

# It's The Season to be Jolly! **INFECTED WITH A COMPUTER VIRUS!**

Xmas is usually a time for giving...

...or in this case a time for receiving!

Every year, around Christmas, there's a significant increase in the number of infected computers. Its not that virus writers are working overtime, or the antivirus vendors are down the pub rather than curing computer virus's...

Simply put, at this time of year we're all Xmas happy, therefore more susceptible to clicking on malicious email links and attachments that we wouldn't otherwise normally go near.

Who wouldn't like to receive a festive e-card from the attractive girl in marketing, thousands of £ worth of free Xmas goodies, or to look after £1million for that nice gentleman from Nigeria?



The Grinch: Hates Xmas. Probably never infected his laptop with a virus. :/

This message was sent with High importance.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Commonwealth Bank [service@commbank.com]  
To:  
Cc:  
Subject: Commonwealth Bank - Important !!!

Notice how the email isn't addressed to anyone specific...  
This is a common trait of phishing and spam email.

Dear Commonwealth Bank client,

This is your official notification that your maestro card has been limited. We recently reviewed your card and it seems that it is linked to more than 1 accounts. Linking your Maestro Card to multiple multiple accounts is strictly forbidden and it can be punishable by law. You are now requested to provide information relevant to your Maestro Card. Commonwealth Bank will investigate the matter promptly and if the investigation is in your favor, we will restore your account.

Look for obvious spelling and grammar mistakes.

• How can I restore my account access?

[Click here](#) and complete the steps to remove limitations.

Completing all of the checklist items will automatically restore your account access.

The Commonwealth Bank Team

Copyright © 2009 Commonwealth Bank Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

The email will usually try and entice you into clicking on a link. It is this link that will either take you to a fake login page (capturing your credentials), or download a virus or piece of malware to your computer.

Be aware that some threats are so new, they may not yet be detectable by AV & malware vendors. Always use caution, never assume an attachment is safe. If you don't know the sender, and can't confirm the validity of the attachment: **DELETE IT!**

FW: CKD Invoice

Attached file: 88N8EM...  
248 KB

-----Original Message-----

From: Jacob Garrett [mailto:mitko.cvetkovski@louisberger.rs]

Sent: 03 December 2015 06:50

To: Lorraine Shaw

Subject: CKD Invoice

Hello

Please check the receipt attached to this message. The Transfer should appear on your bank within one day.

Best regards

Jacob Garrett

Look out for malicious attachments.  
In this example, the threat was so new, the AV vendor didn't detect the Trojan attachment, nor did any of the 55 AV vendors on Virus Total.

Look carefully at the From address. You may notice that these emails aren't from the companies they claim to be from, or from an email address that you don't recognise.

**Stay Educated, Stay Informed!**

