FAKE IDENTITIES ON SOCIAL MEDIA

SOURCE: https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

How Social Media Networks Facilitate Identity Theft and Fraud

Article by:

Kent Lewis

EO Portland

Recent research reveals that identity theft affects millions of people a year, costing victims countless hours and money in identity recovery and repair. What causes this pattern of online theft and fraud? It's a combination of factors: a lack of consumer knowledge regarding protecting your identity online; growing comfort with, and trust in, social platform providers; the need for social platforms to generate revenue; and a lack of standards or policing of these standards. Although this issue is not yet in the mainstream consciousness, it likely will be sooner rather than later.

Fueling the Fire

Social media sites generate revenue with targeted advertising, based on personal information. As such, they encourage registered users to provide as much information as possible. With limited government oversight, industry standards or incentives to educate users on security, privacy and identity protection, users are exposed to identity theft and fraud. Additionally, these platforms have a ton of confidential user information, and are likely vulnerable to outside (or inside) attack. On the marketing front, Google recently patented an algorithm to rate individual's influence within social media. Once publicized, it will likely encourage greater participation by active users in order to boost their influence score.

Crimes of Opportunity

With the increased global use of social media, there are more opportunities than ever before to steal identities or perpetrate fraud online. For example, status updates posted on Twitter, Facebook and many other social media sites can be used by criminals. If you post that you're out of town on vacation, you've opened yourself up for burglary. If you mention that you're away on business for a weekend, you may leave your family open to assault or robbery. When it comes to stalking or stealing an identity, use of photo- and video-sharing sites like Flickr and YouTube provide deeper insights into you, your family and friends, your house, favorite hobbies and interests.

That being said, social networking sites have the greatest potential for abuse. While everyone knows they should never share their social security number and driver's license, many social networking sites ask for, if not require, similar sensitive information that can be used against you in a variety of malicious ways. The following profile elements can be used to steal or misappropriate your identity:

- **Full name (particularly your middle name)**
- **Date of birth (often required)**
- **Home town**
- **Relationship status**
- **School locations and graduation dates**
- **Pet names**
- **Other affiliations, interests and hobbies**

<u>Horror Stories</u>

You're probably asking why sharing your pet's name, high school graduation date and membership to an organization with the public is a potentially dangerous move. There are a variety of reasons why you should keep personal information confidential, or at least closely managed. Below are just a few examples of how this information can be used to compromise your identity:

- **Phishing attempts using this information can be used to gain trust in order to obtain non-public information through online conversations. A Portland, Oregon, USA, company was recently attacked with false Better Business Bureau complaints in order to obtain additional information about the company and its employees.**
- **GPS-enabled phones sharing your location can reveal sensitive information like your home address, work address and the places you visit.**
- **Ninety-five percent of Facebook profiles have at least one application, many of which are not reviewed and can be used for malicious and criminal purposes.**
- **False profiles can be used to fuel resume fraud or defamation of character. A Canadian reporter recently was defamed via a false profile that included misleading posts, poorly considered group memberships and intellectually inconsistent political positions.**
- **An American soldier abroad in Iraq discovered his bank account was repeatedly being accessed online and drained. A security expert was able to**

replicate access with nothing more than his name, e-mail and Facebook profile.

Best Practices

Before you jump online and cancel all of your social media accounts, consider that there are ways to be smart about what you share and who you share it with. By following the best practices outlined below, you can enjoy the benefits of social media without making yourself a target for criminals.

- **Never, ever give out your social security number or driver's license numbers.**
- **Consider unique user names and passwords for each profile.**
- **Vary your passwords and change them regularly.**
- **Don't give out your username and password to third parties (even if it helps you connect to others and build your network).**
- **Assuming you plan to be active in social media, minimize the use of personal information on your profiles that may be used for password verification or phishing attacks.**
- **Avoid listing the following information publicly: date of birth, hometown, home address, year of high school or college graduation, primary e-mail address.**
- **Only invite people to your network that you know or have met, as opposed to friends of friends and strangers.**
- **For password security verification questions, us a password for all answers (rather than the answer to the specific question, like "What is your mother's maiden name?").**
- **When age-shifting to protect your real birthday, keep the date close; otherwise, you may expose yourself to age discrimination.**
- **Watch where you post and what you say, as it can be used against you later.**
- **Google yourself regularly and monitor your credit using the free annual report or monthly monitoring services.**

Consumers need to be educated on the proper use of social media as it relates to protecting privacy and security. Social networks need to also understand the impact of not addressing security and privacy issues. If the information becomes corrupted, it not only casts doubt on the social network, but on your real-life personality, as well.