Facebook Scams

Scammers constantly target Facebook and other social media with all types of scams, some with links to malware that can affect your computer or other takes to defraud you. It is important to stay alert.

The following is a list of some of the general types of scams that have targeted Facebook users recently.

1. **Profile Viewers and Profile Blockers -** These scams promise to show you who has been looking at your profile or who has blocked you from theirs. NONE of these apps work. Facebook doesn't give the developers access to the data required to create them.
2. **Free iPads & iPhones –** Don't be fooled by messages stating you can test and keep an iPad, iPhone etc. These are all marketing gimmicks.
3. **Free Facebook Credits –** This scam is targeted for the gamers on Facebook. Credits are used to purchase items in Farmville, Cityville, etc. Credits cost real money and you aren't going to receive a large sum of them for free.
4. **Free Items, Gift Cards & Tickets –** If it sounds too good to be true, then you can be sure that it is on Facebook! You aren't going to get free airline tickets, Subway or Starbucks gift cards or a Facebook hoodie just by completing a survey.
5. **Breaking News Stories –** Anytime a major news story breaks, keep your guard up. Scammers love to trick unsuspecting users with promises of "exclusive coverage."
6. **Phishing Attempts to Steal Your Login Info –** If a scammer can get your login credentials, then they can wreak all sorts of havoc before you reclaim your account. Messages pretending to be from Facebook Security is a popular way they trick users.
7. **New or Extra Facebook Features -** Dislike buttons, apps to change your Facebook colour or see who unfriended you are just a few examples of these scams. While there are legitimate browser extensions that can offer these features, scammers often insert adware or malware into the plugins. We recommend that you only install apps and extensions from trusted, well-known developers.
8. **Shocking & Sexy Headlines –** Anything that starts out with "OMG" or "Shocking" is best left alone on Facebook. They lure in victims with outlandish, steamy or perverted messages. These usually end in a survey scam and a video that doesn't play.
9. **Fake Celebrity Stories –** Facebook is not the place to receive your celebrity news and gossip! Scammers use fake deaths and other sensational stories to entice users. These often spread very fast, because users share the posts before verifying the story.

10. **“Help I’m Stranded and Need Money” –** If you get a message from a friend stating that they are stranded in London or some other exotic locale, don’t rush down to Western Union to send them cash. They have likely had their Facebook account hi-jacked by scammers.

11. **False Privacy Settings:** scammers mainly want to get your login details, so make sure to verify messages claiming to be from Facebook security. Even the examples above show that they can look very credible and trustworthy

Latest specific scams

1. **Girl killed by husband -** The scam involves a fake video that's being shared across Facebook titled "Girl killed by husband just because she kissed another man. "The video seems to show an Asian woman about to get her head chopped off with a sword, and it looks like tons of people have already liked and shared the video. But if you come across it, DO NOT CLICK ON IT. The video, the comments, the shares and the likes are all fake. If you do click on the video, you're taken to a third-party website that looks like Facebook but it isn't. Once you try to play the video, you're first told to share it with your friends (which spreads the scam) and then claims you need to install a plugin for the video to work on your computer. "When clicking on the install button, users end up downloading an executable file on their computers, which drops adware or malicious code.

2. **Free iphone 6 -** The scam that promises to give you a free iPhone 6. Yes, it sounds too good to be true and it is. The scam first shows up as a shared post. Users who click it are taken to a Facebook fan page where they are asked two or three things. The first is to "like" the page and the second is to share the page with your friends so they can enter the contest too. Sharing the page spreads the scam to your friends. Then to get your free iPhone, you're taken to a different website, and that's where the real trouble begins. That external site tells you to fill out a quick survey to get your free iPhone, but if you fill it out, you instead sign yourself up for services you likely don't want.

3. **Rihanna sex tape with her boyfriend -**The scam is there is no sex tape nor a Rihanna DVE, nor a Rihanna MP4 video

There you have it! This is not an exhaustive list by any means, but certainly gives you a good start on what to look out for.

These scams can spread Wall to Wall between users by click-jacking and like-jacking attacks, rogue applications and Fake Events, etc. Scammers will exploit any method they can, and sometimes can be quite creative. A common end game is a survey scam, but others are more malicious in their intent. Many users have received trojans, viruses and other malware infestations by falling victim to scams on Facebook.

To check out the best way to minimize the risks when using Facebook have a look at the following link
http://www.thatsnonsense.com/facebook.php

Posted 1st October 2014