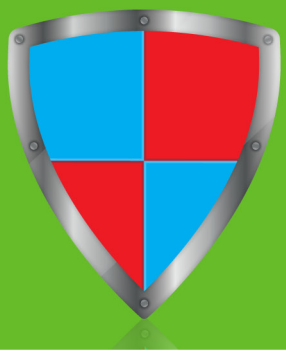
NCi TECHNOLOGIES

BEWARE OF CRYPTOLOCKER RANSOMWARE

DON T BE HELD TO RANSOM

A **malware** that restricts access to the computer system it affects and demands a **fee paid** to release it



Your **personal** files are **encrypted!**

To **decrypt** your files you must obtain a **private key.** To do this you must pay **300USD/ 300 EUR/** similar amount in **another currency.**

Never open ANY attachment from ANY sender you don't recognise. Protect yourself with responsible IT use.

Cryptolocker is 'ransomware' that presents itself as a spam email, software that pretends to be a required program to view online videos or via 'exploit kits' linking the user to a landing page on hacked websites. Once installed, Cryptolocker scans a computers local and network drives then encrypts over 50 different file types and demands a payment to de-crypt them.

"I have anti-virus, shouldn't that stop Cryptolocker?" Not all anti-virus software is equal, and your antivirus definitions may be up to date - but is your antivirus engine? (the program that downloads and runs the definitions). Viruses spread automatically, Cryptolocker won't spread itself, it has to be opened in order to activate on the users PC. Some antivirus software will quarantine Cryptolocker **AFTER** it has activated, in which case the damage may already have been done.

The Cryptolocker emails that have been seen by NCI all contain a .zip file and pretend to have originated from companies like Amazon and other genuine internet companies as an invoice or other such email. On closer inspection the domain names or people the email was sent to are suspicious. I have never received a genuine invoice from Amazon that ever contained a .zip file, and I know you haven't, don't open this one.

Backup your data, backup, backup, backup!

At the time of writing this there is no known way of decrypting the data other than paying a ransom fee (and even then you are not guaranteed to receive the private key necessary to unscramble your encrypted data). By opening that .zip file it might not just affect you, it could also cripple your company by encrypting networked files. Once infected, you have up to 72 hours to pay or you'll lose your data **FOREVER** if you have no other means of restoring from backup.

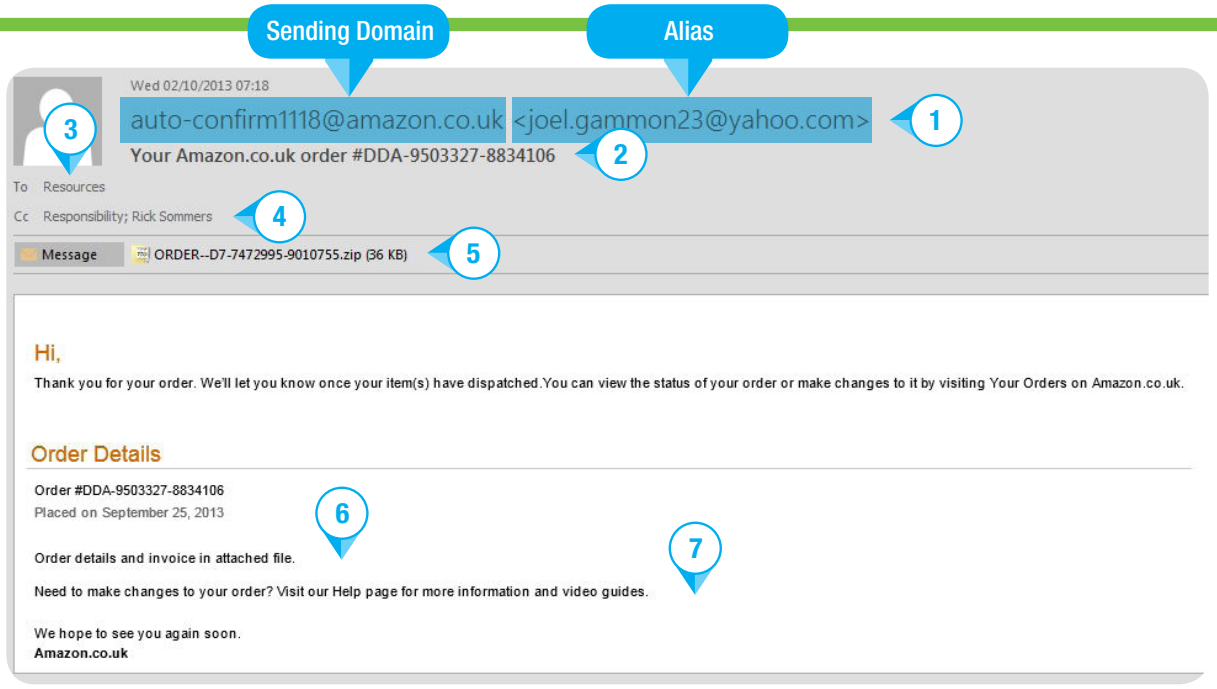
YOU HAVE BEEN INFECTED WHAT NOW?

