Social Media Threats To Be Aware Of

Social networking sites like Facebook, Twitter, Instagram, Google +, and many other popular online hubs link us together in a digital society where we can make the most out of our social liberties. More businesses are also starting to re-allocate budgets towards social media in place of traditional advertising. While there are numerous benefits to sharing and communicating through social media, it also has its share of risks. Cybercriminals have taken advantage of the carefree way that people use social media platforms, usually with bait schemes that puts users at risk with a simple tap or click of a disguised link.

Here are some widespread cybercriminal schemes that you're most likely to encounter on social networking sites, what they really do, and tips on how to avoid them.

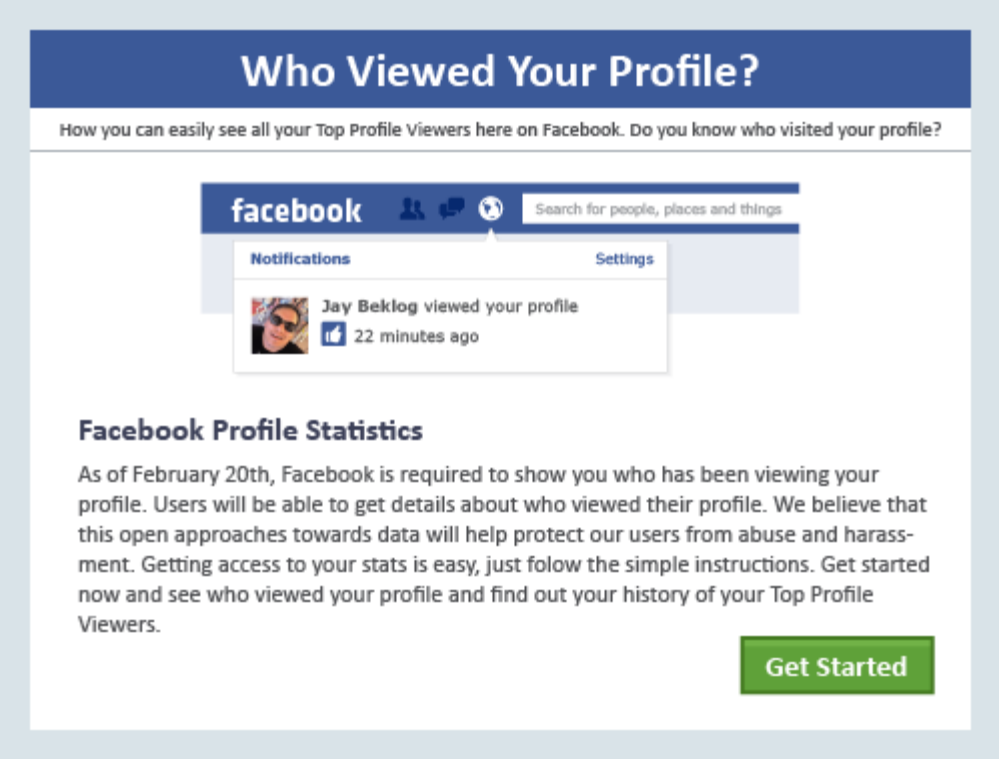
1. The Facebook Color Changer

Say goodbye to the boring blue profile and say hello to the new pink profile! An enticing scheme that lures users to malicious phishing sites, the Facebook Color Changer asks you to share it with your friends or watch a tutorial video by tricking you to click on an ad. At one point, it also offered a variety of colors. But what it really does is allow hackers to obtain access to your profile and spam your friends. Mobile devices could also be infected with the malware brought by the Facebook Color Changer, offering users fake antivirus apps.

How to avoid: While Facebook constantly improves its security to address current threats, it's still better to do the tune-up yourself and know which apps to block. Beef up your security by changing

your password regularly and deleting unnecessary apps. Do not trust third party notifications and make sure you follow credible sources.

