OMG is this you in the video?... and other social media scams

Posted At : January 29, 2013 3:43 PM | Posted By : Admin
Related Categories: Social Media, Security

How many friends do you have on Facebook? Can you really say that you know more than 20 percent of them well? Social media is an incredible tool for connecting people despite physical distance and other real life barriers—but can you fully trust all the communications you receive from these seemingly legitimate online personas?

The interconnected nature of social media is also its risk. Social media sites are an attractive playground for people trying to hawk pyramid schemes and scammers are quick to abuse your private information, whether to make money or for malicious reasons. Facebook recently disclosed that it has found 14 million accounts churning out spam and scams. Fake profiles are also flourishing on Twitter, where they are sold as followers or used for shady tricks.

Scams almost always come from social media "friends" so it is important to be aware of the lurking dangers.

It sounds too good—or too terrible

Scammers will often try to track your activities and target your weak spot. Think twice before you click on a sensational link or respond to an emotional request, even if it does seem to come from a "friend." Keep an eye out for these common scams:

Dubious URLs

- **"Is this you in this video?"** Usually this type of Twitter direct message comes with a short link that hides the real URL—which transfers malicious software onto your computer and hacks into your account.
- **"Justin Bieber did WHAT?"** This is an example of Facebook comment-jacking. A bait-link takes you to a fake captcha test and posts your text as a comment to the fake story on your Facebook wall.

Phishing attempts

- **"Get a free gift card."** The free gift scam takes on many forms and there is always one running at any given time. The objective is to steal your information and sign you up for expensive services.
- **"Confirm your email account."** Password confirmation e-mails may appear to be legitimate, but they rarely are. Always go directly to Facebook, Twitter or LinkedIn to update your personal information.

Application scams

- **"See who viewed your profile."** Another empty promise. This one gets you to share your details via a fraudulent survey application. You also need to allow an app to access your profile—generally a bad idea.
- **"Must-see man-eating snake video."** Outrageous? Sure, but you'll never actually get to see the video. This "Play" button is disguised to lead to survey applications that earn commission for the scammer—and bait your friends.
- **Rogue apps.**Designed by cyber-criminals, these Facebook applications take the

form of games and quizzes. Not all of them infect your computer, but they do pass on all of your personal data (including that of your friends) to advertisers without your knowledge.

Scams cannot always be avoided, but taking reasonable precautions can help minimize your risk online. Follow the advice below and visit social networking sites that use https:// in the URL rather than http://. This secured protocol will encrypt your online connection for added security.

- **Set your profiles to "private"**
  Unless you adjust your privacy settings, the details you post on social networking sites are visible to the public. Note that your contacts still have the option to share your content with their connections. Also take care when integrating your social networking accounts. You may have privacy on Facebook, but be exposed on Twitter.

- **Keep personal details offline**
  Besides the fact that letting your guard down may help scammers take advantage of you, it is also important to know that social networking sites make their money from collecting and selling data. Privacy settings protect you from other members of the network, but the data you reveal on sites such as Facebook belongs to the owners of the service.

- **Don't make others vulnerable**
  Do you really want tell the world where your child goes to school? Consider how others feel about you posting their information online. Too much detail, such as someone's date of birth, can make things easy for identity thieves.

- **Change passwords regularly**
  Make changing your passwords regularly a matter of routine. This will keep you one step ahead of scam tricks and help you protect your accounts. Furthermore, don't use the same password for every account! This puts all your accounts at risk, should one be hacked.

- **Associate with people you trust**
  People are not always who they say they are, especially online. It may be wise to consider connecting only with those you trust not to misuse your information. Organize these users in groups or create separate profiles for different purposes.

- **Go easy on IM**
  The instant messaging tools offered by many social networks are some of the most insecure ways to communicate online. Keep the conversation light-hearted or use an encrypted client, such as Pidgin, to ensure a secure chat.

- **Think before you click**
  Many links shared via social media lead to no good, so when in doubt, double check with your the sender or contact. This way they will also be aware if they have unknowingly shared scam content and have the chance to remove it if need be.

Online, as in real life, it can take time to build a trusted social or professional image—yet a scammer only needs a few seconds to destroy your good reputation. Many social media profiles are connected to your real name and if you unwittingly expose your real friends to online scams, your personal credibility is at risk. As with many dangers lurking in our modern world, it helps to act responsibly.