ramsac
at the heart of IT

10 tips for better cybersecurity

Cybercrime affects every organisation. It is vital therefore that you take appropriate preventative action. This starts with employee training and planning how to react to a breach to minimise the risk of a cyber-attack. We have put together our 10 top tips for better cybersecurity.

1 Do not use public Wi-Fi

Public Wi-Fi is a huge security risk and we recommend not connecting to it unless you can verify its legitimacy, even then use it with extreme caution and always with a VPN. A classic scam involves hackers sitting in the corner of places like coffee shops broadcasting a "free" wireless access point. If you connect your mobile device to that Wi-Fi point scammers are then able to access your device and all your data.

2 Train your staff on the importance of cybersecurity

Training employees will radially reduce an organisations cyber security vulnerability, 90% of breaches happen due to human error (tech radar, 2019). By showing employees how to be vigilant to protect themselves and the organisation they work from cybercrime the risk of an attack will be reduced. This is also a requirement under GDPR and thus is not optional!

3 Subscribe to phishing tests

We recommend organisations subscribe to a phishing testing and awareness service. These services carry out random simulated phishing attacks, ensuring that every user receives a very realistic phishing email at least twice a year.
The emails mimic phishing emails from well-known brands such as LinkedIn and Microsoft, and if the user clicks on a link they will be taken to a safe web page, that highlights what they have just clicked on and offers them an immediate online training session on how to spot attacks in the future.

4 Create a cyber response plan

A cyber response plan is vital to minimise the impact of a cyber security breach. Make sure that everyone in your organisations knows exactly how to respond in the event of a cyber attack. Being level-headed when an attack happens is vital. Once you have a plan, share it, test it and make it visible.

5 Physical security is just as important as cyber security

Physical security protects your data by preventing people from literally getting their hands on it. It includes your CCTV, locks, fences and other means of limited physical access to your business and your business's data. Not letting people in to wander around your building unchallenged. Ensuring employees don't leave machines unlocked or passwords on post it notes.

6 Manage your passwords

Its vital for organisations to have a password policy, to prevent employees using the same password for multiple websites or tools. Passwords should be complex, unique, changed regularly and not shared with others, a stand alone password manager (Like PasswordBoss or LastPass) that can help with managing passwords.

Always use Multi-factor authentication too wherever it it's available to make this process even more secure.

7 Report malicious websites and web ads

There are many websites that aren't genuine and are malicious in nature. It is important to report these misleading websites, phone numbers, web ads and text messages. You can report these via Action Fraud.

8 Analyse any previous breaches

It's important to assess cyber-attacks the organisation has suffered to analyse what happened. E.g. Was it malware? How did it get in? Did everyone act promptly? Could the infection have been prevented? Were there any lessons learned? What needs to be improved?

9 Install updates regularly

By installing updates regularly, you will reduce your risk of ransomware attacks. Plenty of malware is designed to exploit security holes, patches and updates are the software company's way of fixing those holes. It is important to make sure you're running updates on servers, PCs, laptops, macs and mobile devices as soon as they are released. If you rely on someone else to do this for you request proof that it is happening.

10 Attend cyber security awareness seminars

Cybersecurity is constantly evolving, as cybercriminals get more sophisticated so do their crimes. The types of cyber-attacks are also changing. It is important to stay up to date by reading cybersecurity news, following experts on twitter and attending cybersecurity awareness seminars. Make sure you are keeping up to date with all the new cybercrimes and that your employees are educated on them.

Find out more

For more information on ramsac's cybersecurity solutions and how you can protect your organisation:

01483 412040

cybersecurity@ramsac.com

www.ramsac.com

ramsac
at the heart of IT