2. Who Viewed Your Facebook Profile?



A clever and tempting scheme that would interest a lot of people, this Facebook scam appears as ads or as messages posted on your wall by your friend (accidental spam) that invites users to check who's viewing their profiles. Clicking on them instantly gives spammers access to your Facebook account and network, as well as possible access to the other people on your friends list.

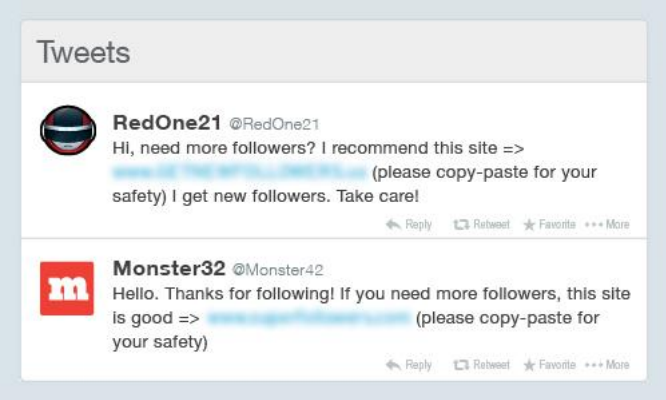
How to avoid: Always be wary of suspicious links, messages and ads, however tempting they may be. Even if they're sent by your friends, don't fall for it unless you get first-hand verification of its legitimacy. After all, if Facebook really wanted its users to have this functionality, it shouldn't take a third party app to enable it. All in all, it's still best to report this abuse and delete irrelevant links and messages to avoid any kind of malware download.

3. Outrageous and “Shocking!” NSFW (Not Safe For Work) Videos Facebook Scam

Scams that play on our curiosities are popular bait methods used by scammers and cybercriminals. Explicit videos with outlandish titles garner a lot of attention and often create a viral frenzy among unsuspecting netizens. Fake videos that come with NSFW labels actually point you to random surveys or fake websites that could harvest your personal information

How to avoid: Before clicking on anything, be sure you know where it’s coming from. Or better yet, don’t click on them at all. As these videos become viral, so does the malware behind it. Even if some posts contain real videos, there could still be malware embedded, such as rootkits that are more difficult to remove even after you clean out or reload your computer. To be safe, run a scan with your security software to make sure your computer is clean.

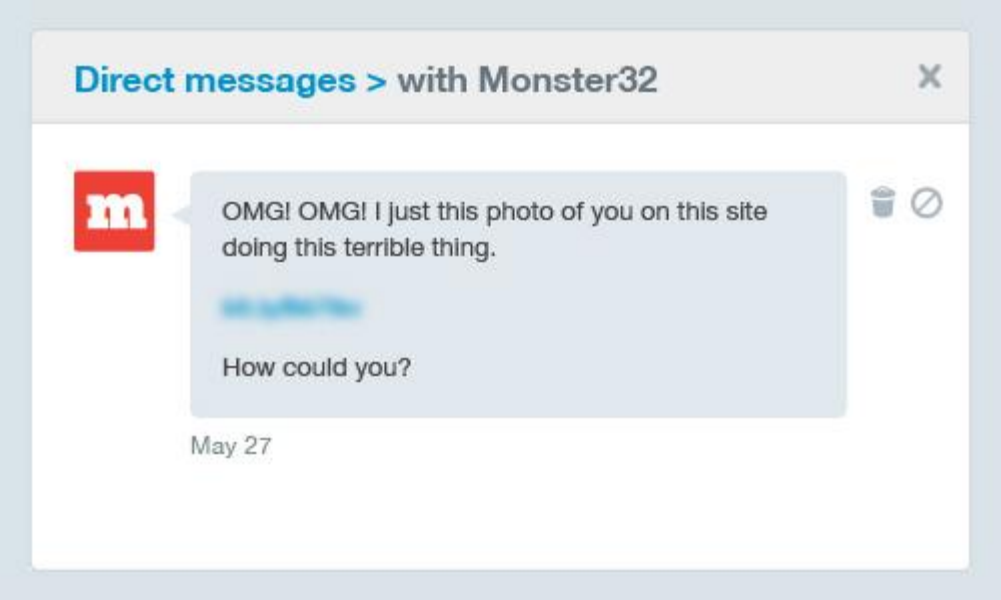
4. Twitter Instant Followers



More followers, more likes, and more retweets allegedly lend more credibility to a user's online image. Whether you want to promote yourself or simply accumulate thousands of followers, using a service that promises such can compromise your security. Apps and services that offer instant followers compromise Twitter user accounts by making the user follow other users of the app and send out Twitter spam that advertise the app.

