

Stay Smart Online Alert Service Newsletter

May 2009

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.

Common online threats

Question: What happens if your username and password is captured and a criminal changes your password and locks you out of your own email account?

Answer: It can damage your business.

This is precisely what happened recently to an Australian business woman who was fooled by a phishing email. The woman runs a small business and had set up a Hotmail account to handle her business needs and personal email.

The Hotmail account (also known as Microsoft Live) gives access not just to emails but the ability to create personal and business documents (such as Microsoft Office Word, Excel (a spreadsheet program) online, make appointments using an online calendar and access instant messaging contacts.

The woman was fooled by a phishing email which pretended to be from Microsoft MSN Hotmail. The phishing email claimed to have been from MSN Hotmail and reported that they were doing maintenance on all MSN Hotmail accounts and were closing accounts that were not being used.

The email asked the recipient to provide passwords for the accounts to prevent the account being closed.

Within a day of providing the passwords the woman was contacted by telephone by one of her clients to check on an email that had been sent from the woman's Hotmail email accounts. At this time, the woman tried to log into her Hotmail accounts only to find the passwords had been changed and she could not do so.

The criminal who sent her the phishing email, had used her password to access her Hotmail accounts and began sending out emails from her Hotmail accounts, pretending to be from her. The emails claimed the woman was trapped in London and urgently needed money in order to return home.

The following wording was used in one of the fraudulent emails sent to the woman's contacts:

Subject: RE: Urgent Help

To: <one of the woman's email contacts>

Hi <name of the person>, I'm <the name of the business woman>. Please I really need your help, with whatever you can afford for me at this point will be highly appreciated. I need to settle the hotel bills and get my ticket back home. Everything is really going bad for me out here, I am just so frustrated. Like I told you earlier. I misplaced my wallet containing my credit card and money. Please I will repay you back as soon as I get home. Just assist me send the money through Western Union, to my details. Then you can get back to me with the MTCN reference no and the amount sent. So I could pick it up over here. Thanks.

Other email contacts received similar requests for money.

What was the impact of this attack?

The attack caused the following damage to the woman's business:

- loss of confidentiality and privacy of her personal and business information;
- damage to her and her business's reputation
- disruption to her supply chain
- lost access to her own business contacts and documents
- lost business.

It is also quite possible that some of the recipients of the fraudulent emails (that asked for money) sent money as requested. So the victims may have included the woman's clients and friends who may have lost potentially thousands of dollars, if they believed the email was really sent by the woman they knew.

How to prevent this type of attack?

It is very easy to fall victims to these types of attacks because many of us trust the organisations that appear to be sending the emails. **It is important to understand that it is very easy for criminals to create emails and web sites that look like they are from or established by legitimate organisations** – so do not automatically trust or assume the request for 'passwords' or similar personal financial information is legitimate. If such organisations are asking for sensitive information such as this then this is a sign the request is fraudulent.

Being aware of phishing scams is the first way to prevent becoming a potential victim. Do not provide your username and password to anyone who asks for it (or other sensitive information) – even if they appear to be legitimate organisations or legitimate reasons. Passwords need to be kept secret at all times. Read the [Factsheet about phishing](#). Another relevant [Factsheet is understanding how to verify web site digital certificates](#) before “logging in” by providing your username and password. It is possible it is not really the web site you think it is.

However, passwords can be captured just as easily by malicious software. Once a computer is infected with the some types of malware, a criminal can take control over the computer and all information and passwords on it, whether the passwords are “saved” on the computer or just typed in via the keyboard. In this case it is important to be routinely following the steps in the Stay Smart Online [Secure Computing Checklist](#).

Have you thought about the risks of relying solely on web-based email systems?