Unplug your PC/Laptop from the network and shut it down. If you are wirelessly connected, turning off your PC is the fastest way of breaking that link.

Then tell *IT* support.

WHAT TO LOOK FOR . . .

1. **Are these emails correct?**
   Alias address doesn't match sending domain
2. **Did you place an order? Is this the correct number?**
3. **Look out for generic email addresses**
4. **Look out for several emails copied in**
5. **Don't open the file until you are sure it's right**
6. **Beware of limited order information**
7. **Don't click any links unless you are sure it's a valid order receipt**



PREVENTION IS BETTER THAN CURE . . .

Protect your data before it is too late!

Consider your Options

Protect your Business

Backup

When was the last time you backed up your data? Could you afford to lose a whole days work if something was to happen just before your next backup? Who checks your backups actually work? These are all questions you need to ask yourself.

"I synchronize my files to the cloud". That is great, well done, but what are you doing for your backup? Synchronizing your files is giving you an exact copy of the data currently on your PC, errors and all, encryption and all. i.e if your files on your PC are encrypted by Cryptolocker then that encryption will also be on the cloud server.

You need a snapshot backup of your data to recover from, one that you can select a time/date in the past is best. NCI offers multiple solutions to meet these requirements, visit **http://ncitech.co.uk/business/bdr11** and review your disaster recovery options.

Network Security

Do you lock up your house when you go out? Do you have an alarm, maybe automatically notifying the police of alerts? Each extra measure you put in place is one more step an intruder would need to overcome to get past your defences.

Consider all the things you can do to protect your data. A Sonicwall firewall including comprehensive gateway filtering. Managing your active directory group policies to limit users ability to accidentally hurt your data. Ensuring your antivirus is up to date and your servers and PCs are patched with the latest security updates. Are your emails filtered for spam and viruses before they get to your company? We can't force you to implement security, all we can do is advise how to do it properly **http:// ncitech.co.uk/business/it-security**

Speed of Recovery

If just reading this document has made you consider if you have the right hardware/software in place to protect your data, think about if you were hit by something that disabled your ability to work, temporarily or permanently, who do you have to turn to for help?

A managed IT Service ensures the responsibility for keeping you safe is outsourced to the Managed Service Provider. Whether it be ensuring your internet is kept at its optimum, your backups complete and are recoverable or you need help with a problem with your PC or Server at a fixed cost for the year we can do it all. Review **http://ncitech.co.uk/business/managed-it-services** and give NCI a call to discuss how we can help you move forward doing what you.

Self Help

The number one piece of advice anyone should give you is . . .

Don't be Stupid

- Don't open any attachments from people you don't know
- Always check the email you have received is from the person/company that says it is
- If you are sent a personal email containing multiple email addresses of people you don't know it is probably dangerous
- If someone you know tells you the email is spam or virus, believe them and pass on the information to the experts to advise
- Do not forward emails you suspect are viruses or spam. If necessary take a screenshot so the experts can confirm
- Put as many obstacles in the way of the intruders as you can, and keep them up to date
- .Zip files that you don't expect WILL cause issues that you don't want

01326 379 497

info@ncitech.co.uk

www.ncitech.co.uk

NCI Technologies, Waterside House, Falmouth Road, Penryn, Cornwall, TR10 8BE