starcom.
A Node4 Company

$$$$$$

8 WAYS TO OUTSMART RANSOMWARE

Ransomware is a type of malicious software that prevents or limits you from accessing your systems, files or data unless a ransom is paid. It's a cybercrime that's on the rise and is becoming more sophisticated, therefore presenting higher risk to business continuity, financial stability and reputation.

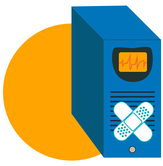
This goes to show that ransomware isn't just techie-talk. It's incredibly relevant in the boardroom, too, and as a business leader, you should be acutely aware of ransomware threats and how to combat them. Here are 8 ways that you can work with your IT team to outsmart ransomware and fortify your defences against one of today's most debilitating cyber threats.

Email education for all

If there's one ransomware risk everybody in your organisation – from support to board level – should be trained to spot, it's suspicious emails. They account for 60% of all attacks but can be prevented with basic training. Look at the domain, spelling and signature, and hover over links to check where they head. And always question the email's legitimacy.

Choose multi-dimensional security

Ransomware can take control of your entire system through a single entry point. So, meet with your IT team and ensure they're using a multitude of cybersecurity measures. Firewalls, anti-virus, email and web filtering, anti-spyware and intrusion prevention tech should all be implemented.

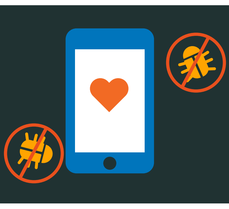


Ensure backup and recovery are robust

If you're attacked, you'll be without the systems that run your business until a resolution in found. So, robust backup and disaster recovery are critical to reducing impact and recovering data and operational function. This calls for a strategic plan and the best-suited tech solutions.

Show endpoints some love

A shrewd ransomware tactic is to access your systems via unused or vulnerable endpoints – internet-capable devices such as desktops, laptops, smartphones and printers. These personal and corporate devices often don't have anti-malware, so make sure your IT team has all endpoints protected with the right anti-ransomware solution.



Update, patch, check, repeat

Many attacks are based on known weaknesses in operating systems, web browsers and applications. Therefore, it's critical that your business applies updates and patches promptly and professionally. Ideally, your team will automate this essential process, so you never miss a trick.

Segment your network

If not stopped, ransomware can spider across your network, until it reaches the server where it can inflict the most damage. Segmenting the network where critical apps, devices and data are isolated can limit the spread, as can separate networks for internal and guest Wi-Fi.

Kick suspect files into quarantine

Ransomware often resides in unassuming files so it can be challenging to identify what is and isn't a threat. Using technology such as sandboxing moves suspicious files to quarantine for analysis before they enter the network.

Protect your Android devices

Did you know that Android devices are prime ransomware targets? Ask your IT team to take precautions such as ensuring devices aren't routed, app installations from unknown sources are disabled and third-party security apps are active to stop attacks in their tracks.

Putting these essential cybersecurity measures in place involves a lot of heavy lifting and expert application from seasoned IT specialists.

If you're worried about the performance of your cyber defences, want to uncover hidden weak spots or need to upgrade software in line with the latest threats, contact the Starcom team on 0844 579 0800 to book a Cybersecurity Health Check.