Expert Warns the Public About Social Media Scams

By Denise Richardson

Social media has become a wonderful place to share and interact with friends and others who share your interests, but according to noted Internet fraud expert Chuck Whitlock, social media remains a priority target for scammers searching for people to victimize. With the rise in popularity of the Internet, and social media in particular, you're likely to find scammers through email, Facebook, Twitter, Google Plus, and more.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

A good rule of thumb is not to post anything on one of these social media sites that you wouldn't be comfortable telling a complete stranger, because that's what these scammers are. If they come upon your private information, they can use it for money scams, identity theft, and hacking attacks.

Facebook Friend Fraud

Chuck Whitlock has pointed out that identity theft and identity fraud are still prevalent on social media sites today. One common example on Facebook is the scheme known as friend fraud, which occurs when a stranger illegally gains access to your social media account and sends messages to the friends in your contact list. By pretending to be you, this imposter can request money from your friends as a result of a fake emergency that left you without any money for transportation, for example. Because of people's generosity and warm feelings toward you, they might send the money to a con artist. Be careful about telling others your login information, check your social media frequently, and be sure that if this happens to one of your friends, you call them first to make sure it's really them.

Twitter Hijack

If you've ever had an awkward night out or been part of a group that gossips, you know that having these private moments made public is incredibly embarrassing. Apparently, scammers recognize this too. By Tweeting or messaging you that an embarrassing picture or rumor has been made about you, from someone you know, scammers are hoping you'll click the link to find out what's going on. When you do it, scammers can hijack your account and send the same link to everyone in your contact list. This link often contains malware or malicious code that will harm the computer with viruses, which is why you should check with the person who supposedly sent the link. If it's from someone you don't even know, you should simply ignore it. (See an earlier blog for help recovering from a hacked Twitter account)
Google Gift Phishing

Who wants a free gift? The answer is, everybody does. How cool would it be to receive free clothes or beverages or electronics for absolutely no reason? Chuck Whitlock says, scammers use this method as a favorite phishing scam when accessing contact information out of victims through manipulative and deceitful strategies. He adds, "Just remember that anytime someone offers you free gifts in exchange for your personal information, it's exactly how it seems: too good to be true." Phishing scammers can offer free brand name products and logos to obtain your data, which is often sold to identity thieves, hackers, or advertisers. It's always wise to ignore anything that seems too good to be true. Always check the brand's official site to confirm the authenticity of any tempting offers.

About Chuck Whitlock: Thanks to his former career as a television investigative reporter, Chuck Whitlock has accumulated a great deal of experience dealing with fraud. He uses his previous experience to give keynote speeches and conduct workshops on what types of fraud exist, such as cybercrime, business fraud, scams against seniors, medical fraud, and many more. With a commitment to fighting scams and educating the public, Whitlock has authored books containing his extensive knowledge on the subject of white-collar fraud, including Easy Money, MediScams, and Scam School.

To find additional tips and helpful anti-fraud awareness information, follow these links to read more about today's latest scams and cyber-security threats.
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS