I've Been Hacked!!!

More and more today we see our friends on Facebook or Instagram posting "I've been hacked. Don't accept messages, or pictures or… " whatever from them.

Or, you did a little shopping on Amazon or Google Play or your favourite Web site and now you're getting all kinds of wonderful offers from places that look just like Amizon, or Wallymart or Googley.

The apparent misspellings of names is deliberate and you'll see why a bit later on.

How does my Facebook get 'hacked':

Easily. You never change your password, and the password you have is so simple a kindergartner could guess it, and you play every game available and follow hundreds of newsfeeds or channels.

Most of the channels and games on Facebook are legitimate and Facebook does take precautions to ensure advertisers and game/newsfeed providers are legitimate and not trying to Phish your account. Despite the security breach that gave out thousands of users passwords to their accounts, Facebook generally has pretty good security on their servers and internal networks.

If you're a regular Facebook user, change your password regularly and make it complex. A mix of upper and lower case, with a number or symbol or two in the password make it millions of time more difficult to guess or use software to crack it. NEVER USE YOUR BIRTHDATE, pet's or kid's names or things you've probably posted all over Facebook that anyone can easily find.

DON'T accept every friend request that comes across your screen and the same goes for game play requests. I may be mean and miserly but I won't give you points in Farmville, or Coins in Vegas Slots or whatever you ask me for as your 'friend'. I may chat with you in Messenger, or share texts or pictures by posting, but I won't let Messenger or game requests introduce a worm or virus or other nasties into my computer.

And you shouldn't either.

Ellen is giving away a car and a billion dollars:

Really… wow. I want in on that! NOT!!!

This is the Googley, Amizon, Wallymart scams you see all the time, and hundreds of people fall for it daily.

REALLY REALLY REALLY read the source of the advertisement, email or message. I've seen Ellen DeGeneres spelled about 25 different ways this week alone, in one of the *Ellen is giving away a car and a billion dollars:* scams.

Disreputable groups want you to login to the website promoting the giveaway so they can get your Facebook user name, and access your 'friends' lists so they can spam them too. Once they have a list of susceptible people they try to force their way into your computer and use your computer to spam your friends or take control of your computer, maybe placing Ransomware on the computer so you can't use it unless you pay them some money, or a myriad of other nefarious things.

Some of the local organizations giving away a fruit basket or dinner for two or such are probably completely legitimate, but you can bet your bottom dollar (and you may be doing so) that the Ellen and Oprah and Dwayne Johnson 'giveaways' are scams.

Practise Safe Computing:

Since we've started doing some computer service in this area we find more and more people are NOT using any kind of decent anti-virus (AV) or anti-malware (AM) software to protect their computers. Think of AV or AM software as insurance for your computer.

You have insurance on your car, and hopefully on your home and contents. For many people the computer is a VERY valuable asset, storing memories in the form of pictures, and important documents (tax returns, bank information, health records) and a tool we use daily to look up information or keep track of appointments and news.

If you're using a free AV or AM software you get just what you paid for. NOTHING. They may do a basic job but provide little protection against Phishing software, hacking or penetration attacks and all but the simplest tools hackers use to extort you or take control of your computer.

Backup Backup and Backup:

Ransomware is on the rise all over North America, even in our little corner of the world. Simpy put Ransomware is a form of malware that locks you out of your computer and won't let you access or open your

files, pictures etc. unless you pay the crooks a sum of money, most often in the form of cryptocurrency or bitcoin.

If you get hit by Ransomware, which will usually happen ONLY if you do not have good AV or AM software, or you are REALLY stupid and open a file/attachment in spite of your AV or AM software warning you the file is infected with something nasty, DO NOT PAY THE RANSOM.

Just say goodbye to the files, pictures or documents that are infected. In my experience the crooks will not give you're a decryption key or disinfect your files for you. They just take your money and laugh all the way to the bank.

The best protection is DAILY backups of your important documents, pictures and data. While Windows has built in backup software, I find it difficult to control and manage easily, so I really recommend purchasing a simple backup program and an external USB harddrive to backup your files and store them safely outside your normal system harddrives.

Daily, or really nightly backups, will allow you to clear out the Ransomware (or have a professional do it and make sure you're disinfected) and then restore your files, pictures and precious documents.

You may lose what you did between last night's backup and the point of infection today, but at least you'll have back all the others.

Conclusion:

Be smart. If it sounds too good to be true it probably is. As nice as Ellen is she isn't giving you a billion dollars or new car just for liking her Web page.

Purchase a good AV or AM software package and keep it updated.

Purchase a simple to use backup software and external USB drive to store your backups.

With the Christmas season approaching and many of us searching for bargains or actually shopping on the net, the risk of being hacked or infected increases as scammers and crooks take advantage of our increased use.

Suggested Software and Protection Items:

AntiVirus or AntiMalware:

ESET	www.eset.com This is my favourite package. Good pricing, excellent protection
Total AV	https://www.totalav.com/
Bit Defender	https://www.bitdefender.com

Backup Software:

SyncBack Pro	https://www.2brightsparks.com/syncback/syncback-hub.html
EaseUS	https://www.easeus.com/backup-software/personal.html
Acronis True Image	https://www.acronis.com This is my personal favourite because it can do file backups like any backup software but it also can image an entire PC drive. It's bit more complex that the other two but worth learning. And of course your can always call us if you need a little help or call the vendor as their support is great.

External USB Drives for Backups:

You can find tons of these drives on Amazon.ca. A one TB drive will run about 65.00, and a two TB drive will run about 90:00. One TB should suffice easily for most average users to backup photos, emails, documents.