fINANCE NEW MEXICO

Article 491 February 26, 2017

# Simple Steps Can Keep IT Networks Safe

*By Steve Resnick, Owner, Capitol Computer*

The information age and rise of the internet have changed the way people live, work and interact. But along with better communication come virus attacks, hijacks and hostile invasions that can make the internet seem more like a war zone than a social and information network.

Savvy business owners can protect their frontlines by acting like commanding officers of their internet armies, ensuring that multiple levels of security are in place to repel and combat enemies.

Protection starts with a good enterprise-grade Unified Threat Management (UTM) appliance — also known as a firewall — as the primary defense against invasion of the business's network, computers and data. Firewalls such as SonicWall, Cisco Meraki and Fortinet connect to the business's Internet Service Provider (ISP) through a modem, creating a blockade between the internet and its users.

Antivirus software provides a secondary line of defense that should be installed on every computer in the business. Bitdefender, ESET and Sophos are strong options that will thwart malicious programs or pieces of code that can run in the background without the user's knowledge and infect all computers on the network.

Wireless access to an internal network also poses a threat. The use of encryption and passwords that give access to employees, but keep others out, can maintain network safety. Ubiquiti is a good brand of wireless access equipment that allows guests to use a separate wireless network and upholds the privacy of the primary network.

A Policies and Procedures manual that covers internet and computer rules can guide employees toward safe practices that protect company data. Policies should address passwords, email attachments and "safe surfing" practices.

Passwords should be changed often, and each account should have a different pass-code. Strong passwords are a combination of uppercase and lowercase letters, numbers and symbols that have no discernible meaning when strung together. More characters are better, and employees should refrain from using personal identifiers related to birthdays, pet names or other easily guessed information.

Set safe internet browsing levels on the control panel of each computer, and advise staff to stick to well-known websites with mainstream content. Employees should also be careful when clicking on links. Hijacking occurs when a malicious webpage takes control of the browser and attempts to influence the user's actions.

While firewall and antivirus software will scan email for threats, an email attachment can act like a Trojan horse when opened, unleashing programs that override normal operations by encrypting data. When opened, ransom-ware embedded in the attachment encrypts important files and renders them unusable. A pop-up window then demands that the user pay thousands of dollars in ransom. Once the ransom money is deposited in a bank account, there is still no guarantee the files will be decrypted and usable.

Identity theft can occur when a hacker steals personal and private information from a computer or online account — or more simply when an email system perpetuates scams by sending messages without the user's knowledge. These and other hostile invasions — of online accounts, networks or computers — can be avoided by taking precautions and using common sense at every level of computer interaction. With the proper armaments, businesses can keep their computers and networks safe.

For more information, visit Capitol Computer and Network Solutions at www.ccandns.com.

*Finance New Mexico is a public service initiative to assist individuals and businesses with obtaining skills and funding resources for their business or idea. To learn more, go to www.FinanceNewMexico.org. Sponsored by:*