

Stay Smart Online Alert Service Newsletter

October 2008

Overview

The purpose of the Newsletter is to provide general advice about online security issues and help you learn to better manage the security of your computer and information when online.

The Newsletter provides additional information about the threats and software bugs which were reported during the period, or about other threats to be aware of.

Feedback

Thank you to those subscribers who have provided feedback to our alerts, advisories and newsletters. We are very interested in your feedback and where possible take on board your suggestions or requests. In this newsletter we have responded to two new feedback questions.

In particular, thanks to those subscribers who completed the recent online survey, which is now closed. This is very important to help us improve this service. The survey will be conducted twice a year so there will be other opportunities to provide your feedback at a later time.

Common online threats

Malicious software*

Recently, we saw a few [fake emails pretending to be from Microsoft](#) sent to Australian internet users.

The emails contained an attachment which was really malicious software. If users opened the attachment and installed the software[†], the malicious software would steal all usernames and passwords from the computer and a range of other personal information, monitor users' online transactions and send the information off to criminals.

* Malicious software, or 'malware', is a general term to describe a variety of harmful programs such as viruses, worms, key loggers, trojans, root kits, etc. The worst type of malware is produced by criminals and is designed to steal your personal information, your passwords and computer resources for fraudulent purposes.

† In some cases, just opening the software may result in the software being installed automatically.

Fortunately, most anti-virus products recognised the attachment was malicious software, and if users had up to date anti-virus software, they probably would have received a warning from the anti-virus program, if they received this email.

The case is a good example of why it is important to exercise caution before opening email attachments or question whether the email is really from the sender that it claims to be. It is easy to falsify “From” fields in email headers.

Harmful PDF files‡

Recently, there have been cases of harmful PDF files being sent to people by email as a way to compromise their computers. It is possible for criminals to exploit bugs in software programs to make the programs behave in ways that can be harmful to the security of your computer.

This is why it is important to keep software programs like Adobe Reader up to date. The bugs described above occur in version 7 of Adobe Reader. If you have not got [the latest version of Adobe Reader](#) installed, which currently is version 9.0.0, now is the time to update this software. More information about Adobe Reader can be found in the following SSO reports:

- [SSO-AL2008-005 – Security update for Adobe Reader](#)
- [FAQ Newsletter PDF file crashes](#)

To check for updates, open Adobe Reader, go to the Help menu and select “Check for Updates...” in the menu list. You will need to be in an account with administrator privileges to install the updates.

Phishing

The following is an example of the type of words you might read in a phishing (scam) email.

Hello

This is the Webmail Administrator. There have been changes to the web accounts recently. Please send me your email addresses and passwords. If you fail to do so your web mail will be terminated.

Thank you.

‘Phishing’ is a form of scam that involves criminals sending potential victims an email with a link to a fake web site or which requests personal or secret information be sent to an email address. Both the email and web site, if applicable, pretend to be from a well known or reputable organisation or person you might normally trust.

The problem is very common and for this reason we have written a [Fact Sheet on Phishing](#). The [Fact Sheet](#) will help you recognise the signs to look for in a phishing email and learn what free technology tools can help you detect it.

‡ A PDF file is a type of file that cannot be changed once it has been created. This Newsletter is a PDF file. PDF files are read with the Adobe Reader software.

Ultimately, common sense will be your best protection. The main thing to remember is NEVER to provide your username and password in response to any request made via email, no matter what the person says will happen if you fail to do so. This is a scam.

Typically, phishing emails and phishing web sites aim to trick people in to giving criminals their usernames and passwords for their online bank accounts and/or email accounts. Criminals then use the usernames and passwords to log in to the bank accounts and transfer money from the account. In the case of email accounts, the criminal can gain access to a lot of your personal or work email, can send emails to others pretending to be from you, including spam email.

What you can do

Follow the advice in the Stay Smart Online [Phishing Fact Sheet](#).

Security tip

Mozilla Firefox 3.0 vs Microsoft Internet Explorer 7 (MSIE)

Mozilla Firefox and Microsoft Internet Explorer are both popular web browsers. [§]

Regardless of your own browser preferences, it is important to know that if you have Windows XP or Windows Vista (or another Windows operating system) installed, the Microsoft Internet Explorer (MSIE) browser has the advantage that it does not require you to run with administrator privileges in order for the automatic updates of the MSIE browser to take effect.

However, the Mozilla Firefox browser will not automatically update itself if you are operating from an account with limited user privileges. You will need to log into an account with administrator privileges to do so.

It is recommended that for general use, users operate from a limited user account to minimise the risk of malware infection. For more information refer to the [Factsheet on setting up a limited user account in Windows XP](#). The information is also relevant if using Windows Vista.

If Mozilla Firefox users need to log in separately as an administrator, they may be slower to update their software or forget to update it (unless they are reminded to update the software through the Stay Smart Online Service).

