How Do You Know If You Have Been Hacked?

Whether or not you have been hacked depends on your definition of “hacked.” In the broadest sense, it means that some of your sensitive information has been compromised … that a hacker or identity thief has gained access to some of your data or network resources such as camera or printer.

If this is your definition of “hacked” I imagine nearly everyone reading this article has been hacked.

In just a single incidence of mega-hacking, hackers gained root level access to over 19 servers at JP Morgan Chase, compromising the information of approximately 76-83 million households and 7 million businesses for weeks! As of 2009, only about 110 million US households had bank accounts, so about ¾ of US households were affected.

Chase is not some hayseed bank. Chase underpins the global banking infrastructure. Worse than the fact that some of your information was almost certainly comprised in the Chase hack or in one of any number of large hacks and is now in the hands of black hat hackers, is that that the hacker or group of hackers had plenty of time to learn everything they wanted to know about the banking industry’s IT security practices.

An increase of fraud activity has not been detected yet, but we do know that the hacker(s) carefully examined all of the network security software, so they will be very well prepared for future attacks and will be much harder to detect. Regardless of whether or not you consider an event like this to be “you being hacked” or not, it still affects you and your OPSEC (operational security).

How Do You Know It?

You might consider the definition of hacked to be much narrower, such as having sensitive data compromised, if that data resides in memory owned by you. If this is your definition of being hacked, there are signs.

But signs for the average user that you may have been hacked …

- You notice in security logs that devices other than your own have accessed your accounts.
- Passwords change or stop working. Hackers often change them or try too many wrong passwords, causing accounts to lock for a period of time in an attempt to prevent dictionary attacks.
- Internet searches are redirected. You can monitor this with browser plugins for http and https.
- You find files containing ASCII art “tags” or other hacker or hacker organization signatures. Believe it or not, many old school hackers were so sure of themselves (and sometimes narcissistic) that they would “sign their work” as if they were an artist or craftsman … or serial killer. Some never stopped and it still occasionally inspires some aspiring, self-taught hackers who imitate the practice.
- You notice new files or changes to existing files that were not made by you or were made at odd times such as while you are sleeping. You can see this in the detailed view of your file structure.
- You notice deleted files or files in your recycle bin that you did not delete. You may also notice when the items were sent to your recycle bin.
- Software or task manager stops working or encounters errors because of corrupted files, viruses or because changes have been made to your program files, firewall, antivirus antimalware or other security settings or these types of programs are disabled. You may notice

processes you cannot identify running in task manager or you may not be able to run or restart your registry editor or task manager.

- You notice new software, programs, icons, shortcuts or toolbars that you did not install or software starts installing even though you did not initiate the installation.
- Drives are shared that should not be.
- New network connections that you did not create.
- You notice unusual account activity or other signs of identity fraud such as purchases you did not make, you receive requests for payment for purchases you did not make, you spot unusual issues on your credit report.
- You learn that someone has been using your social media, email or other accounts. You may hear from contacts that you have been hacked or that someone is using your identity to spam them or email malware.
- You see your mouse moving around the screen, opening things and changing settings, but you are not moving your mouse. This is a clear sign someone has installed terminal emulation software and captured your computer.
- Your antivirus software detects certain types of malware used by hackers to gain control of your device or computer. Most antivirus programs keep knowledge bases of which malware and viruses to help you make this determination.
- You see fake virus or malware messages. Do not click on them. They will launch programs that may damage your computer.
- Your antimalware and/or antivirus software has been disabled.
- Your computer running slow and decreased download and/or upload speeds are also common symptoms.
- You notice unusual TCP or UDP port activity. You can monitor this in utilities such as FPort and TCP View.

