HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
WEEKLY

Volume #4 - Issue #145
February 2nd, 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.

Secure Your Facebook

Some time back, a Facebook account was irrelevant to hackers. There was no reason to hack anyone's account since there was no reason for hacking an account in the first place. Ever since it has grown to billions of users, Facebook contains enough data for hackers to use for either monetary gain or blackmail. A celebrity's account, for example, can be hacked in order for a person to advertise a page or brand. The hacker can also post embarrassing or discriminating posts that will leave the celeb's fans furious. Your account is also prone to hacking even if you aren't a celebrity. You obviously have to protect your Facebook account from malicious hackers.

It is not that hard to protect your account. Just follow these guidelines, and you'll be good to go:

1) AVOID SAVING PASSWORDS ON PUBLIC DEVICES

Cybercafés are awesome alternatives when you do not have any data on your device. They are also reserves for passwords since most people just click on 'yes' on the save password dialog box.

They do so because of the rush they face during browsing. This might also happen to you. If you do not have a device to browse the web, never save your passwords on a device you have no control over.

The password will remain there, and someone will definitely log into your account without any hustle.

2) ALWAYS LOG OUT ON OTHER DEVICES

Not saving your password is not the only way to prevent hacking on public devices. Leaving your account logged in also paves the way for hackers to take control of your account.

Even if you close the browser after a session, Facebook will recognize the session as continuous for a while. If a person comes in just right after you, he should have access to your account.

You have to ensure that you have logged out and that neither your number nor email address is displayed in the authentication tabs. You'll otherwise find some nasty posts up on your wall if the guy is aiming to destroy you.

3) OPT FOR TWO-WAY VERIFICATION

This feature sends an authentication message to your phone every time you or a hacker tries to log in to your account. You can use this through third-party software or Facebook's verification mechanism.

When logging in, you receive a unique code that will enable you to access Facebook in that session only. Once the session has ended, you will need to receive another authentication message to access your account once more.

4) CLEAN UP YOUR BROWSER
It is always advisable to clean up your browser every once in awhile…. Most phishing and virus activities are found in porn and torrent sites. If you are a frequent visitor (not judging), always clear your data before someone gains access to your authentication details.
If that seems like much of a hustle, just download an adware removal tool to take care of that for you. The next person trying to hack you will not find the ones and zeros he/she is phishing for.

5) PROTECT YOURSELF FROM SPYWARE AND MALWARE
The hacking problems are not only web-based. A person can hack your browser through malicious software you may have unknowingly installed on your computer. Some of this software could also spam some pop-up ads onto your screen or browser. You can avoid this by using malware, adware, and spyware removers.

If your Facebook account has already been hacked, don't panic. Next week's newsletter will discuss your options for recovering a hacked Facebook account.

This Week's Cyber Alerts:

Alert Issued 2/1/18 Millions of Fortune 500 Email Credentials Found on the Dark Web

Alert Issued 1/31/18 If You use Firefox, You need to Update it Right Now

Alert Issued 1/29/18 ATM Jackpotting Hacks Reach the US

Alert Issued 1/29/18 Millions of PCs Targeted by Cryptocurrency-Mining Malware

Alert Issued 1/27/18 Windows 10 Can Now Show You the Data it's Sending Back to Microsoft

Alert Issued 1/24/18: Apple Text Bomb can Crash iPhones with a Single Message

Alert Issued 1/22/18: OnePlus Confirms up to 40,000 Customers were Impacted by Credit Card Hack

Alert Issued 1/21/18: Kansas Republican Exposed 945 Social Security Numbers

Thank you for subscribing to our email and I hope the information we have shared will make your online life a little easier.

Home Cyber Defense Weekly

is a service of

House of File Technologies