Are you **Ransomware** Ready?

Don't let the hackers bring you down…

What is Ransomware?

It is a type of malware, malicious software used as a part of a scam that is designed to prevent you from accessing your computer system or data until you pay a sum of money. Even if you pay, you may still not receive the key to unscramble your encrypted data or locked PC. It can affect both PC and mobile devices.

What does Ransomware do?

Lockscreen

Shows a full-screen message that prevents you from accessing your PC.

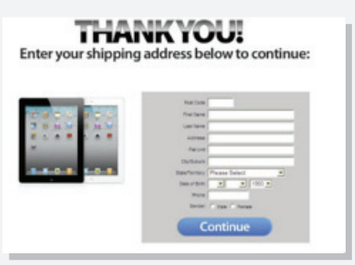
Encryption

Changes your files by encrypting them so you can't use them.

Apps lock

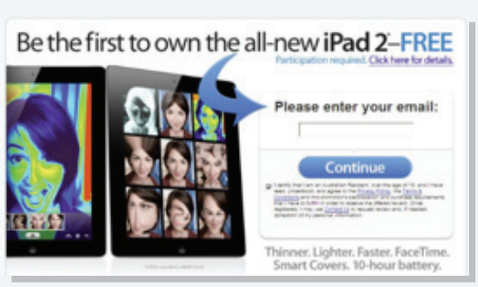
Prevents certain applications from running, like your web browser.

What should you look for?



Spam email, exploit kits, websites with pop-up requests, an attachment or link that appears genuine but requests payment or information from you – see the 'Ransomware Checklist'.

Pictured are examples of types of Ransomware.



Why do you need to know about Ransomware?

You could be encouraged to pay money to release access to data you already own.

It violates your privacy.

It can disrupt your work or personal life.

It could harm your reputation.

Types of Malware scams:

Cryptolocker

Hidden in a fake Amazon order (or other internet retailer) but includes a malicious zip file attachment.

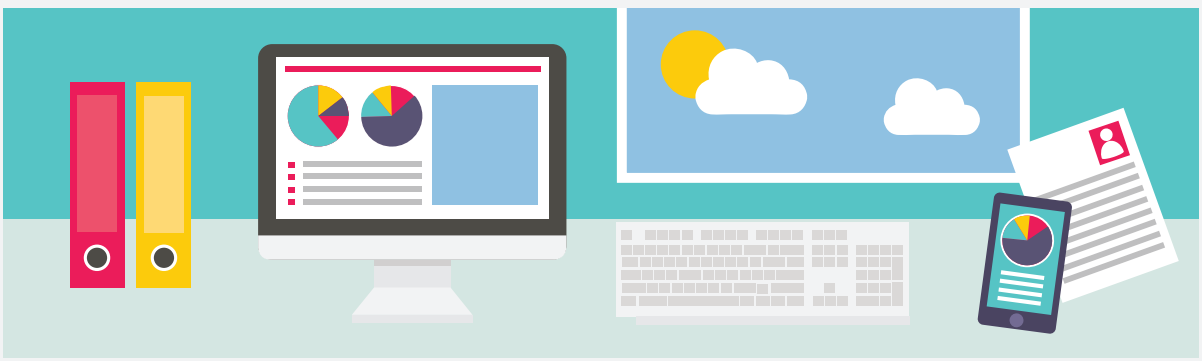
Paypal Trojan

A refund request from a genuine Paypal account with link to a malicious site and file.

Bogus Boss

Phishing email scam that crafts a fake email (or phone call) to the user imitating their boss and requesting immediate funds transfer for important purchase.

Prevention! How can you avoid an attack?



Antivirus

Find the best software for maximum security and ensure it's kept up-to-date. Not all AV packages are the same, some may not detect or stop all ransomware and may only quarantine a file after it has been activated, which could be too late.

Web/content filtering

Web/content filtering or smart screen protection – this will prevent you from browsing sites that are known to be hosting malicious files and protect you from malware downloads.

Backup, backup!

When was the last time you backed up your data? Are your backups checked, updated and complete? Can you afford to lose data or potentially lose a day's work to fix it? Can you ensure reliable and quick recovery of data if needed? This can be a headache to manage which is why so many businesses outsource their IT security services for less stress, peace-of-mind and proven reliability and protection.

Change Settings

Enable file history or system protection.

Train your Staff

Know what to look for - beware of phishing emails, spam and click-ing malicious content – see Checklist.

