More Security Alerts!

Spot bad Emails and Websites | Tech Tips Video by PcCG

Subscribe via Itunes [1] | Subscribe via RSS [1]

Lately we've been hearing in the news a lot about Chinese hacks on American companies and government entities. Underground groups have also been hard at work hacking away and obtaining a lot of private information. ***There have been a couple major sucesses lately by the hackers to obain information from LivingSocial and Drupal.org.*** It's happened to other major companies before as well, and will again. It sucks, but that's just the age we live in.

It is impossible for any company to guarantee a 100% secure system that is linked to the internet; and these systems must be linked to the internet in order to allow us to interact with them by doing things such as making a credit card purchase.

We live in an age of cyber-threats and the attacks are only going to continue to grow in magnitude and complexity.

For a home user, what does this mean?

It means simply a little bit of learning, understanding in concept how these things happen, and doing your best to be on guard, while not paranoid for cyber attacks on you.

Home users and computers are almost never the target of "hackers" trying to break into your computer and steal your personal information. There is too little payoff, frankly nobody cares about you (or I) that much. There are billions of devices connected to the internet, therefore being singled out isn't likely or practice. There are however blanket schemes designed to just "toss a net out" and see whom they catch; and you might get caught in this net if you are fooled.

The primary methods of attacks are

- Scams
    - Email and Internet Phishing (Trying to trick you into submitting sensitive info to the bad guys)
    - Fake Downloads (Downloads that pretend to be Adobe Flash player, but really aren't)
- Viruses
    - Trojans (programs that can do a number of things including recording your keystrokes and transmit them to the bad guys)
    - Scareware (things that try to scare you into acting, submitting your information to the bad guys, such as the infamous FBI warning some people have got that isn't really from the FBI)
- Security Breaches
    - Information stolen from a websites database that can then be used to access other accounts.

What can be done by you? A simple few things might go a long way.

- Education
    - Doing things like reading this article (and a few others on this and other sites) will go a long way. If you spend just 15 minutes a week checking out a few of the articles here or else ware for the next few weeks you'll be well armed to avoid many scams!
- Keep a good Antivirus up to date
    - Can't stress this one enough. McAfee and Windows Security Essentials in my opinion don't make the cut. My preference is Norton Internet Security, but several others are good as well.
- Avoid "Optimization" programs
    - Most of the time the freebees are gimmicks to get you to download the software, they run a scan, then tell you that you need to purchase the software to fix 10 million errors or your computer will burst into flames. Rarely do these programs offer any significant benefit and frequently they actually create more problems. Some of them are fraudulent as well!
- Watch what you download
    - This isn't to say don't download anything or run around paranoid all day, but you must use some caution as to what you are downloading and where you are downloading it from. If you go to watch a video on some unknown website … say NicksVids.com and it tell you that you need to download some unknown video player in order to watch the video, that should set off 2 alarms! If however you are at Netflix.com and it's telling you to download Silverlight from Microsoft, that's fine, you can trust both the site and the download.
- Manage your passwords
    - Security experts recommend different passwords for every site. That realistically isn't particle. Others recommend a password manager, which I'm not a proponent of. Instead a simple balance of practicality and security might work best
    - Keep 2 sets of passwords. One for "Critical" items (Bank accounts and Investments, Credit Cards and Email), and a second set of passwords for less critical items such as facebook, ebay etc.
    - CHANGE these passwords AT LEAST once a year (or even once every 6 months). Even a simple modification, such as changing a 1 to a ! or a 5 to a $ work. Don't just add 1 or 2 to the end of the password.
- Education
    - No it wasn't a typo. It was first and last on the list because it's so very important. You don't need to become a security expert, but knowing at last a few simple concepts like items noted in this and other tech tip posts goes a long way!

So what are you waiting for? Go on and change your passwords, make sure you have a good antivirus and enjoy a well oiled computer system!

Tech Tips [2]
Tech Tips Articles [3]
Tech Tips Podcasts [4]

Source URL:https://www.pccomputerguy.com/tech-tips-podcast-more-security-alerts

Links
[1] http://pccomputerguy.com/podcast/feed.xml [2] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [3] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles [4] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Podcasts