Volume #4 - Issue #173
August 17th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Social Media Hacking

Social Network Hacking usually takes one of two forms, either your site was been hacked and someone is posting items on your site or sending messages to your friends, or another site has been created to look like yours. (Usually to post damaging information, usually fake, about you.) When people talk about hacking and social networks, they're not referring to the common definition of hacking, which is using malicious code or backdoors in computer networks to damage systems or steal proprietary

information. Hacking into social networks requires very little technical skill. It's much more of a psychological game — using information on personal profiles to win a complete stranger's trust.
It is often difficult to realize that your social media account has been hacked, so it is a good idea to watch for the following signs that something is going on with your account:

- You observe "likes" and "follows" that you had nothing to do with
- You have your status updated, although you have not done anything
- There is an increased amount of ads on your page
- You are having issues logging in
- Private messages are posted on your behalf
- Spam posts are posted on your behalf
- You have new friends that you do not recall adding
- Others inform you of sharing malicious content on your wall

If you notice some of these signs, you had better check it out immediately. It is more than likely that your account has been hacked and you need to act promptly and effectively. The first thing to do is change your password and get control back of your account. Then try and access the damage done and whether or not you should delete your site and create a new one. (Definitely a last resort step since you will lose all your friends, followers or contacts.)

Why are Social Media Accounts Hacked?
For the LOLz.
Why social media accounts are hacked varies. For famous accounts, one of the biggest reasons is not one you'd expect: For the LOLz. For fun. Todd McFarlane, the comic book artist from above, is Canadian. When his account was hacked the person in control of his account tweeted out lyrics from fellow Canadian Drake. There wasn't much point to it. Little harm could be found besides the fact that Todd no longer followed fellow frequent collaborator Greg Capullo. As far as anyone can tell, it was for fun.

For forced shares

The second reason that social media accounts are hacked is to force shares. A guy on Facebook had shared and tagged many friends in a link to a website full of nude women, the only thing is . . . this guy was gay! It didn't take any special computer knowledge to know that he was hacked. These types of hacks can be more harmful than you think. Let's say that one of your friends isn't a gay man and wants to see these naked women. This person clicks on the link and is sent to a website that's devoid of naked ladies but full of trojan horses, phishing pages and all forms of malware. It all starts from one click on a piece of content that seems enticing.

For forced follows

The third reason that your social media account could be hacked is for forced follows of other accounts. This can involve your account being hacked as part of a wider plan to hack accounts and get them to follow a specific account. This account that you've been forced to follow, that may have a fake brand name, will then be used to spread malware like in the example above. Worst of all, you may never know that there's any problem at all. One day you'll see a post from someone in your Timeline or Newsfeed. It will look *kinda sorta* like a brand you actually follow, only it's not.

For information

The last reason someone will hack your social media is to steal information from you. This can be your password itself so that they can steal it and use it to try and sign into accounts you have with banks and online retailers. This can be information about your place of work. This can be a crazy stalker trying to find out what your plans are for Friday night.

How Can You Protect Yourself?

To understand how to protect yourself, Let's look at some common hacking methods used on social media accounts and explain a method of defense for each.

Brute force hacks
This is when a hacker gets hold of one piece of information, your email as an example, and then uses a tool to guess your password. This can be as simple as a password recovery tool altered for criminal purposes.
Protect yourself: You can protect your social media accounts from this by having complex passwords. Make sure they're not common words. Mix upper and lower case and include at least 12 characters. I use 15 now. These are nearly impossible to crack via brute force hacks.

Man in the middle hacks
This is when hackers insert themselves between the conversation your computer is having with a server or other computer. This is most commonly done at public WiFi hotspots, but it can, in theory, be done anywhere. You may never know that one of these hacks has been carried out, as it can be impossible to detect it happening.
Protect yourself: With the hacker inserting themselves between you and who you're trying to talk to, simply encrypt your information. The easiest way to do this, and most flexible, is by choosing a well ranked and regarded VPN for your particular goals.
These tools will encrypt your traffic from your computer to the server or computer you're speaking to. Anyone trying a man in the middle attack will get nothing but encrypted gibberish which they can not read or decode.

Phishing Pages
These are pages which look legitimate in some way but are actually only built to steal the information you freely give them. These messages are often found in your email but they can spread via social media, as well. The basic premise is that you have to enter your login details for a specific website, like your bank, for some 'urgent' reason.
Protect yourself: Your best bet for defending yourself against these types of hacks is to trust no one and nothing. Enter the URL of the business claiming it needs your information yourself to make sure it's the right website. Contact the administration before you follow the message. Do not be gullible!

Trojan Horses
This is when you authorize a download onto your computer for something you think you want but you don't want it at all. When it comes to hacking social media, this is usually a keylogger that records your keystrokes.
Protect yourself: Know where you're downloading from! There are dozens of websites built just for this; they're called 'warez' websites. Going to the source for your downloads should always be priority number one. Second, a good piece of antivirus software, with a strong firewall, will take care of 99% of the rest.

So you mostly play that games on Facebook and chat with your mom or friends now and again. While it might be nothing but fun and games for you, it can be serious business for a hacker who gets into your account and gets hold of the right information.

There are real world consequences that you can face if you don't better secure your social media accounts now. Start with better passwords, add some encryption, and don't be gullible!

Thank you for subscribing to our email!