INTELLIGENT
TECHNICAL SOLUTIONS

Effective Ways to Secure Your Business Network

PHYSICAL SECURITY

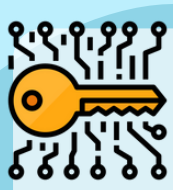
Physical security is one of the most overlooked security risks in networking. Too often servers and network equipment are kept in publicly accessible locations within a business where very little effort would be needed for someone to gain access to business, client, and financial data.

PASSWORD SECURITY

Passwords are one of your first lines of defense against unauthorized access to your network. The first thing anyone should do when putting in a network device is changing the default password. A good practice for any business is to require everyone to change their password every 3 months and to use some type of password complexity rules. (For example, a minimum of 16 characters, must have numbers and letters, and must have at least 1 capital and 1 lowercase letter.)

SEPARATE NETWORK FOR GUEST ACCESS

With so many types of malware, have any guests connect their personal laptops to a separate network from your production network. This will eliminate any contamination the guest's laptop may carry.



WIRELESS ENCRYPTION

Many older wireless devices are still using WEP encryption, and while better than no encryption at all, a WEP key is now easily captured within 10 minutes of an intruder starting an attack.

SOFTWARE UPDATES

Non-Microsoft software is vulnerable to holes in security as well. Adobe Acrobat Reader and Java are pieces of software on every computer. They were recently in the news when Google and 31 other corporations were hacked because the software was not updated properly. Now there are many viruses using this same attack to pull data from PCs all over the world.

WINDOWS UPDATES

Windows updates are very important in closing security holes in your operating system and Internet Explorer. Updates are released regularly and should be run often.

ANTIVIRUS

There are hundreds of viruses released every day. Having a good antivirus is a crucial first line of defense in protecting your data.

ANTI-SPYWARE

Spyware is becoming an ever-growing problem. Not only does it cause PCs to crash and run extremely slow, it also captures personal data as it is typed into websites.

SPAM FILTERING

Phishing has become a large security risk lately. Intruders create fake emails that resemble e-mails from trustworthy institutions (like banks) or social media sites. These e-mails ask for personal, sensitive information like usernames, passwords, and credit card details. Spam filters can catch these e-mails before you ever see them, reducing the risk of someone replying.

LOGGING

Logging is a major key in finding potential attacks on your network. By logging failed attempts you can find if someone's login is at risk of being hacked. On firewalls, you are able to see who is trying to access information both coming into your network and leaving your network.

INTELLIGENT TECHNICAL SOLUTIONS

For more useful tips on how to improve the security of your computer network, check out our Learning Center: https://www.itsasap.com/learning-center