Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

OCTOBER 2012

(U) **LEGAL NOTICE:** THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

# Top security tips for the home user

There are a lot of things to think about when it comes to security on your computer. In the same way that you are careful about how you use your computer at work, why not have the same level of security at home? So what are the most important things that you can do to improve the security of your personal devices and the security of your information? Here are our eight top tips.

1. **Update your software.** Recently Skype conducted a survey in Europe that found that at least 40% of people do not update their software. Most people think it takes too long or they don't understand why it is important. Did you know you can set your computer to apply most updates automatically in the background so you do not have to remember to check? **Why is it important?**

   a. New versions of software are released to address security problems that have been found. Updating your software ensures you take full advantage of all the security upgrades.

   b. If you do not update the software you can put your computer at risk of viruses and other problems because the software is no longer supported.

2. **Use anti-virus software**. This means it should be from a reputable company and you need to keep it up-to-date. Anti-virus software does not have to be expensive. Many companies have anti-virus software that is free to download from their websites. **Why?**

   a. Anti-virus companies spend their time ensuring their software helps stops known viruses. If you have a current and up-to-date version, you can be assured that the software is looking out for problems and blocking them.

3. **Think about your online presence**. Check your privacy settings on sites like Facebook to make sure you know who can see your information. Privacy settings sometimes change after functionality is added to the website so it is important to check them regularly. It is best not to put personal details on to the internet unless you are sure they are safe. Consider checking the information that others put on the internet about you. While some information might not seem important, many pieces of information can be put together to form a picture about you. **Why?**

   a. If your personal information is accessible to others it can be used against you. This could range from something as simple as sending you spam emails to something as serious as accessing your accounts and deleting all your information or even identity fraud.

4. **Be suspicious of unsolicited phone calls or emails.** Do not follow instructions from someone who rings to tell you your computer has 'technical problems', unless you can prove they are from your internet service provider. You should also check out an email before you open it or click on any attachments or links. If someone

has sent you an email that you think is a bit strange or you do not know the person sending the email, consider deleting it before you open it. **Why?**

a. Unsolicited emails and phone calls are trying to get you to do something that will benefit someone else. It might be just spam trying to get you to buy things, or it might be trying to get you to access something that will put a virus on your computer or give others access to your information.

5. **Back up your data.** This means saving all your files onto a different device such as a USB, external hard drive, cloud based service or DVD. **Why?**

a. If you have a problem with your computer and it needs to be reset or even replaced, you will still have access to your information.

6. **Use legitimate software.** You should always use legitimate software that you have purchased from a vendor or downloaded from the company's website. **Why?**

a. If you use pirated copies you open up your computer to viruses that you may not know about. The software itself may contain a virus, or it won't be supported by the vendor, meaning you won't receive regular security updates.

7. **Set strong passwords and use different passwords for different accounts**. You should have passwords set for your computer and any login account that contains a combination of upper and lower case letters, numbers and symbols, wherever possible. It is a good idea to change your passwords regularly. Try to use different passwords for different accounts and most importantly do not store an unencrypted list of your passwords on your computer. **Why?**

a. A password that is strong and changed regularly makes it harder for people to access your information.

b. If you use the same password for all your accounts and one account is compromised, the person accessing your account is more likely to be able to guess all your other passwords and access those accounts too.

c. If you store an unencrypted list of your passwords on your computer and someone gains access to the computer, they then have all your passwords.

**8.** **Do not lose your device**. It may sound logical but one of the biggest risks to your information is from a lost or stolen device. So make sure you know where your tablet, phone or laptop is at all times and avoid leaving them unattended. **Why?**

a. If someone gets your device, they may have access to all your information and plenty of time to access it.

## Further Information

To get further security information on these tips and others, see:

www.asd.gov.au

www.staysmartonline.gov.au