Various online companies offer free email accounts to anyone in the world. These companies include Microsoft’s Hotmail and Live email, Yahoo and Google’s Gmail. The advantages of these accounts are that they are:

- free
- they no longer just include email but give users the ability to share photographs and create documents online and make them accessible to others if you choose.
- they do not require the installation of client email program or other business software on your computer (other than a web browser). For people who cannot afford to purchase business programs such as Microsoft Office products, this can be a huge incentive as these documents are compatible with Microsoft Office files.
- they are accessible from anywhere in the world, wherever you have access to the Internet and a web browser
- access to the account (including the email other files) is encrypted, which means that emails or other content accessed via the account cannot be read by anyone in transit. But of course they can be read by anyone with the password!

On the downside, the email, contacts, photographs and documents created are stored on a database remotely (usually in another country) and the only way to access your email account is via a username and password.

If you don’t have access to an Internet connection then you cannot access the emails or the documents stored on these web-based accounts.

How to recover?

The woman wanted to regain control over her email accounts. However, sometimes it can be hard to prove who you are online when you only have a password to verify your identity. The woman was referred to contact Hotmail’s abuse email address – abuse@hotmail.com and explained the situation and hoped that they were willing to reinstate access to her account.

Also, once in control of the account, it is quite possible the criminal could delete contacts or other documents or use other personal or business information for other forms of financial fraud. In other words, the full impact of this relatively easy attack may not be known for some time.

In situations like these, if the woman had stored all her business information locally, on her own computer, instead of remotely on a web-based account then a criminal may have been able to steal information off her computer but at least she would still also have access to her contacts and business information stored on the computer.

The importance of back-ups

There are free email programs (such as Microsoft Windows Live, Mozilla Thunderbird) and free office programs (such as Sun's Star Office) that can be installed on your own computer if money is the main issue. However, there are also disadvantages with storing information locally on your own computer. Your computer's hard disk may malfunction or your computer may become infected with malware that corrupts access to your files.

Whichever arrangement you choose, the important factor is to have back-up information of your most important contacts, personal and business information.

Mobile telephone SMS scams

Most people have heard the warnings about not trusting unsolicited spam emails, but would you trust information sent to your mobile phone?

Scammers are now sending mobile text messages, like the following one:

You won \$123,000 USD, send your email address by sms text message to (+85xxxxxxx) so we shall send you an email with more information on how to claim your money.

This is a scam – if you get a text message like this, don't reply. Even if you know it is a scam and reply, you may be inadvertently replying to a high charging telephone number which has been set up by the scammer. When you view your mobile telephone bill you may be horrified at how much this simple text message cost you. The more people that reply, the more money the scammer receives.

Scams that claim you have won huge amounts of money, or are eligible to receive a large financial windfall, work by fooling you into believing the claim is true and then inducing you to send the scammer money instead!

Once the scammer has got a reaction from you, the scammer will sooner or later advise of the need to pay 'fees' associated with releasing or transferring the money to you or other problems which have arisen which can only be addressed by more fees and payments.

Victims rationalise paying the scammer with the view that their small outlay will reap a much greater return. But there is no return, just more demands – some of which may be quite convincing – for payments to the scammer. Police report that some victims will over a period of time pay out thousands of dollars in the hope of obtaining reaping their windfall – which never arrives.

The government's [Scam Watch](#) web site has more about the various scams.

New factsheets

We have prepared a number of new [factsheets](#), which explain how to detect and remove malicious software from your computer. These factsheets, which are called “You have malware – what should you do?” cover the following topics:

[Part 1](#) Use an installed anti-virus product to detect and remove malware

[Part 2](#) Use a web-based online anti-virus product/s to detect and remove malware

[Part 3](#) Use a bootable rescue disc to detect and remove malware

Parts 1 and 2 are easy and can be performed routinely whether you suspect your computer is infected with malware or not. Part 2 is an especially useful way to check that the installed anti-virus product on your computer has picked up all potential malware that may be on your computer.

Are you a new or recent subscriber?

Don't forget that the Stay Smart Online Alert Service has a web site where previous Newsletters can be read. These Newsletters often contain security tips or provide greater details about common computer threats.

Disclaimer

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

The information is intended for use 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.

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.