Small Business Security Guides

Securing your start-up or small business

AVG AT WORK

Keeping systems running and information secure in an online world

Small businesses can suffer hours of downtime per year for every computer used in their company, whilst the last two years have seen identity and information theft become the top security concern for the majority of business owners.

> *"A security breach is far more likely to have a devastating effect on the revenues, or even the survival of a start-up or small business."*

The technology landscape in smaller organisations and the resources available to tackle Internet 'malware (malicious software) are likely to be radically different from larger enterprises, however, a security breach is far more likely to have a devastating effect on the revenues, or even the survival of a start-up or small business.

This guide presents some simple but effective steps that you can take, to ensure that you keep your valuable business assets and customer data secure. Use the top-tips presented both when you first start your business and also as a reference set, perhaps referred back to every three months or so, to ensure that you are following best-practice and doing everything you can to keep your company and your employees safe online.

Business basics:
Three essential steps to protecting your business

Securing your business from Internet malware is a relatively simple matter, but it does require some forethought and a small investment in money and time. By taking action now, however, the time and cost will be more than offset against the potential lost revenues and wasted management time in dealing with security issues that are likely to occur at a later date if you are not properly secured.

When thinking about online security for your organisation, consider the age-old medical adage: "prevention is better than cure".

The essential steps to take can be broken down into three categories – Policy, Technology and Process.

Policy

1. Decide whether computers, laptops and software are to be supplied by your company, or by your staff – and reflect these decisions in your policies, purchasing and processes
2. Document a simple acceptable-use policy for any computer that is used for company business or media that is used to store or transport company data
3. Create an acceptable password-strength policy and ensure that all computers and other IT equipment are password protected
4. Require that all security incidents are promptly reported and managed to a business stakeholder

Technology

1. Ensure all operating systems and application software are updated with the latest security patches as they are developed – preferably using automatic update technology
2. Ensure all computers have an up-to-date security software suite on them
3. Every computer should have its own firewall software, in addition to any premises based network firewall you may be running
4. If managing your own file storage and email servers, ensure these are also running up-to-date security software

Process

1. Ensure all staff receive basic online security training and instruction in your policies
2. Ensure regular backups are taken of all company files, data, email and other systems
3. Change all passwords regularly, especially when an employee or contractor leaves the company, and in particular change administrator passwords or shared passwords to centralised networks or systems
4. Take security breaches seriously – isolate any compromised systems from the network and involve an IT security professional if necessary to ensure the malware is fully removed

IT Security Policy

This section provides more detail on the key elements of an IT security policy for smaller businesses

As a small business you are unlikely to overly worry about lengthy documented policies, however most small organisations do at least have a simple 'Staff Handbook' – rules for being part of the company – to supplement employment letters and contracts, if only to keep themselves out of the employment courts!

The Staff Handbook is an excellent place to also put your key policies relating to the use of IT equipment and company data, whilst most Staff Handbook templates you can download from the Internet or acquire from a lawyer include basic provisions in this area.

You should however make sure that the template provisions for the IT security section suit your needs, and as such, you should consider the following key elements.

> "The Staff Handbook is an excellent place to also put your key policies relating to the use of IT equipment and company data"

Company vs. Personal equipment

Are you going to provide all of the PCs and laptops that your employees and contractors will use?

Many larger companies do not allow staff to use their own computers on the company networks or for company business, however, as a smaller organisation this may not be practical for you – particularly if you frequently use contractors.

If you can supply all of the IT equipment then you are in a position also to define and supply the software that is allowed to be run on that equipment.

If you are going to allow some permanent or temporary staff to use their own equipment then you will need to decide if you are going to supply software for their use, or again, require them to source their own.

If employees are to source their own software then you should supply a list of acceptable software for use on company business, and require those staff to run a security software suite and keep all software up to date – as you would with your company owned computers. Remember, that employee owned equipment is going to be connecting with your secure networks and sharing your sensitive company files and information with your other staff, suppliers and customers.

Also be aware that if employees use software that hasn't been properly licensed, often the software vendor then has a claim over any assets produced using that software – so make sure your policy guards against employees sourcing and using pirated or unlicensed software.

If you are going to supply software for use on company owned equipment, make sure your policy states that you will supervise its removal when the employee departs the company.

Implementing a security policy

This section provides further information on how to execute a successful IT security policy

Acceptable Use

The key decision here is to decide whether employees may use company equipment and software for personal use.

Most companies allow personal use, as it is both too impractical and frankly, too de-motivating to disallow it.

