LEGAL workspace
Your Law Office in the Cloud

5 WAYS
EMPLOYEES ACCIDENTALLY THREATEN SECURITY

Learn more about today's cloud computing solutions for law firms.

A Legal Workspace® White Paper

5 Ways Employees Accidentally Threaten Security

What do you think is the biggest threat to your IT security system? A hacker getting past your firewall? Unencrypted emails? Lack of consistent back-ups? Those may be serious concerns, but the biggest threat to security for a law firm is actually its employees.

That's right: The very people who keep your organization running are the same people who might be putting your data at risk. Here are the top five ways in which employees jeopardize security.

Opening email virus attachments

An attorney receives an email with an attachment called myresume.zip. He or she opens the attachment, and—just like that—a CryptoLocker Ransomware virus is running rampant through your network.

CryptoLocker Ransomware viruses install a program on the infected computer that systematically accesses and locks all of the data files—including network files. To regain access to the files, money (usually hundreds of dollars) must be sent to the hacker. This type of virus can be increasingly aggressive and quite lucrative for the hacker. And, there's no guarantee that the hacker will honor his side of the deal and unlock the files.

This is one of many viruses that an employee could unleash into your law firm's network by simply clicking the wrong link or opening an unsafe email attachment. To halt this type of attack, educate employees not to click on anything unknown. Make sure that your antivirus programs are regularly updated and can sufficiently block malware file types and are capable of removing infected files.

Weak user IDs and passwords

As the number of usernames and passwords needed by the average person increases, some employees take the following shortcuts to remember their information.

- use the same ID and password across multiple accounts
- use common words or phrases
- use personal information, like a spouse's name or birthday

Weak user IDs and passwords account for a significant portion of data breaches. A 2015 security analysis states that along with weak remote access security 94% of breaches were because of weak passwords. Often, news stories about famous people being “hacked” are actually about people or automated programs gaining access to celebrities’ information because they’ve been able to guess their usernames and passwords.

Educate users about what constitutes a strong password and put systems in place that require frequent password changes.

- use passwords of 10-charcter length or more with complexity
- randomly insert symbols and numbers mixing lowercase and uppercase letters
- use multiple security questions

Phone scams to access a computer

An employee might receive a telephone call from someone claiming to be from Microsoft support. The caller might say that the attorney’s computer has been compromised and is sending out critical personal information. In order to correct the problem, they must allow the caller remote access to his/her computer or give other identifying account information.

Of course, the caller isn’t really a Microsoft support representative. It’s a very sophisticated hacker. Warn employees about phone scams. Callers might claim that they’re following up on open service tickets or investigating virus infections. Employees should never allow unknown callers remote access to their computers.

Unrestricted administration rights

If every attorney and staff member has permission to install programs or applications at the firm, it forms a security loophole. These security risks create vulnerabilities on the computer that can be exploited by hackers to gain access to the network. Many employees are tech-savvy and aware of current security threats, but some may inadvertently download a virus or malicious application.

To prevent these weaknesses and diminish the risk of downloading malware, tighten administrative rights so that an individual—someone in a supervisory position or an IT legal professional—manages program and application installation. .

BYOD security risks

Bring Your Own Device (BYOD) opens security holes in a couple of different ways: through home computers and various other devices.

When employees use home computers, a Virtual Private Network (VPN) connects them to the company network for remote access. But, the company doesn't have any control over the home computer's security. Is there robust antivirus software installed on that computer? Are there others at home using the computer unknowingly downloading viruses? Is it updated regularly? All of these threats, if not regulated could place the entire law firm's data and security at risk.

Tablets, Smartphones, and other devices can also complicate the process of securing a network. One potential issue has to do with applications installed on Smartphones or tablets. Permissions for those applications might allow a third party access to data, such as images or contacts, on that device. Access to images on one of these devices could leak sensitive confidential information that compromises your client or law firm.

How to protect employees from themselves

Provide a work station use policy, which outlines dos and don'ts for employees. Training helps employees understand the reasons behind the policies and reinforces appropriate actions.

Legal Workspace is a cloud service for law firms that provides IT training for its clients and employees. We work with clients to implement a number of security policies and procedures to protect data against security threats. And, because Legal Workspace's cloud-based solution is designed in such a way that remote devices can only access the environment through an encrypted channel, BYOD issues get eliminated.

Employees' mistakes could have serious consequences to your business. Take the necessary steps to protect your system today and increase your data security for the future.