Avoid and Prevent Hackers

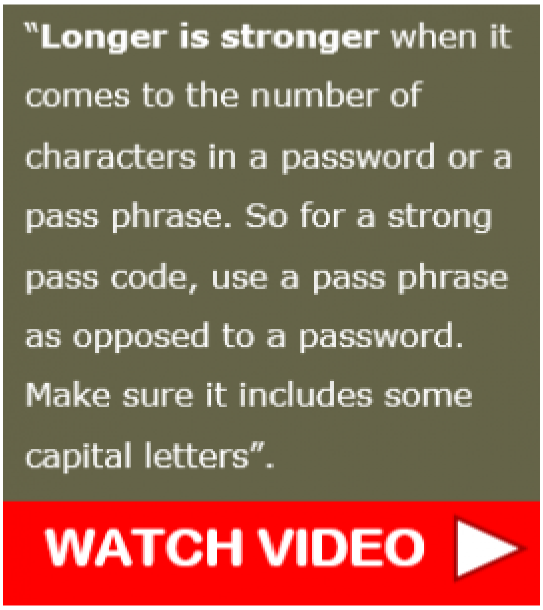
Do not let the talking heads in the media, Hollywood, big business or big government convince you that privacy is unobtainable. I have read some articles by low-level IT people who claim that hacking cellphones is “trivially easy.” I suppose it can be, as long as the target uses a standard phone from a major US cell provider and do not root it or run any security, encryption or VPN software.

People who buy or sell the lie that privacy no longer exists either have a vested interest in you not protecting your sensitive data or they are slaves to convenience. Patriots paid for your rights with blood sweat and treasure, and those rights include privacy.

Do not buy into anti-privacy rhetoric. 50% of all US sales are generated by direct marketing. That is a lot of money. If you believe that the anti-privacy crowd values the truth or your rights above their share of that money, what I write here is probably not for you. If you truly trust bankers, corporations and the liberal media to value your privacy above your money, you should probably stop reading this right now and follow your shepherd.

Feel free to bleat and “bah” your way back to the feed lot … maybe today he will choose to take you to feed again … then again, his freezer might be running low.

To avoid and prevent hackers, create a bulletproof OPSEC SOP, (operations security, standard operating procedure) invest the time to commit yourself to importance of sticking to it, implement it and diligently enforce it to the letter.



"**Longer is stronger** when it comes to the number of characters in a password or a pass phrase. So for a strong pass code, use a pass phrase as opposed to a password. Make sure it includes some capital letters".

WATCH VIDEO

This is not something that you are going to be able to learn to do reading 600-1000 words, but a course manual designed to do those very things.

Make sure you keep all of your software up to date and make backups and recovery drives.

Do not run executable files that you do not trust and be cautious downloading free content and programs.

Probably the single most overlooked tool to protect your data is encryption. As long as you follow certain rules regarding encryption, even if someone gains physical possession of the your computer or memory, all they will see will be a meaningless jumble of 1's and 0's.

Researching and following proper encryption guidelines such as the ones laid out in the course I contributed to is a good start.

Most people do not understand how much control they still have over their privacy and data security.

Damage Control Once You Have Been Hacked

If you learn that you have been hacked:

- Disconnect your device or computer from the internet immediately. Disconnecting your router from your DSL, cable, satellite, microwave, leased line or other data connections or at the utility demarcation is safest. If you are away from home or accessing the internet through a WAP (wireless access point) you do not control, disable your wireless adapter and any other data connections you have.
- Take your computer in for service, request a service call or restart in safe mode if you plan to fix it yourself. It is best to reboot your computer from a boot disk. You can make boot disks with utilities such as Windows Disk Boot Creator.
- Check the settings in your antivirus software and scan your computer for viruses and malware and fix them. Hopefully your antivirus and malware software are up to date. If not, run them anyway, but you will have to update them and scan again after you reconnect to the internet.
- Search your computer of device for new software programs that you did not install and uninstall any you find.
- Backup your data.
- Change your computer and local passwords.
- Check your recycle bin for deleted files.
- Use a file restoration utility to restore deleted files that you want to keep.
- Look for changes to your files in detailed file views or with a utility program such as File Analyzer.
- Once back online, update antivirus and malware software if necessary.
- Check your online accounts, internet domains and network

connections to verify they are all functioning.

