12 Ways To Protect Against
RANSOMWARE ATTACKS

SECURITY ASSESSMENT

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

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.

PASSWORD SECURITY

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.

did you know?

60% Small businesses shut down within 6 months after suffering a breach.

82% Ransomware attacks on businesses smaller than 1000 employees.

1.7M Estimated number of ransomware attacks per day.

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.

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.

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.

ADVANCED POINT SECURITY

Protect your computers and data 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 Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

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.

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!

DATA ENCRYPTION

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

DATA BACKUPS

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.

*Sources: National Cybersecurity Alliance, Verizon, Splunk

Cyber Insurance

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

Breeze LOGIC
IT SERVICES & SOLUTIONS

Get started with a 7-point cybersecurity risk assessment to see how protected you are.
Schedule yours today: 0330 320 2223 | info@breezelogic.co.uk