15 Ways To Protect Your Business From A CYBER ATTACK

Updated for 2020

DID YOU KNOW?

1 in 5 businesses will suffer a 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.

CYBERSECURITY IN THE NEWS:

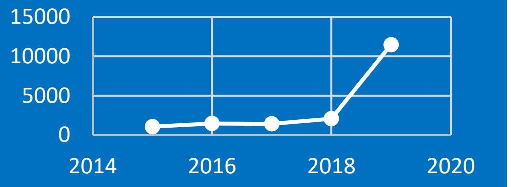
In 2020 during the Coronavirus Pandemic working from home has become the norm, however doing it safely hasn't been.

Analysis by researchers at cybersecurity company Tessian reveals that 52% of employees believe they can get away with riskier behaviour when working from home, such as sharing confidential files via email instead of more trusted mechanisms.

"People will cut corners on security best practices when working remotely and find workarounds if security policies disrupt their productivity in these new working conditions," said Tim Salder, CEO of Tessian.

It's more important than ever to have a qualified IT team backing your business, they can make sure best practices are still being enforced even while employees are working home and develop strategies to keep your business flowing smoothly even in the midst of a crisis.

Annual Cost of Reported Cyber Crime Incidents By Millions



*Cybercrime damages are expected to be $6 Trillion by 2021.

□

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.

□

Support Team:

A single IT support person may be overwhelmed and not able to assist you promptly or effectively. With a Managed IT Department behind your business you can feel confident there is an entire team available to assist your business – so you won’t be left hanging.

□

Advanced Endpoint Security:

Protect your computers and data from malware, viruses, and cyber attacks with advanced endpoint security. Today’s latest technology protects against file-less and script based threats and can even roll back a ransomware attack.

□

Multi-Factor Authentication:

Utilize multi-factor authentication whenever you can including on your network, bank 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.

□

Work from Home Strategy:

Develop a work from home strategy for your employees. May include disallowing accessing personal accounts on work devices, using a VPN, and using remote access to make sure they stay up to date on necessary patches.

□

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. Encryption can make all the difference in a cyber security event.

□

Backup:

Backup local. Backup to the cloud. Have an online 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 income and business with cyber damage and recovery insurance policies. Many places offer inexpensive policys and your IT team can make sure you stay compliant in the event you need to use it.

Valley TechLogic, Inc 111 Business Park Way, Atwater CA 95301 (209) 357.3121 www.valleytechlogic.com