Magic Stone Cyber Solutions

Magic stone 7 tips for better cyber security

Cybersecurity is a major concern for SMBs today; 25 million of SMEs are active today in the European Union and employ more than 100 million workers.

Why are small & medium businesses vulnerable to cyber-attacks?

Small & medium sized businesses are more likely to be targeted by cyberattacks. For smaller companies, the problem stems from a **lack of assets and expertise**. Small and medium-sized businesses usually don't have dedicated cybersecurity experts to keep their systems secure.

Cyberattacks can cause devastating consequences for any business, but small businesses are uniquely at risk. When a cyberattack hits, unprepared small businesses may deal with overwhelming financial repercussions as well as hits to their reputation, pricing structure, productivity, employee morale, and much more.

Magic stone 7 tips for better cyber security

Tip 1- 90% cyber-attacks begin with a phishing email

That staggering figure is placing email security as the number one focal point of every business leader. We share, collaborate information and communicate mainly via email.

Bottom line:

- Awareness & training – make sure that you and your colleagues are up to date with identifying phishing scams. Be suspicious of emails, phone calls, and text messages
- Be suspicious with unknown senders
- Known senders can also be infected and send malicious content, be cautious
- Do not open when only a link or attachments are sent
- If you are not sure, call the sender, do not reply!
- Check for grammatical errors
- **Invest in advanced email protection**

Magic Stone Cyber Security B.V
Rembrandtweg 343
1181GL Amstelveen, The Netherlands
Chambers of commerce 75316455 Te Amsterdam VAT NL860235427B01
Bank ING NL08 INGB 0009 4400 13

Magic Stone Cyber Solutions

Did you know 

Expert cyber-defense technologies and services are considered large investments aimed at larger companies. Enterprise-grade solutions that are now available for the SMB market!

Tip 2 - Change passwords more frequent, Use Strong Passwords and/or Use a Password Management Tool

- Don't use the same password twice
- Strong passwords are important in keeping hackers out!
- Strong passwords - should contain at least one lowercase letter, one uppercase letter, one number & known symbols
- Reset forgotten passwords, change passwords at least once a year
- Use a password management tool and/or a vault for your passwords

Tip 3 - Use Two-Factor or Multi-Factor Authentication (MFA or 2FA)

Two-factor or multi-factor authentication is a service that adds additional security layer on top pf the username and password identification. With multi-factor authentication, you are requested to enter more than two additional authentication methods after entering your username and password

Tip 4 - Keep Your Software Up to Date

One of the most important cyber security practices to mitigate ransomware is patching outdated software, both operating system, and applications (Zero-day attacks)

- Turn on automatic system updates for your device and/or check systematically for updates
- Make sure your applications, desktops, browsers and plugins are up-to-date

Tip 5 - Backup Your Data – recovery plan

Backup and recovery are essential in case something has happened in your digital environment. The quicker you are able to overcome a cyber attack makes your business more resilient. Cyber attacks are not just about ransomware. A business should think also about its reputation, brand and losing clients.

- Backup frequently
- Choose backup that is also checked for malicious content and ransomware
- Choose a backup plan and software that you understand

Magic Stone Cyber Security B.V
Rembrandtweg 343
1181GL Amstelveen, The Netherlands
Chambers of commerce 75316455 Te Amsterdam VAT NL860235427B01
Bank ING NL08 INGB 0009 4400 13

Magic Stone Cyber Solutions

Tip 6 - Anti-Virus Protection / Endpoint security & Firewall

Anti-virus (AV) software is the most common prevalent solution to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data.

Firewall - a firewall built in to prevent attacks on your network

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules

Tip 7 - Protect your most important data and make sure your business is compliant

The General Data Protection Regulation (GDPR) consists of a number of rules for the (automatic) processing of personal data. This EU regulation forces you as an entrepreneur to act more carefully and responsibly when dealing with personal data of customers, personnel, or others

10 steps for being GDPR compliant - what are the rules?

Did you know

A resilient cybersecurity strategy is essential to running the business while protecting against security threats and preventing data breaches and other enterprise cybersecurity threats