- Change your online passwords. Passwords should be changed frequently anyway, but if you learn you have been hacked, you should change them again and consider changing as much of your information as possible.
- Check your financial statements and credit report for unusual activity or suspicious entries. If you spot any, take action immediately. Call companies and suspend cards or accounts until you can clean up the mess.
- Make sure that you keep your software patched and up to date.
- Check email and social media accounts. If your accounts were used to spam your contacts, notify your contacts, tell them not to open any attachments and explain how to resolve the issues.
- Some OS’s have options to refresh without losing your data, but you will need to reinstall some software. If refreshing doesn’t work, you may have to reinstall. If reinstallation doesn’t work you may have to reformat and reinstall. Hopefully you can see the importance of preventative maintenance, backups, file history, recovery drives, disk images and boot disks. Like many areas of emergency preparedness, you can pay a little now or a whole lot later.

Some information, accounts and passwords are easy to change, but some can be difficult and time consuming, so it pays to prevent or avoid being hacked.

For example, the IRS will not just let you change your SSN unless you succeed in convincing them that:

- Sequential numbers assigned to members of the same family are causing problems;
- More than one person is assigned or using the same number;
- A victim of identity theft continues to be disadvantaged by using the original number;

- There is a situation of harassment, abuse or life endangerment; or
- An individual has religious or cultural objections to certain numbers or digits in the original number. ("We require written documentation in support of the objection from a religious group with which the number holder has an established relationship.") – ssa.gov

Even if you succeed in changing your SSN, your old number will still be linked to your new number for tax purposes.

A Very Special Kind of Theft

Cleaning up the mess left by identity theft is not as easy as TV commercials make it sound. Some companies claim that they will pay up to a million dollars to repair your credit if you use their service and become a victim of identity theft. If you listen closely, these commercials now say that they will prevent identity theft or cover your expenses if they occur with "companies in their network."

Most banks also limit your credit card fraud liability to $50, but terms and conditions apply to those programs as well. The only thing you can be sure of with programs is that your card will be declined "in network" (i.e. the places you would typically shop as opposed to places identity thieves shop) or if you travel without reporting your every move.

One of the most tragic losses you can suffer is the loss of your data, photos, music, books and other data that you value highly that is not easily replaceable. I have learned that the majority of self-reliant folks, for all their talk of tight OPSEC and preparation, do not walk the walk. Unfortunately, many of us have either difficulty understanding technology or are beholden to convenience.

This results in many of us becoming "cloud-phobic" and refusing to use any could-based service (or worse yet, only services that have the word cloud in their name) or are too lazy to read privacy policies and do enough research to be able to choose products and services with confidence.

I could say “that’s fine, do it your way” but the problem is that users who do not know how or who are too lazy to configure a backup are exactly the users who need cloud-based data backup services the most. So resist those urges and figure it out, spend 20 minutes to figure it out, ask someone for a favor, strike a barter or pay someone you trust to set up an automated, properly encrypted backup.

One anti-hacker strategy that I’ve employed in the past is that of setting out a “bait machine” or “bait network” out for hackers to see and try to hack. Much like “bait cars” used to catch car thieves, “bait machines” keep a meticulous record of every bit sent to the computer, and they are bad news for hackers. Your real network will be hidden. You would be amazed how even relatively sophisticated hackers tend to be lazy and see exactly what they think they are looking for.

Even if you are unwilling to invest the time to track down a particular hacker, by the time they realize they’ve hacked a bait machine, you’ll know enough about their hacking practices and modus operandi that they will not likely return, and if they do, you will be ready. I have used bait machines like this for years, not only to protect my own infrastructure, but to learn about the threats my IT clients are most likely to encounter.

This article has been written by ***Cache Valley Prepper*** *for* *Survivopedia*.