However, you should at least have a policy on disallowing the installation of software that is not required to fulfil company functions, whilst of course you should disallow the viewing or preparation of content that might offend others. Remember, the vast proportion of Internet viruses and spyware are hidden in documents, images and videos that are designed to make users want to open them.

Also, make sure you set the rules on the storage of files and company information on removable media, such as USB/Flash drives, external hard disks and writeable CDs/DVDs. All too often company assets are lost or leaked because care is not taken with such devices or the information on them is not encrypted and password protected.

Password policy

Short passwords, or passwords comprising just a word or two are easily broken - or even guessed – by human or automated hackers.

A good 'minimum-strength' password should be at least 8 characters in length and should be a mixture of letters, numbers and perhaps one other character, such as an apostrophe, exclamation mark or dollar sign.

Any passwords that grant administrator access to equipment should be at least twelve characters and appear seemingly random to the human eye.

Finally, ensure your password policy makes it a company offence to share personal passwords with anyone else, whether inside or outside of the company, and also to provide shared/ administrative passwords with anyone who has not been authorised by the company directors.

Reporting of Breaches

Everyone gets a computer virus or potentially loses company data once in a while – however, too often staff feel guilty about reporting this, yet their silence makes matters worse as either the malicious software then spreads, or the data loss becomes public and a threat to the companies reputation or intellectual property.

Go easy on staff responsible for any unintentional security breach, as long as they have followed your policies, but make the non-reporting of an incident a serious contractual breach.

It is essential that you know immediately of any security attacks or data loss, and take the appropriate technical and public relation steps to deal with them.

"The key decision here is to decide whether employees may use company equipment and software for personal use."

Security Software Technology

This section provides an overview of the technical steps you can take to ensure your business stays safe online

Everyone knows they need 'anti-virus' software on their computers, whilst unfortunately anti-virus technology alone only goes some of the distance when it comes to putting up barriers between your equipment & files and the Internet malware that now exists.

The free or open-source software that may be appropriate for home users is usually not comprehensive enough for most business needs, whilst products used by larger organisations often require technical infrastructure and IT support skills that aren't available in smaller companies – so think carefully about your needs and the range of security software that is right for your business.

Operating System and Application Updates

Malware only has two real ways to execute on a user's computer: either by deceiving the user into manually running it, usually by pretending to be something more friendly or inviting, or by automatically running through exploiting software holes or 'bugs' in the operating system, Internet browser, email software or other applications installed on the PC.

Commercial vendors of operating systems and applications spend vast sums of money to ensure that they learn about new holes found in their software as soon as hackers and criminals find and exploit them, and then on promptly fixing or 'patching' those holes.

It is therefore extremely important that you keep all of your company's and employees' computers up to date with the latest service packs and patches, and if you don't have dedicated IT staff constantly learning about new patches released and applying such updates, that you automate the process.

Most commercial software has an auto-updating facility which should be enabled. However, be aware that often open-source software does not, as typically new updates cannot go through the rigorous testing processes that commercial vendors use to ensure cross-software compatibility.

Therefore, if you are going to use any open source operating systems or software on your company PCs or servers make it at least one employee's job to be watching for new software updates, testing them for compatibility when they are released and then notifying all other employees to install them.

"The free or open-source software that may be appropriate for home users is usually not comprehensive enough for most business needs"

Server Security Software

If you use hosted or 'cloud-based' file storage services, email services or Intranets then your server security should be being taken care of for you.

If however you have any servers of your own then it is essential that you run security software designed for the operating systems and email software that you use.

If any computers on your network are compromised by malware, there is a good chance the first thing that malicious software will do is try and replicate itself across any file servers it can find; whilst a good email server security product will guard against viruses, spam and phishing attacks before they ever get to a user's email box where they might be opened.

You also of course owe it to your suppliers and customers (morally, if not also legally) to ensure that any email you send through your servers is free of malware – whilst a compromised email server may even be used by Internet criminals worldwide to distribute their wares.

Online Security Software

A comprehensive security software package will protect you against viruses, spyware, phishing attacks (website links that take you to sites other than the one you think they are taking you to) as well as provide detection and prevention for activities that apparently legitimate software on your computer may be performing that perhaps it shouldn't – i.e. it will analyse and detect aberrant behaviour of software that might have been compromised by malware.

Consider the detection methods in the software that you use. You want malware detected as soon as it is received in your company email software, your instant messaging product or through an Internet Browser download ... you don't want to risk that malware actually been opened or run.