How to avoid: Be cautious about giving unverified apps or services access to your Twitter account--or any other account, for that matter. Scammers behind malicious activities know exactly what you want based on the hacked intelligence they gathered from you. Be wary, despite of yourself, of anything that promises quick or on-the-fly solutions. Additionally, before logging into your account, make sure that you're logged into the official Twitter website (https://twitter.com/). Signing into a disguised log-in page is like giving cybercriminals your credentials on a silver platter.

5. "Just Saw This Photo of You" Twitter Bait Scam

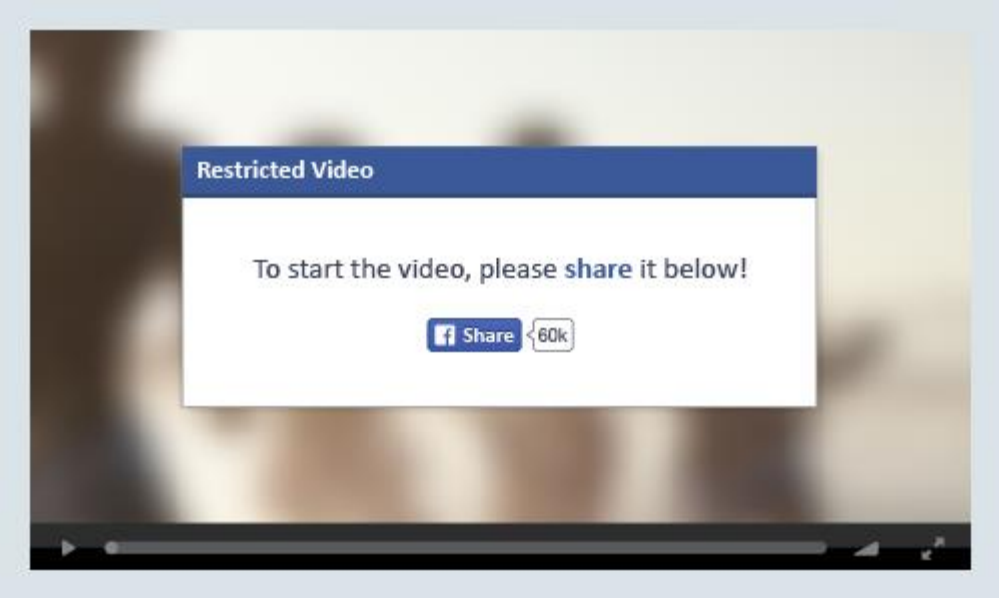


Some scams just get so desperate that they're willing to cramp your personal, intimate space. This Twitter scam is designed by cybercriminals to compel you to click on malicious links with messages such as "just saw this photo of you". Whether you have naked photos or not, it could make you paranoid enough to check it out. This scheme can hijack Twitter accounts and consequently spam followers and other users or lead them to phishing sites.

How to avoid: Don't be tempted to click on links that speak to you directly. Remember that they are scams that are designed to invade your privacy and hack into your system and accounts.

Increase your security and don’t follow back people you don’t know. Make your profile private to avoid getting suspicious requests.

