

[Oakmere Road: Top 5 social media scams to avoid](#)

Scammers have been worming their way into giant social media networks to trick people into giving over their personal and financial information.

Over the past year, the number of phishing attempts on social media networks like Facebook (FB, Tech30), Twitter (TWTR, Tech30), Instagram and LinkedIn (LNKD, Tech30) has exploded 150%, experts at security firm Proofpoint (PFPT) say.


That's because fraudsters can use social media to target hundreds of thousands of people at once, but also blend in with the crowd. They mimic users and their activities, and they take advantage of the way people use social media to deal with business problems.

Here are five of the most cleverly cloaked scams on social media right now, according to Proofpoint:

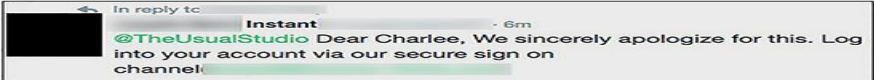
[1. Fake customer service accounts on Twitter](#)

Online criminals set up fake customer service accounts to phish for bank login and password information and other sensitive data. These imposter accounts look very similar to that of real businesses, but are often one character off -- or they include an extra underscore or other keyboard character.

When someone tweets at their bank or example, scam artists will intercept the conversation, and reply to that message with what seems like an authentic answer.



A real customer tweets at a major bank.

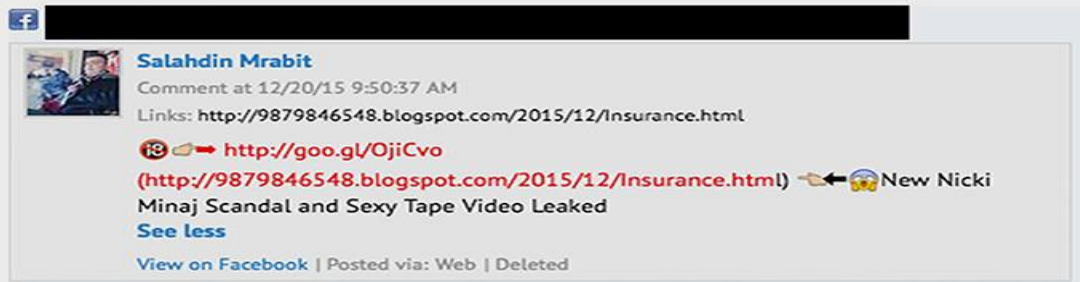


Fraudsters intercept the tweet with a link to a fake support site that tries to steal her actual bank account credentials.

PROOFPOINT

2. Fake comments on popular posts

A popular news story or social media post might generate a lot of comments. Fraudsters like to take advantage of that large audience by adding their own comments with links to other buzzy headlines that lead to credit card phishing scams.



Scammers often pretend to be Facebook users so they can comment on posts that lead to a credit card phish.

3. Fake live-stream videos

As more media companies start streaming their shows and movies online, scammers are jumping on the bandwagon.

They do things like comment on the Facebook page of a sports team with a link that leads people to believe they can watch a free live stream of a game. But the links lead to a fake website that asks for personal information in order to start the video, which very often doesn't exist.



Here's a comment that an online thief posted on the Facebook page of an NBA team that promises a live-stream of a game.

4. Fake online discounts

Fake online discounts work similarly to fake customer service accounts. Schemers will set up social media accounts that look like legit businesses, then pretend to offer a real promotion. In reality, they want to trick people into giving up their personal information.



Fraudsters create fake social media accounts for real businesses like Netflix to carry out financial phishing scams.

5. Fake online surveys and contests

These tactics have been around for years and are designed to get answers to personal questions that fraudsters can mine and sell later. But criminals embed them into social media posts that often look legit because there's a normal looking profile picture and link, thanks to URL shorteners.



Criminals use the comment section to target as many people as possible with fake online surveys and quizzes that steal personal information.