**Cyber Security**

Protecting an employer’s data and information technology systems may require specialized expertise. Depending on the particular industry and the size and scope of the business, cyber security can be very complicated. However, even the smallest business can be better prepared.

Every computer can be vulnerable to attack. The consequences of such an attack can range from simple inconvenience to financial catastrophe. While a thief can only steal one car at a time, a single hacker can cause damage to a large number of computer networks and can wreak havoc on both the business and the nation's critical infrastructure.

Start with these simple steps:

* Use anti-virus software and keep it up-to-date.
  + Activate the software's auto-update feature to ensure cyber security is always up-to-date.
* Don't open email from unknown sources.
  + Be suspicious of unexpected emails that include attachments whether they are from a known source or not.
  + When in doubt, delete the file and the attachment, and then empty the computer's deleted items file.
* Use hard-to-guess passwords.
  + Passwords should have at least eight (8) characters with a mixture of uppercase and lowercase letters as well as numbers.
  + Change passwords frequently and have different passwords for different accounts.
  + Do not give the password to anyone.

* Protect the computer from Internet intruders by using firewalls.Back up computer data. Many computer users have either already experienced the pain of losing valuable computer data or will experience it at some point in the future. Back up your data regularly and consider keeping a copy of the data off-site.
  + There are two forms of firewalls: software firewalls that run on your personal computer, and hardware firewalls that protect computer networks, or groups of computers.
  + Firewalls keep out unwanted or dangerous traffic while allowing acceptable data to reach the computer.
  + Don't share access to computers with strangers.
  + Check the computer’s operating system to see if it allows others to access the hard-drive. Hard-drive access can open up the computer to infection.
  + Unless you really need the ability to share files, your best bet is to do away with it.

* Regularly download security protection updates known as patches. Patches are released by most major software companies to cover up security holes that may develop in their programs.
  + Regularly download and install the patches or check for automated patching features that do the work for the user.
* Check the security on a regular basis.
  + When clocks are changed for Daylight Savings Time, evaluate the computer security. The programs and operating system on the computer have security settings that can be adjusted.
  + Are there multiple door locks and a high-tech security system at the office? It could be that tighter security for the computer system is also needed.
* Make sure coworkers know what to do if the computer system becomes infected.
* Keeping data in the cloud doesn’t relieve business leaders of liability if your data becomes compromised. Cloud service providers should “do their due diligence” in making sure your data is secure, but IT must do theirs to make sure those providers are doing their job.
* Sign up to receive free email alerts from the Department of Homeland Security National Cyber Alert System about new threats and learn how to better protect cyberspace, at [http://www.us-cert.gov/](https://www.us-cert.gov/).
  + Train employees on how to update virus protection software, how to download security patches from software vendors, and how to create a proper password.
  + Designate a person to contact for more information, if there is a problem.

Here is a great one page overview of email phishing to distribute to employees: Social Engineering Red Flags.

US-CERT is a partnership between DHS and the public and private sectors. It was established to protect America's Internet infrastructure through coordinated defense against and responses to cyber-attacks.If you need assistance developing your data security policy or in dealing with employee issues related to it please call Catapult's Advice team at 919-878-9222.

Written by a Catapult Advisor