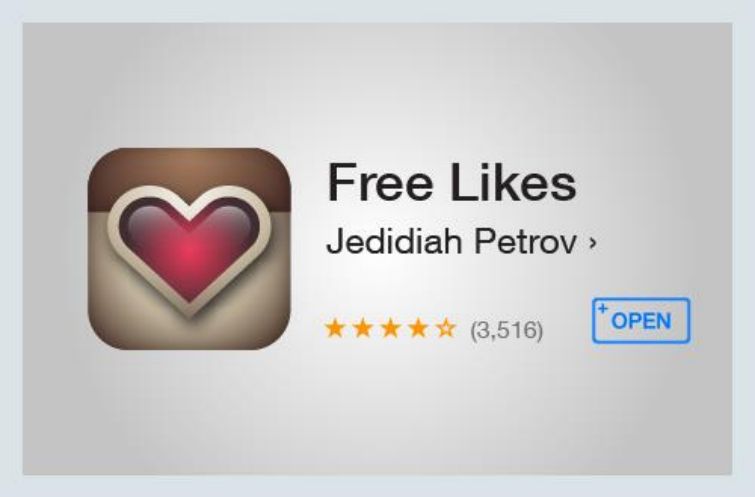
6. Naked Video Facebook Scam



Any material that offers graphic viewing of any form of nudity becomes more or less, viral. Most people like to look out of sheer curiosity but in reality, it is a crime and an invasion of privacy. The “naked video” Facebook scam which appears as an ad or post revolves around the premise of distributing malware by leading you to a fake YouTube video after clicking on the link. The fake site will display a message that says your Adobe Flash Player crashed and that you need to install an update. The fraudulent Flash Player installer then triggers the infection and its malware, usually a Trojan, installs itself as a browser extension. This malware can then access your Facebook photos and repeats the malicious activity by inviting your friends to view fake naked videos.

How to avoid: Stay away from so-called scandalous videos. Make sure you use robust security software that guards you from drive-by downloads and run a regular scan to make certain that your computer isn’t running rogue programs.

7. Instagram InstLike Promises Free Likes and Followers



Thousands of Instagram users were duped into sharing their account details with the InstLike scam. In return, they gained plenty of likes and followers. According to reports, this malicious app steals the user's password and other information to feed the malware and spread the infection. Despite being reported and flagged, InstLike is still operational and continues to scam unknowing users.

How to avoid: It's difficult to avoid getting reeled in by social media scams, so it's important to be aware of trending cybercrime methods. If you were tricked by this scam, change your password and delete the app. Use security software to check your system and rid your device of any remnants of the infection. In a nutshell: don't download anything that offers quick fixes.

8. Tumblr Dating Game

Scammers like to take advantage of the naiveté of uninformed single people. The Tumblr Dating

Game has tricked many such users into clicking on links that appear in messages. Victims are then urged to make accounts which only led them to adult splash pages and ads. These ads would generate cash for the scammers, which they get for every sign up.

How to avoid: Cybercriminals go to great lengths to lure people into subscribing to solutions that offer personal satisfaction. In most cases, they profile their victims so they know how to target you. If you're not sure about a website or a mysterious message, don't click or visit them. It's also wise to report and block anything suspicious.

9. Pinterest Bogus Pins

Normally, we wouldn't think social networking sites like Pinterest would be bombarded by scammers. But in reality, cybercriminals are as interested in your pins as you are. Apart from using other apps and services, these online con artists entice users to click on bogus pins that direct them to fake surveys or other phishing websites. The pin could be anything from freebie ads to promotional schemes that appear to be from legitimate companies. Once you fall prey to this scam, your security will be instantly compromised and the malicious code will start spamming your followers.

How to avoid: Think twice before you open notifications from your email or from your Pinterest account. Always check sources and be careful when viewing pins and boards. Report incidents at once and block suspicious users. Change your password if you think you've been compromised and bookmark the real Pinterest website (https://www.pinterest.com/) to avoid visiting counterfeit ones.

Conclusion

Scammers are clever and they know just who to target with fake offers that are hard to distinguish from legitimate ones. This is how they play on our unsuspecting nature and attack us with one scam after another, stealing our accounts and feeding the spam ecosystem. The best way to avoid scams is to be educated on such online abuses and secure your devices with a security solution that's designed to protect you against social media scams.