On the other hand, if users generally operate from an account with administrator privileges this increases their online risks in other ways by making them more vulnerable to malware attacks.

§ A web browser is software that is used to access web content, for example any web site or web-based email.

Remember – just because you have up to date anti-virus software installed this is not a guarantee the software will detect all of the very latest malware in circulation. So taking other precautions, like operating from a limited-user account, will help reduce your online risks.

Feedback questions

This section is devoted responding to feedback or questions submitted by people who have subscribed to the Stay Smart Online Alert Service.

Does installing more than one software (personal) firewall on my computer provide better security?

One subscriber asked if installing two personal (software) firewalls provided better security. The firewalls were Microsoft Windows Firewall, which comes built in with both Windows XP and Vista, and Zone Alarm.

In general it is not appropriate to have two software firewalls installed on the same computer at the same time. The greatest problem with this approach is that the two firewalls may conflict with each other and cause problems with connectivity and system functioning. This in turn may mean that one or both firewalls fail to function properly.

Of course, as mentioned in the [September Newsletter](#), if you are managing a small network for your business, it IS good security practice to have a hardware (appliance) firewall at the network gateway as well as one software (personal) firewall installed on each (client)** computer in the business.

The Windows Firewall is a basic, though effective, software (personal) firewall . The Zone Alarm firewall is also effective but has more settings that can be modified. The Windows Firewall is automatically included as part of the Windows XP or Vista operating system. The Zone Alarm firewall has two versions – one that is [free for non-commercial use](#) and a commercial version.

Information about configuring the Windows Firewall for Windows XP with Service Pack 2 can be found [here](#). The information is also relevant to Vista even though the firewalls are slightly different.

For more information about firewalls and their strengths and weaknesses refer to the [September Newsletter](#) .

**A client computer is one that people use to store their files, read email or surf the web. You would read this newsletter from a client computer. A server is a more powerful computer that is used to 'serve' information to many client computers. For example, a client computer (such as the one you are using) connects to a web server computer in order to view a web page on that web server. The distinction is important as there are different approaches to protecting different types of computers.

Can my anti-virus software detect malicious software in zip file attachments sent by email?

Yes. Anti-virus software scans the content of email attachments to look for any potentially harmful malicious software (such as viruses, worms or other malware). The only time that anti-virus software is unable to do so is if the zip file is password protected.

But this does not mean you should automatically open every zip file or email attachment you receive.

Care should always be exercised when opening attachments in 'suspicious' emails or from people not known to you, whether the attachments are zip files, PDF files, word documents or any other type of attachment. A lack of any warning by the anti-virus product may mean either that:

- There is no malware and it is safe to open; or
- The email/email attachment contains malware but the anti-virus product has not got the 'signature'^{††} which allows it to detect the malware and warn the user.

The latter situation arises because there is always a time lag between when criminals send new malware out by via email and on web sites and when anti-virus companies find the new malware and develop new signatures for their anti-virus products. There is a further lag between when those signatures are developed by the vendor and installed by customers in their "updates".

Page 21 and 22 of the [AusCERT Home Users Computer Security Survey 2008](#) explains the problem with lags in malware detection by anti-virus products further.

Disclaimer

This Newsletter has been prepared by AusCERT for the Department of Broadband, Communications and the Digital Economy.

The information is intended for used by home users and small to medium sized businesses and is general information only and not intended as advice and was accurate and up to date at the time of publishing. The material and information in this newsletter is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. In any important matter, you should seek professional advice relevant to your own circumstances.

The Commonwealth, AusCERT, and all other persons associated with this Newsletter accept no responsibility or liability for information either included or referred to in the Newsletter. No responsibility or liability is accepted for any damage, loss or expense incurred as a result of the information contained in the Newsletter, whether by way of negligence or otherwise.

†† A 'signature' is a like the fingerprint of a malicious file. In the same way that a human fingerprint can uniquely identify an individual person, a file's signature uniquely identifies it as a type of malicious software (such as a virus). The anti-virus software looks for signatures in email attachments and files. If it finds a signature then it is able to warn the user that the email attachment or the file is harmful. If the particular signature is not present then it will not recognise the file as potentially harmful. Every time the anti-virus software is updated, the list of signatures for malicious software it can detect grows.

The listing of a person or organisation in any part of this site or Newsletter does not imply any form of endorsement by the Commonwealth of the products or services provided by that person or organisation. Similarly, links to other web sites have been inserted for your convenience and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

Please note that material in this Newsletter, as the case may be, includes views or recommendations of third parties, which do not necessarily reflect the views of the Commonwealth, or indicate its commitment to particular course of action. Material on this site or in this Newsletter may also include information provided by third parties. The Commonwealth cannot verify the accuracy of information that has been provided by third parties.