AVG’s Small Business IT Security Guide

Small businesses can’t afford to ignore the danger of hacking. All the research points to hackers targeting businesses they see as an easy target for stealing customer or employee data and bank details. Our IT Security Health Check is a starting point for small businesses to gauge how prepared they are – and here are our best practice answers to each of the 17 quick questions.

Part 1 – Employees

Do you limit access to data within your company, designate trusted employees and adopt a strict need-to-know policy?

Administrator privileges should be given only to those who need them. However, every employee must be trained in safe computing practices. Most cyber attacks that result in data breaches require some user to surf to an illicit website, to open a malicious attachment, or to click on a booby-trapped e-mail link; so educate employees about the dangers.

Do you educate employees on data security policies and procedures, including the need for strong passwords?

Do not simply instruct your people. Inspire them. Educating employees about security is an opportunity to make everyone feel like a member of a team on which the welfare of one is the welfare of all.

Have you determined which members of staff should be trusted to possess administrator privileges?

Determine who on your staff should be trusted to possess administrator privileges: the level of access that allows the installation of new software and the changing of configuration settings. By limiting such privileges to the fewest possible people, you reduce the number of individuals onsite who might – accidentally or purposely – upload malicious software or configure a system to reduce its security.

Have you informed employees about the dangers of accessing cloud-stored data through unsecured wireless networks in public places such as airports and cafes?

Create crystal-clear policies on the use of laptops, tablets, and mobile devices outside of the office. Restrict the use of flash drives and other portable storage devices. Stolen portable devices are a leading cause of critical data breaches. For employees who travel, provide laptops or tablets loaded with the bare minimum of data – if any at all. Employees can access needed data files in the cloud, without having to download or retain anything.
Part 2 – Company Processes

Do you routinely destroy unneeded information – shredding old paper files, physically destroying old hard drives, wiping portable devices, and removing and destroying any memory or SIM cards in smartphones and other devices you dispose of or sell?

Take stock of the data you routinely gather and accumulate. Retain only the information you actually use or are required to hold by law.

Have you ensured that third-party partners and vendors have proper security procedures in place?

Look beyond your own four walls. Third parties, including outside partners and vendors, are the cause of many breaches. Vendors in particular have been implicated in at least a third of serious data security incidents. Work closely with all third parties to ensure proper security procedures are employed after data leaves your immediate control.

Have you considered restricting web surfing on company computers and smartphones or distributed a list of off-limits high-risk websites or website categories?

Consider restricting web surfing on company computers and smartphones. You may simply distribute a list of off-limits high-risk websites or website categories, or you may invest in a web proxy to automatically filter out specific web addresses or categories of addresses.
Part 3 – Policy

Do you know the law on data security and on notifying customers about any breach?

Consult a law firm with a specialty in this area. Ensure that your internal policies and procedures are compliant. Because regulations change and case law evolves, budget for a yearly review of your policies. Educate employees on data security policies and procedures. If your state has regulations governing required training and education, comply.

Have you created a Data Breach Notification Policy, which is a document you provide to all of your customers, telling them how your business will notify them should a data breach occur?

A Data Breach Notification Policy is a document you provide to all of your customers, telling them how your business will notify them should a data breach occur.

Have you created an internal incident response plan for dealing with breaches and post-breach notification?

In addition to the Data Breach Notification Policy, create an internal incident response plan for dealing with breaches and post-breach notification. Identify who will be responsible for liaising with customers, communicating with employees as well as ensuring that the breach has been fixed.

If you detect a breach, fight the urge to panic and, whatever else you do, do not even think of ignoring the incident.

- Gather all the facts of the incident—whether a breach is confirmed, suspected, or potential.
- Act according to your incident response plan.
- Notify relevant financial institutions, starting with the bank or company that manages your credit card or other online payment processing.
- Notify your data breach insurance carrier.
- If your insurance carrier does not furnish legal counsel, secure outside qualified legal assistance to help identify what laws may be involved and whether the incident warrants or requires consumer and/or government notification.
- Notify affected customers in accordance with the terms of your Data Breach Notification Policy.
- Ensure that you have fully addressed the breach itself, so that no more data is being lost and no more data is at risk. If necessary, consult with a cyber security expert.

Do you have a policy to ensure strong passwords are used across the network to protect critical systems?

Provide the appropriate training to build in your workplace a password-intensive cyber culture. This means requiring everyone to create and use passwords – strong passwords that are guarded seriously.
Part 4 – IT Infrastructure

Have you upgraded all the computers in your business to the latest operating system?
Upgrade all the computers to the latest operating system. The latest versions of operating systems are almost always the most secure.

Is your network configured to automatically install security updates?
After upgrading your operating system and other critical software, configure all security updates for automatic installation. Malware evolves continually. Security patching struggles to keep up, and automatic updating keeps your defenses as up to date as your software vendors manage to be.

Have you installed firewalls, anti-virus, and anti-spyware programs?
Install firewalls, anti-virus, and anti-spyware programs. Configure these for automatic updating.

Does your email provider offer virus and phishing scans?
Use an e-mail provider that offers virus and phishing scans. By all means, install on each of your computers anti-malware software that scans incoming and outgoing messages. However, it is most effective to scan email that has already been filtered by your provider.

Have you encrypted critical hard drives, data storage devices, folders and files?
Encrypt critical hard drives, data storage devices, folders, and files. In addition to encryption, use strong passwords to protect access to critical systems and files.

Have you reduced to the necessary minimum the number of devices that have administrative access to your company’s servers?
If your business is sufficiently complex to warrant even a small IT staff, consider reducing to a necessary minimum your number of connections to the Internet. Ensure that all of these gateways are managed by one IT person or IT team. The fewer points of entry and exit, the easier it is to provide adequate security. A data breach attack typically begins with the compromise of just one networked PC, laptop, tablet, or smartphone. For this reason, reduce to the necessary minimum the number of devices that have administrative access to your company’s server(s).

Take a lesson from the government and the military. Federal agencies seeking the highest possible level of cyber security “air gap” computers that store their most sensitive data. This means putting the most highly confidential and proprietary data on computers that are neither physically nor wirelessly connected to the Internet. This will undoubtedly create inconvenience, but you must weigh this against the consequences and costs of a breach of your most critical data.