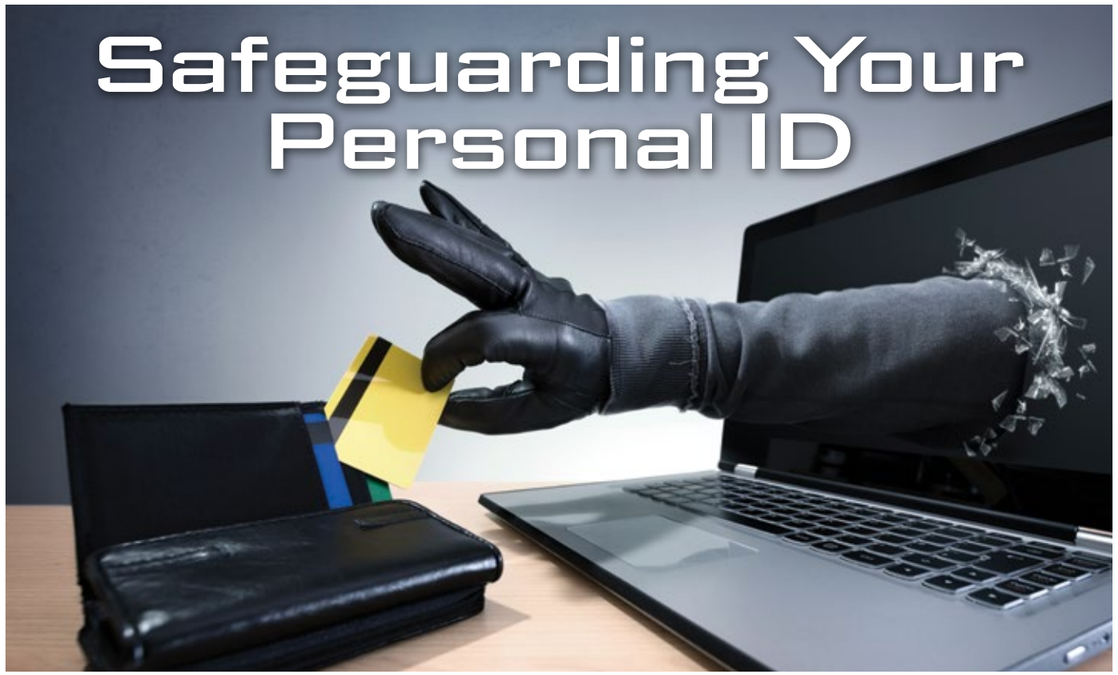
Money Matters

Common Sense and Professional Advice



© BrianAJackson

This three-pillared plan will help keep the wolves from the door.

by Jeff Huse

Chief Technology Officer at Cornerstone Advisors, Bellevue, WA

No company, government or agency has a greater interest in protecting your personal information than you do. Sure, companies have a legal obligation to protect your information, and some do a much better job than others. But it's you, not the company, that feels the consequences most severely when your private information is misused.

The companies and agencies that do a good job guarding your information usually work within a robust framework that includes the three Principles of Protection: (1) Need to Know; (2) Least Privilege; and (3) Defense in Depth. By taking your cue from them and creating a Personal Information Protection Plan, you may reduce your and your family's risk of becoming victims of information misuse and ID theft.

The Three Principles of Protection in Action

Need to Know: Think carefully before you give out any personal information, and only give enough info to get the job done. For example, does your healthcare provider really need to know your Social Security Number if they already have your insurance information?

Least Privilege: Be aware of who has access to your computer, tablet and mobile phones. And if you have someone helping you with your bills or other personal information on your computer, make sure they don't have more access than they need.

Defense in Depth: You may back up your computer regularly and run virus software, but that itself may not be enough. Talk to your computer service technician to do a full system check, make sure your virus software is updated and running properly, and ensure that your mobile devices (tablets, laptops, smartphones) are all in good defensive mode.

© Alex Belomlinsky

The Principle of Need to Know

Need to Know means that information should only be disclosed when it is necessary for a job or task to be completed. Be aware and question the reasonableness of the information requested from you when you conduct any personal business. For example, many medical offices will ask for this information, but few actually need it, especially if you are also providing insurance information. When asked for it, you can omit it outright, such as on a form, or ask why it is needed and put the burden on the requestor to justify the request.

A simpler example has to do with your phone number or email address. Retailers often ask for your phone number at the point of sale. In many cases, this information is used to gain marketing intelligence about the company's customers. Little bits of information collected in this way are joined to large caches of data that retailers purchase. By combining this information, the retailer can then know a great deal more about you than you had intended when you simply provided a phone number or email address at the register.

By itself, this may not be a problem, but when the retailer's systems are compromised and data is stolen, your personal information is suddenly in the wind, to land who knows where or for what purpose.

"No company, government or agency has a greater interest in protecting your personal info than you do."

The Principle of Least Privilege

Least Privilege means that a person operates a system with just enough privilege or access to complete the job, and no more. For example, personal computers generally include three types of user accounts: Administrator, Standard and Guest. If your everyday user account has Administrator privileges, you have the authority to install software and make configuration changes. The risk is that these changes can also be made without your knowledge in the background by malicious software and viruses.

Standard user accounts generally do not have the privileges required to make these types of changes, so your system is better protected. In most corporate environments, ordinary users do not have Administrator privileges on their workstations.

The same should be true at home: Use a Standard account for everyday use, and only log in as an Administrator when you need to install software updates or make other system changes.

The Principle of Defense in Depth

Defense in Depth is a concept that recognizes the reality that *no single solution protects any individual or organization from every security threat*. Security at any level is difficult, and effective security depends on an array of cooperating tools, technology and behavior to remain so. Each tool or technology has a role to play, and taken together the whole is greater than the sum of the parts.

Castles built within a moat, an outer wall, layers of inner walls, and a citadel are classic physical examples of Defense in Depth. Modern threats are of a different nature, but defending against them relies on the same principle.

Personal computing environments must be defended by network firewalls, strong encryption, user access control, device firewalls, least privilege, need to know, and a robust back-up and recovery plan to ensure the privacy and security of the information on the network. Talk to your computer service technician to do a full system check and review your own levels of defense.

Protecting your personal identity and that of your family depends mostly on high awareness and informed choices. Start thinking about your personal security in terms of your own Personal Information Protection Plan. This will help you avoid needlessly giving away personal information or exposing your computers and mobile devices to common threats.

Stay up to date with security patches, make sure your passwords are strong, and use multi-factor authentication wherever it is offered.

A good Personal Information Protection Plan will allow you and your family to enjoy the modern conveniences offered by today's technology without being fearful that your next mouse click could result in catastrophe. ◆