Australian Government Initiative
Stay Smart Online

STAYSMARTONLINE

Fake speeding ticket emails distributing ransomware

View Online

An Australian Government Initiative
Stay Smart Online

Stay Smart Online ALERT SERVICE

STAY SMART ONLINE

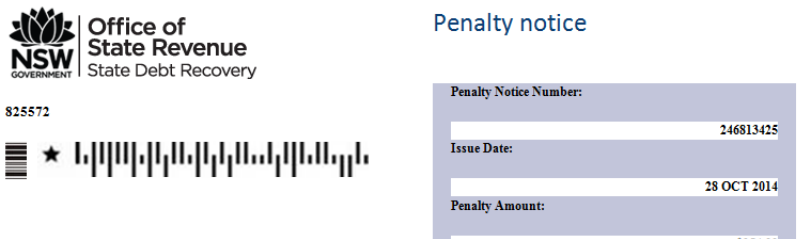
31 October 2014

Fake speeding ticket emails distributing ransomware

Australians should be wary of a new scam email campaign pretending to be a speeding ticket issued by a government authority such as the NSW Office of State Revenue.

The 'Penalty Notice' email and the website appear to be authentic, featuring convincing official design and branding and replicating official statements about the offence. The email includes an 'ACT NOW' button, this button links to a website where you are prompted to download a file containing details of a penalty notice. This file contains ransomware.

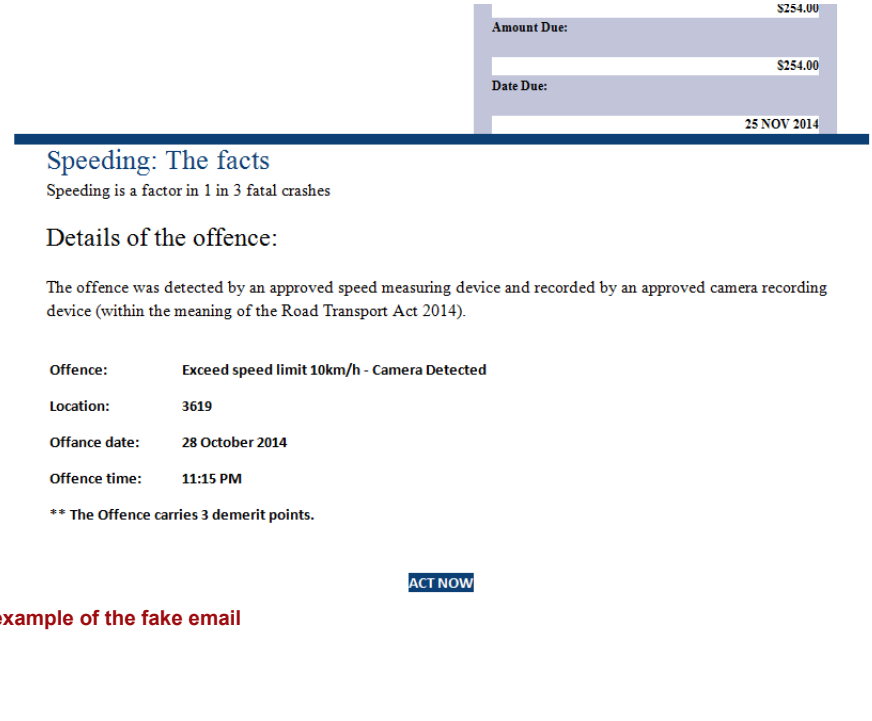
If you receive this email you should delete it immediately. These messages are a scam and the ransomware could severely impact your system.


NSW GOVERNMENT Office of State Revenue
State Debt Recovery

825572

Penalty notice

Penalty Notice Number:
246813425
Issue Date:
28 OCT 2014
Penalty Amount:



$254.00

Amount Due:

$254.00

Date Due:

25 NOV 2014

Speeding: The facts

Speeding is a factor in 1 in 3 fatal crashes

Details of the offence:

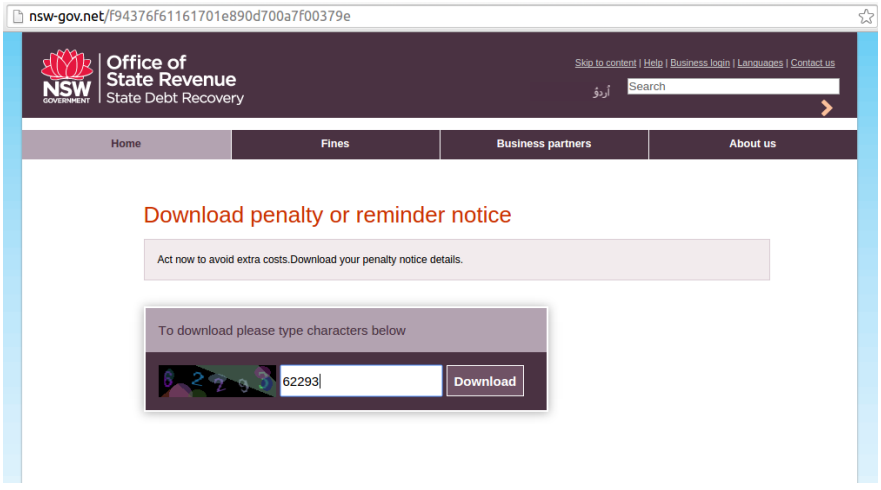
The offence was detected by an approved speed measuring device and recorded by an approved camera recording device (within the meaning of the Road Transport Act 2014).

