VIRUS & MALWARE IN THE OFFICE

Get a Free copy of the "8 Layers of Defense" for your company today!

JUST TEXT **"CYBERSAFE" TO: 33444**

858-633-1132
LIVE HELPESK

When it comes to protecting your company and personnel's private and priceless data, be sure to implement **ALL 8 Lines of Defense!** **This could be** the difference between safety and disaster!

1 POLICIES

Security begins with **P O L I C Y**. When employees are shrugging their shoulders and management doesn't know where to look for guidance, you have the seeds of a **MAJOR IT issue on your hands**. A written, clear, concise use, device, remote work, data protection, and other policies help to ensure all parties are acting in accordance with the company's safety and best interest.

2 EMPLOYEE EDUCATION!

Policy is only as good as the education that backs it. What good is investing in new technology or even documenting best practices if your team hasn't been educated on safe-computing practices? **The best education is recurring and includes pre-scheduled notices and alerts!**

3 PERIMETER DEFENSE | FIREWALL

A company's first line of defense is a strong and secure firewall that protects the company's perimeter. Locking down open and unused "ports" is often overlooked, but this is essential to prevent numerous, automated hacks employed by the "bad guys."

4 EMAIL & SPAM PROTECTION

Today, **9.5 out of 10 emails are SPAM, and many contain dangerous malware, spyware, and viruses.** Thus, preventing suspicious emails from entering your network in the first place is one of the best strategies to avoid serious danger. This is why a **perimeter SPAM defense system** with archiving capability is the smart solution.

5 VIRUS SOFTWARE

Virus solution companies spend millions of dollars to stay one step ahead of the "bad guys." The problem is, even the best virus software can only play "catch-up." This has truly become a "cat and mouse" game. Virus companies can never technically "win." The best they can do is contain and quarantine KNOWN viruses.

6 PASSWORD + 2 FACTOR

Even the most complex passwords today aren't enough. There are simply too many smart guys with bad intentions. Today, best practice for passwords involves something known as **"2 Factor" authentication.** This means that any login involves both a password and a secondary confirmation **device,** such as a cell phone or email.

7 BACKUPS

Backups. Backups. Backups. Backups need to happen automatically for all data that is considered essential. Multiple backups of various types must exist—full and differential, for instance. It's essential that backup media vary, and never store all your backups at a single location.

8 ARCHIVES

Backups are great, but ARCHIVES for important data (offsite storage of a dated backup) are even more essential. Should data be lost or backups prove to be backing up incorrectly or with corrupt data, your only recourse is a data ARCHIVE!

FORTRESS NETWORX
Service: Our Specialty. Security: Our Forté.

© 2017—2021 | Fortress Networx | www.fortressnetworx.com

San Diego's Premiere IT Outsourcing Company—Over 25 Years! We LOVE I.T.! 2x Better Business Bureau Torch Award Winner!