If your company operates primarily from a single location, consider remote-administration features that will let you ensure all security software on every computer is up-to-date and that reports centrally if a potential breach is detected.

Make sure your security software updates itself regularly and automatically – anti-virus, anti-spyware and anti-phishing products are only as good as their last update.

Finally, consider the support and assistance you get as part of your chosen security software suite. Most small businesses can't afford dedicated IT staff and, however expert your team is, they simply can't afford the time to learn how to deal with every security threat that might arise.

Computer based Firewall Software

Many people think that having a company firewall, perhaps as a separate device, or perhaps as part of their Internet router, is adequate firewall protection.

However, router and appliance firewalls are typically less restrictive than PC based firewalls, as they typically can't understand the applications that an individual employee needs to run and why each application may or may not need access to (or from) the Internet – so most 'border' firewalls are configured to allow pretty-much any web, email, chat, voice, video or gaming traffic through.

You should strongly consider installing a software based firewall on each employee's PC as it is only there that each individual application being used can be considered, first by the computer, and then by the firewall software asking the user, as to whether or not that software should be able to exchange data with the Internet.

Information Security Processes

This section covers the actionable steps you and your staff need to be taking on a day-to-day basis to ensure that your company's information assets are protected

Having information security policies and using good online security technology gets you a long way towards keeping your company's electronic assets safe. There are however activities you need to carry out manually to protect against data loss.

Large organisations will tend towards the risk management and mitigation processes defined by worldwide information security standards such as ISO27001, however, as a small business you are unlikely to have the time and resource to address such a heavyweight suite of measures, so as a minimum should look to carry out as minimum the following set of procedures – although, it is worth going the extra mile and considering many of the guidelines in ISO27001 if you are running an online business or if your organisation is governed by a regulatory body.

Security Training

Most employees don't need to be security experts, but don't underestimate the lack of basic IT knowledge most IT users, even those that come from other professional environments, will have when they join your company.

Security Training doesn't need to be rigorous, but a one-hour session on your IT policies and on best practice when it comes to IT security can go a long way towards keeping your information assets safe.

Make sure you teach staff to only open files that come from a trusted source and to recognise and avoid executable files they may inadvertently download or receive through email or instant messaging software.

If you don't have a centralised management system and IT staff to ensure that all of your users' PCs are up to date with the latest operating system, application software and security software patches, then you should train your staff to check and update their software on a regular basis. If you don't have the in-house skills to teach this, then any of the cheap, or often, government funded courses that target the European Computer Driving Licence qualification, or the ITQ, do cover off these basics.

If staff need occasional 'Administrator' access to their PCs in order to install new software, make sure they only use those administrative privileges when appropriate – and use a more restricted user-level account for day-to-day activities.

Regular Backups

Consider the damage that could be done to your company if information was lost or if unavailable for a lengthy period of time. You may no longer be able to operate your business, or you may lose reputation with your clients if you no longer have the information they expect you to hold.

Taking regular backups of your company information is essential and as a company director you are now legally accountable if your business is damaged through loss of data.

Wherever possible mandate that files, emails, source-code and other information assets are stored centrally on servers you control, in order that you can be responsible for backups.

If you use an email server or database software, make sure you use backup software that is designed to understand those server programs as it backs them up, so that, if necessary, you can restore individual emails/records or partial datasets, rather than an entire point-in-time backup.

Similarly, if you build software products for a living, consider using specialised source-code control software or online services that again, understand the complex structure of those information assets.

If employees need to work away from your company servers for any length of time and are therefore unable to take advantage of your centralised backup facilities, make sure they are provided with facilities, either securely online or using specified backup devices or media, to ensure regular backups of their data and activities can be taken.

Data storage

This section covers the actionable steps you and your staff need to be taking on a day-to-day basis to ensure that your company's information assets are protected

Data storage is relatively expensive, so it is worth spending time thinking about your backup model and how long you need to keep each backup for. Many companies elect to use the 'Grandfather, Father, Son' model whereby a different backup is taken every day, then once every week, one backup is retained as the weekly backup, but all other backup media is re-used for the next week's archiving. Then, each month, one of the weekly backups is taken out of rotation indefinitely to ensure that you have permanent point-in-time records of your data.

Regular backups should be stored off of your company premises, in case you suffer a catastrophic premises-based disaster, or in case some malware infects all of your local facilities; and increasingly there are Internet providers who will securely store different types of backup for you 'in the cloud' rather than you necessarily having to worry about taking backup media offsite for secure storage.

