Internet Threats

LifeInNaples • July 31, 2014

It is often thought that if you have a Mac, you are safe from all bad things that can happen to PC users. Although the majority of viruses written are executable files (.exe files) that a Mac cannot open, todays attacks do not attack the hardware as much as they attack the person using it. Whether you are Mac or PC, iOS or Android, there are threats that need to be taken seriously that can affect any user of any device. I will review the five most common internet risks you are likely to encounter.

1. Phishing

Most of our digital life takes place through email. We make purchases, sell items, reset passwords and receive bills and account statements. Email is easy to send yet also easy to fake.

When a hacker sends an email that seems legitimate but is actually a trick to cause you to respond, it is called phishing. Phishing basically falls into two categories: those that get you to click on a link that installs malware, and those that manage to take cash from you or steal passwords.

Some of the most common methods are:

- A great financial opportunity from overseas, usually to assist a deposed official of a foreign government.
- A problem with your bank account, credit card, eBay, Apple or Amazon account that ask you to confirm your account information.
- A false invoice or statement that needs review and often installs malware on your system.
- A message from a friend that is in broken English or offering a product,

that does not sound like their writing and often has a link to click.
- An urgent plea from a relative or friend that suddenly needs money for travel, repairs or bail. This person will often not be able to call you, yet they can send an email!

How to Protect yourself against Phishing:

Use a major email service that filters spam and malware. Gmail and iCloud do this, as well as most major email services. Use common sense: don’t open unexpected files even if you know the sender. Hover over a link in an email, most will show you the actual site you are being directed to which is not what it appears to be. Type the name directly into a browser window to get the actual site. Never respond to unsolicited financial or business offers through email.

2. Watering Hole or Search Scams

These are websites set up to appear in standard searches and they appear to be legitimate sites. They often are most used in searches for repair and how-to guides, where there are many results from a variety of small sites. The hacker will hide malware on these sites, so when you think you are downloading a PDF on toaster repair you are actually installing malware on your machine.

How to Protect yourself against Search Scams:

Never assume that because a site was in a search engine listing it is safe, even popular sites like Google and Bing can be fooled into listing a scam site. Keep Java disabled until needed, and update your Flash player when available. Think twice before downloading software from vendors you have not heard of.

3. Online Commerce Fraud

Amazon lists their independent Marketplace vendors along with their listings, yet often items are less than full quality, and you can return through Amazon if there is a problem. Be cautious using Craigslist if the seller asks for payment in gift or prepaid cards rather than a check. Online sites may sell counterfeit or stolen goods that are not as advertised. Some stores and auctions never deliver goods, and they are gone when you try to contact them.

When using eBay, some buyers may claim the item was damaged or not as described, which can affect your seller account.

How to Protect yourself against Online Commerce Fraud:

Stick with the bigger sites, they often have buyer protection. If you pay with credit cards or PayPal you also have protection, just keep good records of all transactions in case you need them. If you are selling an item, wait until payment clears before you deliver or ship the item. If selling, photograph and document what you are shipping.

4. Account Hijacking

This is still a rare occurrence: when a hacker takes over one of your online accounts. If an attacker can get into your accounts in the right order, they could effectively take control of your digital life. This often occurs when a password is guessed by the hacker or he obtains it through a website security breach, or through malware installed on your system. Once in, they will send out phishing attempts from your account or may target your digital life and try to access accounts you have online.

How to Protect yourself against Account Hijacking:

Use a strong, unique password for every web site and account. Apps and software such as 1Password (agilebits.com) and LastPass (lastpass.com) can offer simple to use password management tools. If you have any doubts as to the authenticity of a site or are worried about a breach, change that password immediately.

5. Social Media Phishing

Social media scams are usually tied to an account hijacking or the compromise of an account by a friend or family member. A common result is that you receive unusual messages from people that are people that you know. There is also the ‘Catfish’ attack, where a fake online identity is created to perpetrate a hoax or fraud. The story last year of Notre Dame football star Manti Te’o and his imaginary girlfriend was a ‘Catfish’ scam.

How to Protect yourself against Social Media Phishing:

Use common sense and use caution with the links you click on and which friends you can trust. Follow the other tips in this article for avoiding phishing and other attacks.

Jeff Bohr
Naples Mac Help
239.595.0482 | jeff@naplesmachelp.com