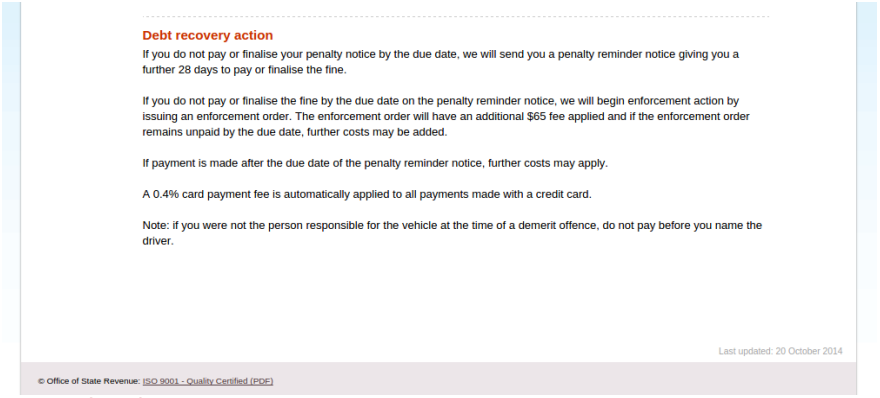
Offence:	**Exceed speed limit 10km/h - Camera Detected**
Location:	**3619**
Offance date:	**28 October 2014**
Offence time:	**11:15 PM**

** The Offence carries 3 demerit points.

ACT NOW

An example of the fake email





An example of the fake website

The scam emails and the website could easily be mistaken as authentic. Current examples circulating are generic and do not refer to the recipient's name, address, vehicle or registered owner details.

NSW Office of State Revenue has also advised it does not issue penalty notices or reminders by email.

This campaign may be linked to another recent ransomware campaign targeting Australia Post customers. It is likely the criminals may adapt or vary their approach again.

Do not click on links or attachments in a message unless you are completely confident about its content.

You can always navigate to the original website or phone the source yourself—independently of links or information in the message—and cross check its information.

About ransomware

There are many different versions of ransomware circulating and it can be difficult to identify which type you have encountered.

The most serious types of ransomware encrypt files on your computer or network using high quality encryption, rendering them useless unless you obtain the unlocking key—usually by paying the ransom. Recovery of your system without the key is virtually impossible. The best alternative solution can often be to restore your files from a clean backup, if you have one available.

Prevention is the best approach for any malware, and particularly this kind of ransomware.

The current Speeding Ticket email scams are believed to be distributing a variation of encryption ransomware called CryptoLocker.

There are also some less sophisticated types of ransomware (such as the recent police ransomware campaign) which simply blocked access to your computer or pretended to lock your files. With careful action you can remove this ransomware and regain access to your files without paying a ransom.

If you suspect your computer or network is infected by ransomware, you should seek technical advice immediately. Time is critical.

More information

Stay Smart Online's advice about avoiding scams and hoaxes.

Information provided by CERT Australia.

The information provided here is of a general nature. Everyone's circumstances are

different. If you require specific advice you should contact your local technical support provider.

Feedback
Thank you to those subscribers who have provided feedback to our Alerts and Newsletters. We are very interested in your feedback and where possible take on board your suggestions or requests.

Disclaimer
This information has been prepared by Enex TestLab for the Department of Communications ('the Department'). It was accurate and up to date at the time of publishing.
This information is general information only and is intended for use by private individuals and small to medium sized businesses. If you are concerned about a specific cyber security issue you should seek professional advice.
The Commonwealth, Enex TestLab, and all other persons associated with this advisory accept no liability for any damage, loss or expense incurred as a result of the provision of this information, whether by way of negligence or otherwise.
Nothing in this information (including the listing of a person or organisation or links to other web sites) should be taken as an endorsement of a particular product or service.
Please note that third party views or recommendations included in this information do not reflect the views of the Commonwealth, or indicate its commitment to a particular course of action. The Commonwealth also cannot verify the accuracy of any third party material included in this information.

CONTACT US
Facebook: www.facebook.com/staysmartonline
Email: staysmartonline@communications.gov.au
Web: www.staysmartonline.gov.au
You are receiving this message at the address [Email].
Update your profile preferences
If you no longer wish to receive this information, you can unsubscribe.

STAYSMARTONLINE.GOV.AU