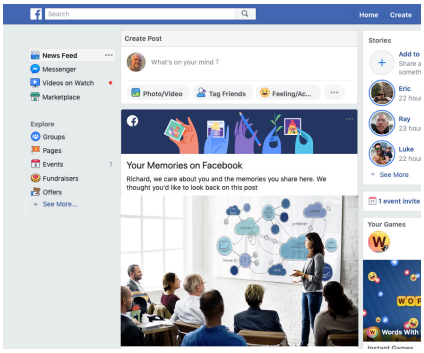
Lessons from four social media scams

The Office Photo Scam

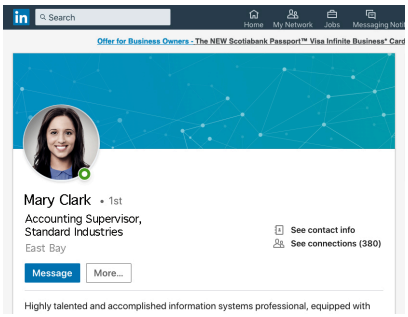


Avoid posting photos on social media that include a work computer or a conference room. If the photo of a workplace computer or information on a whiteboard is clear enough to read, fraudsters can steal information. Even if the photo is small or slightly blurry, fraudsters can identify icons that appear on a computer desktop such as the type of anti-virus that's installed. The fraudster uses that information to sound credible when calling an employee, posing as someone from tech support.Last year, this trick helped law enforcement catch the man behind one of the world's biggest robocalling operations.

The Account Verification Scam

It's an old scam that still works: no, your social media account doesn't need to be "verified." An email arrives, warning you that your social media account will be suspended "soon" if you **don't click the link and verify who you are.** Ignore that message! This scam is still one of the most common because so many people fall for it. Victims click the link to "verify" the account by entering their password. This allows fraudsters to gain access, take over the account, and lock the user out. Since many of us still use the same passwords on multiple accounts, it gives fraudsters access to other accounts.

The Targeted Victim Scam



If anyone is able to view your social media account, crooks will take advantage of it. If the setting on your social media accounts allows "friends of friends" or the "public" to view your posts, fraudsters can cause trouble. Last year, a large US company's accounting system was breached because of an employee's Facebook post. The fraudster identified the employee on LinkedIn, searched Facebook for her personal posts, saw that her son played high school basketball and downloaded the practice schedule, embedded a virus in the document, and emailed the "revised schedule" to her from an email address that was similar to the coaches. The victim opened the document on a work laptop computer, exposing the company's accounting system to the computer virus.

The Game Player Texting Scam

Fraudsters are playing games online, so be careful what you disclose in chats. Many web and app-based games like Fortnite and "Words with Friends" allow players to chat with each other. Crooks masquerade as players who need money right away to solve a personal crisis or are interested in information about the player's employer. Patient fraudsters establish a casual relationship with the unsuspecting player over the course of days or weeks, gradually piecing together information that can be used for fraud. Kids are at risk, too. The FBI says parents should monitor their children's online gameplay and ensure that children don't disclose personal information to strangers.

SYNOVUS®