Understanding Computer Security

Purpose of Computer Security

The purpose of computer security can be explained with three words. They are **CIA**:

1. **Confidentiality** - Ensures only authorized persons have access to classified information.
2. **Integrity** - Ensures the information has not been tampered with.
3. **Availability** - Ensures that the needed information is available.

There are Five Types of Computer Security

1. **Physical Security** - Prevents unauthorized persons from physically accessing information systems containing classified information.
2. **Operational Security** - Acceptable Use and Operational Policies. Includes limiting information to a need-to-know basis. This means personnel have access only to information necessary to do their job.
3. **Personnel Security** - Takes preventive measures through background investigation and screening. Ensures that employees have the ability to identify potential threats.
4. **System Security** - Protects your system with strong passwords, anti-virus software, anti-spyware software, etc.
5. **Network Security** - Protects the network from external *and* internal threats through use of firewalls, content filters, and network security configurations/protocols.

Common Security Violations

- Weak passwords are probably the number one security violation. Weak passwords are under 8 characters, and are not alpha-numeric. Easily accessible information such as names and birth dates should not be used. Many people use one password for everything. This means if you tell someone your password to Powerschool, they also know the password to your email, Pay-pal account, online banking, etc. Never write down your password and leave it where it can be found. What good is a password if everyone knows it?

- Another common violation is leaving your door unlocked and your computer logged in. This may seem like a no-brainer, however it is a very common security violation. Unauthorized persons can gain access to everything you have in a matter of seconds if they can gain physical access to your computer. Hackers have programs that can log your every keystroke. They take only seconds to install via flash drive, *if* they can gain physical access to your computer.

- Rogue access points are the bane of network security. Wireless access points are convenient and inexpensive. So why can't we just put them all over the place? Basically, they punch holes into network security. Professional grade access points have special security features that maintain network security. Linksys-type access points do not have adequate security, which means that anyone who can pick up on their signal has an 'open window' to exploit the network.

Data is an Asset and it Must be Protected!

Data is every bit as important an asset as school buildings, vehicles, employees, etc. Once it is compromised, it becomes worthless. Please do your part to protect our data!

Tech Tickler edition three. June 2010. Tom Brown. Technology - 435-868-4238 - ICSD District Offices