Finally – the golden backup rule – test it! There is nothing worse than relying on a backup system, only to find that when you need to recover the data you are missing something crucial. It does take time and effort to restore and check backup data, however, it is your business that you are protecting.

Dealing with Security Breaches

Despite your best efforts, sometimes you and your employees may fall foul of the clever malware that continues to be developed by Internet criminals.

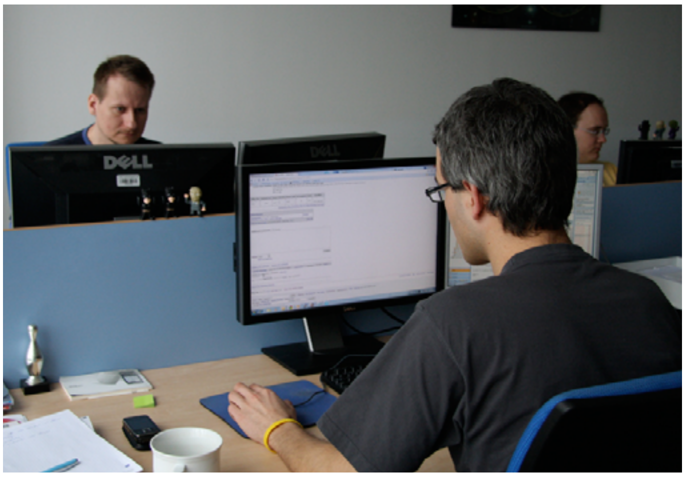
Hopefully this will be detected by the PC user and reported to you immediately, according to your policy and if there is any potential that malware has been installed on a user's PC, the first rule is, disconnect that computer from all company networks as well as from the Internet.

A 'Trojan' or Spyware on a PC may continue to download more Internet nasties or exchange information for as long as it has a World Wide Web connection, whilst many viruses and 'worms' will continue to seek out places to hide itself for as long as it is on your network.

You must then make an assessment of the damage. What other company equipment, information stores or data backup might have been compromised? What important company information might have been lost? What sensitive company information might have been leaked? Who else inside and outside of the company do you need to notify and with what communications?

Once you have taken every step to limit the damage and recover any lost information (or reputation) you will then need to recover the comprised computer(s).

If you are in any doubt during the recovery process (we can't all be IT security experts after all), find an expert to help, perhaps though the support service you have contracted as part of your online security software license, or perhaps through a local computer repair outlet – before you declare the problem technically fixed and allow the computer to be re-attached to any network or again used for company business.



Changing Passwords

Generally you should require that all users change their passwords to any system used for business purposes every month. If a security breach has occurred through password discovery, but remained undetected, this will at least determine a timeframe after which you may be protected again.

Frequently changing passwords also helps protect against the password sharing, that despite your policies, will occasionally occur. At least if an (ex-) employee or contractor comes to know of a password that they shouldn't they will be locked out again after a month.

Where you have a centralised server that manages some security elements on each computer through a 'group-policy' then you should force monthly password changes, but otherwise, you will need to continuously re-enforce to your staff the need to change passwords every month.

It is particularly important to change passwords on all systems after a key employee leaves your service – it is unfortunate, but ex-employees may often be more disgruntled than they appear, whilst you never know when they might be going to work for a competitor.

Don't forget other IT password when you are going through your change process – Wi-Fi (Wireless Network) passwords are all too often forgotten, yet they are probably the most shared of passwords when it comes to visitors to your company, whilst of course, often they can be used just-outside of your company's physical premises without you necessarily noticing.

Summary

Getting a business off the ground and then keeping it running smoothly is undoubtedly tough and the threats posed to our businesses' computers and electronic information in this online world are yet another concern for every small business owner.

However, following the simple steps outlined in this paper, adapting the policies, technology needs and processes to your own venture, should provide you with the security and protection you need to operate with the minimum of effort and cost.

Founded in 1991, AVG is a leading international developer of Internet threat protection solutions for businesses and consumers. AVG protects more than 110 million computer users around the world. The company has offices in Europe and North America and employs some of the world's leading experts in Internet security, specifically in the areas of threat research, analysis and detection. AVG's award-winning products are distributed globally through resellers and over the Internet as well as via third parties through Software Development Kits (SDKs).

AVG SMB group at:
bit.ly/AVGSMB

Become an AVG Fan at
facebook.com/avgfree

Read our blogs at:
blogs.avg.com

Follow us at
twitter.com/officialAVGnews

Become an AVG affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

AVG AT WORK