recruiters and send a message with a link to an illegitimate website that asks for personal information. Any personal information obtained by the fraudulent recruiter will allow them to steal your identity, access bank accounts or even install harmful malware on your computer or other mobile devices. The scammers will usually ask for financial information or even social insurance numbers or birthdays.

According to Linkedin, there are more than 250 million users worldwide.

Instagram Scam

How the scam works:

Active Instagram users notice an account from a credible and established business. Scammers are impersonating various businesses including retailers, luxury fashion brands and even airlines. The accounts are promising a lavish prize or giveaway in an attempt to secure more followers. Once you've started following the fake business account, users receive messages soliciting personal information which some users willingly provide thinking they are required to hand over in case they are selected as the prize winner.

According to Instagram, there are over 200 million active users per month.

Pinterest Phishing Scam

How the scam works:

Targets receive an email from Pinterest saying that a friend has shared a "pin" (the term Pinterest uses for digital scrapbook image). Common scam pins include celebrity and beauty photos, giveaway offers, before and after diet pictures and even infographics. Targets are intrigued enough to open the email and click on the pin to find out what their friend has shared with them. Clicking on the "pin" redirects targets to a foreign website that has nothing to do with Pinterest and instead the site is a selling ground for counterfeit products, promoting fraudulent work from home jobs, telling bogus news stories or worse, installing malware on your computer.

According to Pinterest, more than 70 million people are pinning worldwide

Twitter Phishing Scam

How the scam works:

This particular scam sent out emails resembling those you might receive from Twitter if you get email notifications of your Direct Messages. The email says something like, "hey! check out this funny blog about you..." and provides a link. That link redirects to a site masquerading as the Twitter front page. Look closely at the URL field, if it has another domain besides Twitter but looks exactly like our page then it's a fraud and you should not sign in.

BBB
Start With Trust

BBB Serving Southern Alberta and East Kootenay

bbb.org
info@calgary.bbb.org
(403) 531-8784