

Is Your Computer Safe Offline?

Probably one of the biggest notions among computer users is that if they are not online, they are safe from identity theft. Their reasoning is that, if they are offline, they are not vulnerable to phishing, viruses, malware, hackers, etc. While, it is true that being offline would protect them from such things, to fall into the belief that they are safe is being somewhat blind to other possibilities for ID theft. Even people who are connected to the Internet fall into a false sense of security. How? Computer users think that once they install a firewall, get adware, malware, and virus protection. Throw into all that, phishing protection. They get lulled into that invulnerable feeling. They think they are safe. But are they? Among the many ways to steal data from a computer is through the peripheral data ports. They can be hooked up to printers, external disk drives, etc. Still another way to steal data has been the use of CDs or floppy disks. This is done by actually stealing the disks themselves or dumping data onto them. In most cases, this can be done without the computer's owner ever knowing. Along the same ideas, hard drives can be stolen or broken into. This is a lot easier than one might think. Here's how. Hard drives fail. There's nothing that can be done about that. We get them replaced, reload the software, and move on with our lives. But what about that old hard drive? Even if it has crashed, data can still be harvested from it. In some cases, it is not easily done. There are softwares written to help map the crashed disk and retrieve information off of it. This software is used by legitimate, reputable companies as a means of data reclamation for their clients. It is also used by thieves to steal personal and company data. Another way to break into a computer involves the thief using his or her own floppy disk or CD to boot your system. With this method, they can bypass your security features and gain direct access to your data. Even more recently, with the advent of flash drives, it is easier to steal data and conceal it. These small devices are roughly the same size as a man's finger and are hard to detect when concealed. They can be stolen or lost very easily due to their small size. When it comes to dealing with these issues, many businesses are removing the extra disk drives from computer work stations. They are also networking their printers, etc. to monitor information flow. Hard drives can be rendered totally useless by drilling holes in the cases and drives. Still another way to do this is by burning the hard drive. Certain types of flash drives are being built with security features in place to aid in preventing theft. By using a security system which encrypts the data, it adds a measure of protection not offered by Microsoft. This encryption feature is called Advanced Encryption Standard (AES) symmetric encryption. It is considered to be the best encryption systems for flash drives. It should also be noted that it is not the only form of encryption available. Many versions of encryption are designed with the user in mind (I.E. ease of use). The final problem deals with the users themselves. Often times, the user will be careless with their user name and password information. They sometimes will paste it to their computer or somewhere close to it. In this case, it is always best to either commit this information to memory or store it in a very secure place.

About the Author

Ryan Smith is the author of the hot, new, blog "The 10 Commandments of ID Theft Protection" Learn more at <http://www.e-profitsubmissions.com/wordpress>

Source: <http://americanahost.com>