COMPASS Computing Group, Inc

15 ways we protect your organization from a Cyber Attack!

503.691.5706
www.compcomgrp.com

Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: _____

Spam Email

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

Passwords

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

Security Awareness

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

Did you know?

1 in 5 Small businesses will suffer a cyber breach this year.

81% Of all breaches happen to small and medium sized businesses.

97% Of breaches could have been prevented with today's technology.

Advanced Endpoint Detection & Response

Protect your computers adata from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

Multi-Factor Authentication

Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

SIEM/Log Management

(Security Incident & Event Management)

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

Web Gateway Security

Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

Mobile Device Security

Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

Backup

Backup local. Backup to the cloud. Have an offine backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

Cyber Insurance

If all else fails, protect your income and business with cyber damage and recovery insurance policies.