

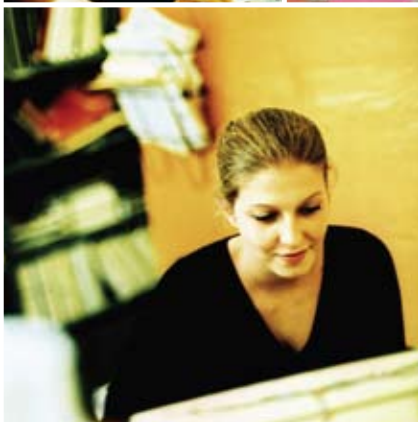


Australian Government

Department of Broadband,
Communications and the Digital Economy

E-security for your business

www.staysmartonline.gov.au



Risks to your business online

The internet provides great opportunities for business to reach new markets and more customers than ever before, but unfortunately, with those opportunities come some e-security risks. When online, unwanted intruders can:

- install malicious software such as spyware and viruses, which can steal sensitive business information as well as slow down your computer
- intercept financial transactions, steal credit card details and access customer information
- steal your download limit without your knowledge and at your cost
- take over your website and modify it
- steal sensitive business information from your business by using a portable device such as a USB.

Fortunately there are simple steps you can take to improve the security of your business when online. There are **some things you need to have**, and **some things you need to do**.



What you need to have

Just as you have locks and alarms for your business premises, there are some simple things to install and activate on your computers to help keep your business secure online.

Security software can identify and block malicious software, like viruses, worms, trojans or spyware attempting to access your computer. Different packages have different levels of coverage—some software only blocks viruses, while others offer more comprehensive protection against a wider range of threats.

You can buy security software packages from computer and office supply stores, and many can be downloaded from the internet.

The most important thing is to keep software up-to-date, so make sure to switch on 'auto updates' function when you install your software.

A **firewall** is software that monitors information going in and out of your computer. It is important to have a firewall installed to ensure that you can control what is being installed on your computer.

A firewall may have been installed on your computer when you bought it. Make sure it's switched on. Some security software packages also include firewalls.

You can also choose **smart settings for your internet browser**, which add another layer of security. Depending on the security level you choose, your internet browser can alert you when you are visiting unsecure webpages, or help to block unwanted pop-ups.

The higher your levels are set the more secure your internet access will be, but you may have fewer options and functions available.

What you need to do

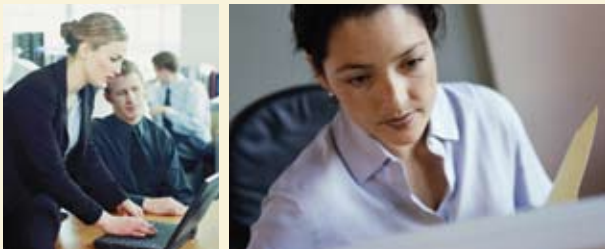
Put into practice basic habits to help keep your business secure online.

Develop a culture of e-security in your business.

Have measures in place to educate your staff about e-security. This includes placing e-security on the agenda at your staff meetings or developing an e-security policy for your business.

Prevent data theft from your system. There are lots of common consumer items including USB storage drives, MP3 players and digital cameras that can be used to store computer data. In many cases, these devices can hold enough data to copy whole databases and hard disks. Employees may also be able to download and copy sensitive information if they have remote access to your computer system.

- Conduct a risk assessment for your business—look at the information you have stored on your company network and evaluate what could happen if employees took it from your office.
- Work out which staff need access to what information—you may want to limit some employees' access by protecting sensitive information with passwords.
- Have clear rules about employee handling of sensitive data.
- Ensure that staff remote access privileges are disabled once they leave the business.



Don't forget about e-security when you're on the road. Protect your office networks and the information stored on mobile phones, PDAs and laptops from access by unauthorised users.

- Make sure devices are secured by strong passwords and not set to log-on automatically. Ensure passwords are not written on or affixed to devices.
- Develop protocols that can be actioned if equipment gets lost or stolen. Keep a list of equipment serial numbers and notify police and insurance companies immediately.
- Think about the sensitive data that might be stored on a missing device. Change all the passwords you use online, and cancel credit cards if information about them is stored on the device.

Use strong passwords and change them regularly.

A strong password should:

- have at least eight characters—14 or more is even better
- use a mix of upper and lower case letters, numbers and symbols e.g. a very secure password would be something like this: j>kb*D-94x.

Keep your software up-to-date. Software manufacturers routinely identify vulnerabilities in their products and issue 'patches' to address them, which can help to protect your computer. You can set your computer to check for updates regularly.

Back-up your data so you can retrieve your business information if your computer is damaged or compromised. Store the back-up copies in a safe location away from your computer systems i.e. away from your home or business premises.

Ensure your wireless internet connections are secure. If you are using wireless internet:

- change the default password from the manufacturer
- ensure you have encryption turned 'on' in your wireless software settings—this will make it very hard for anyone who somehow manages to intercept your transmitted data to make sense of it.

Ensure your VOIP connection is secure.

Voice over internet protocol (VOIP) allows you to make cheap calls over the internet. If you are using VOIP:

- set-up your service to allow connections only from people you know and block others
- if your service includes a public profile, don't include any sensitive, private or confidential information.

Turn off your internet and VOIP connections when you aren't using them.

Educate your family about secure behaviour online.

Home-based businesses often share their computer resources with family members. Make sure that your family members also follow your security measures when using the business computer.



For more information

For more information about how to keep yourself and your family secure online, visit the Australian Government's Stay Smart Online website, www.staysmartonline.gov.au

You can also subscribe to the Stay Smart Online Alert Service. You'll be sent regular emails to help keep you up to date with the latest e-security risks and provide useful advice about how to avoid them.

For more information about the types of online scams, visit Scamwatch,

www.scamwatch.gov.au

To learn more about how to protect yourself against identity theft, visit Protect your ID,

www.protectfinancialid.org.au

Always remember the five simple steps that need to be followed

1. Install, update and use your security software.
2. Use strong passwords and change them regularly.
3. Be careful when sharing personal information online.
4. Think before you click—if it looks too good to be true, it probably is!
5. Be smart and stay informed—visit www.staysmartonline.gov.au, and sign up for the new Stay Smart Online Alert Service.

www.staysmartonline.gov.au