FACEBOOK IS FERTILE GROUND FOR FRAUDSTERS

You know what to expect when you visit Facebook. There are pictures, comments, videos and news stories posted by your friends and family. You'll see their newborn babies, cute puppies, read about their job promotions and cross-country moves, and a lot more. However, sometimes there are unexpected posts that catch your eye.

It may be a Burger King, where the fast-food company is giving away free food. It could be a beautiful photograph of Big Ben in London, with a message from a major airline promising a chance for you to win a trip. What luck!

Of course, you're no dummy. As much as you want to bite, you know scammers are trying to trick you into clicking on a link to their malicious site. If you do, they'll cleverly ask you for your personal information, sometimes including your online bank credentials and Social Security number.

So, what do you do? You avoid the phony post or report it to Facebook.

THE “HOOK”

Many very smart people are falling for Facebook scams because they think the site is well policed and won’t allow fraudsters on board. But scammers know that you are generally wary of online scams. So, they're always upping their game with improved schemes that look like legitimate posts from reputable companies.

Here are three clever Facebook scams that are fooling a lot of people these days. Unfortunately, once a scammer has your personal information, you will often have a really hard time unwinding the mess. Worse, the scammers could infect your computer with spyware.

So, protect yourself. Be on the lookout for these three Facebook scams.

1. FRAUDULENT COMPLIANCE MESSAGES

A fraudulent compliance message uses Facebook’s logo and appears to be a direct message, starting with “Dear Customer.” The message goes on to persuade you into confirming your credentials on a fake website.

Although this particular phishing scam is targeting business pages, there are significant consequences for all Facebook users. If the scam is successful, the hackers gain access to these business pages, which they use to launch additional attacks. These subsequent attacks appear to come from the business itself, rather than the social media platform.

Beyond that, hackers are also gaining detailed information about the personal details of the administrators who are operating these business pages. Oftentimes, these administrators hold management positions at the targeted businesses, which opens the doors for hackers to launch additional scams, such as email phishing attacks.

Note: To avoid being a victim of this phishing scam, look for these three red flags.

1. The link is from ow.ly, not Facebook
2. The notification uses demanding or threatening language
3. The message comes in your notifications section, not messages (notifications typically don't include greetings)
2. BOGUS CUSTOMER SERVICE

Be careful if you post complaints about your bank, credit card company, airline, or any other business that hasn't lived up to your expectations. If you do post a complaint on Facebook, you might get a response from someone pretending to be that company.

Here's how it works: You feel wronged by a company and you share your frustrations on Facebook. "This company is terrible."

Suddenly, you get a response from the company's customer service representative. That's awesome. Or, it would be awesome if it were truly that company's customer service team.

Scammers, unfortunately, set up fake accounts that seem to be from that company. For example, if your complaint is about Bank of America, they might set up an account with an extra letter or symbol, like Bank_of_America.

They read your complaint and take over your conversation, promising to help you. Warning: Their next question will be something like, "What's your ID and password?"

3. FAKE SURVEYS

It's so tempting to answer surveys on Facebook, isn't it? You see a fun-looking post that might say, "Take our survey and get a discount on your next purchase."

It seems innocent. But all a hacker needs to start stealing your personal information is your Facebook user name. They find out a lot about you that way. They know your family and friends, where you live, and maybe even where you work, shop and take vacations.

Or, worse, they'll create a legitimate-looking profile of a well-known company, like Netflix, for example. But, it may have a tell-tale sign, like a strange symbol in the name. If you fall for it, they'll offer a discount. Of course, they'll need you to confirm you are you by asking you to provide your name, account number and financial details.

THE LESSON

Don't fall for these scams, no matter how the scammers get your attention. One red flag to look for is when a company posts a comment in your profile or another company's profile. Legitimate companies aren't going to contact you in the comments. If you feel you have spotted a fraudulent solicitation or phishing scam, don't take the bait or respond. Contact your State's Attorney General's Office and report the incident and give them enough information to double check your suspicions. Also consider reporting the scam to the Federal Trade Commission.