SMALL BUSINESS IT SECURITY HEALTH CHECK

WHAT ARE THE QUESTIONS THAT YOU NEED TO CONSIDER REGARDING THE STATE OF YOUR IT SECURITY?

Small business: the targets of cybercrime

Small businesses are the engines of economic growth and innovation. But they are also targets for cybercriminals intent on stealing valuable data. It might be staff records with social security numbers and salary details, banking and payment data or customer account information.

Security: knowledge and software

Part of the challenge is to have secure IT infrastructure in place. But you also need to ensure employees understand risks posed by cybercriminals and that your business has the processes in place to deal quickly with any security breach.

Our 17-step IT Security Health Check can give small business owners (SMBs) a snapshot of how secure their business is against online threats.

The key issue is that of awareness. Action comes from the top, and if business owners and managers are unaware of the threats, little will – or can – be done. SMBs' focusses and areas of expertise are rarely that of internet security, so it is no surprise that is isn't front of mind. Only when a business is subject to attack does it become so, by which time it is too late. So, it's essential that you organise or empower others to protect your business through cybersecurity: training and infrastructure.

As a small business owner or manager, are you aware of the following areas of potential vulnerability that could be leaving your business open to attack?

- Company policy – failure to wipe/cleanse company devices, weak passwords, unrestricted bring your own device (BYOD) policy, widespread access to data
- Compliance – lack of knowledge of data law and breaches, risks from non-compliant partners and vendors
- Employee knowledge – no training on passwords, public Wi-Fi, or software protection
- IT infrastructure – out-dated operating systems, no firewalls or antivirus, unsecure email services, no encryption for hardware, large numbers of devices with server access

It may that you're addressing some of this, but one weak link is all it takes to allow in perpetrators. For example: if one of your employees uses unsecured public Wi-Fi in a café on a device they use to access private or sensitive company data, bad actors may be able to use this as a point of entry into the wider company network. This can give them access to hard drives, devices/endpoints and software, allowing them to steal or leak data, or stage ransomware attacks.

AVG Business

SMALL BUSINESS IT SECURITY HEALTH CHECK

Threats to your business

- Staff computing devices
  - Cybercriminals try to get employees to install spyware, adware, malware or viruses to their computing devices – from tablets and mobiles to desktop computers – so they can access everything your employees can access, and sometimes more! These can take the form of simple malicious links or more complex social engineering attacks that trick employees into handing over passwords, logins or data.
- Network
  - While networked computers allow easy access between employees and data sources, it also means anyone linked in is a vulnerability and could be the entry point to the whole of your business' network.
- The Cloud
  - While the Cloud has great benefits, it can leave you open to data loss or theft, and service hijacking.
- Passwords
  - Learning passwords for devices and software is a key way that cybercriminals acquire access to your assets.
- Mobile devices
  - Whether you operate a BYOD (bring your own device) policy or you provide company devices for work, your business is open to new risks. The main threat comes from devices without a PIN (or a weak PIN) that get stolen.
- Staff
  - As well as external attacks, companies can fall prey to their own employees taking advantage of access: stealing data or damaging/infecting systems on purpose or through ignorance.
- Emails
  - Emails are a common source of entry, from phishing to malware. For example: perpetrators send out mass emails disguised as an authentic communication from a bank (or similar) telling recipients to verify their account information by clicking on a link. The victim supplies log-in information and the bad actors take money from that account or divert money to theirs.
- Websites
  - Many websites carry malware, adware and other threats that can be downloaded to devices automatically. Sometimes the sites themselves have been attacked and the editors don't know of the risks their website poses.

By addressing these threats, you can help to protect your business. Take the IT Security Health Check again to see your progress and remaining areas requiring your attention.

LEARN MORE ABOUT AVG BUSINESS PRODUCTS

AVG Business