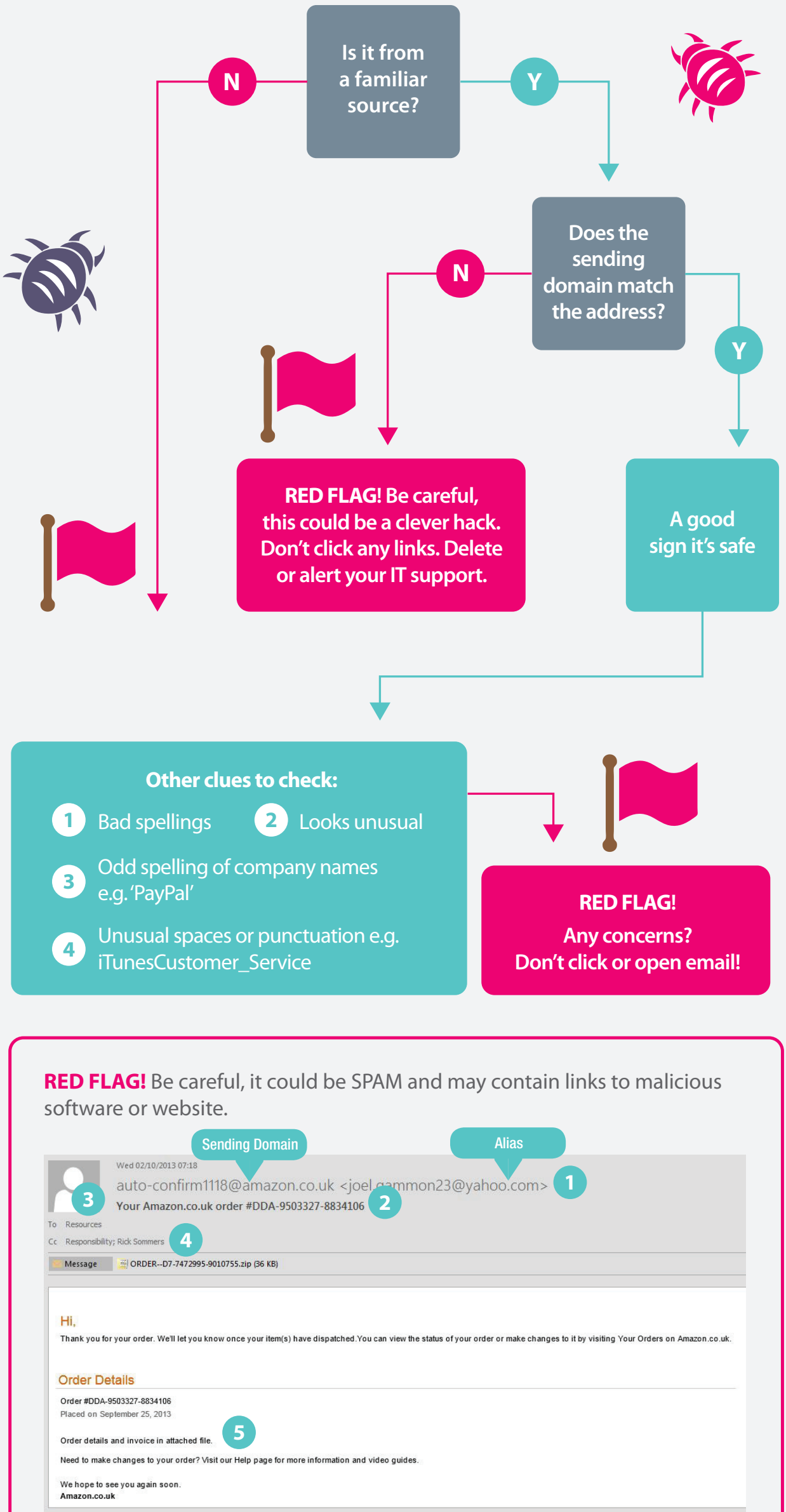
Disable Macros

This could automatically run an executable file without your click.

Password Protection

Use a password protected internet and/or wireless connection.

Detection! Ransomware 'email' checklist!



RED FLAG! Be careful, it could be SPAM and may contain links to malicious software or website.

1. Does the alias address look suspicious or unusual?
2. Did you place the order it refers to? If so, is the order number correct?
3. Be careful with generic email addresses often they are genuine but can also be a route for hidden ransomware e.g. To: 'resources'
4. Look out for several emails copied in especially if you don't know them
5. Beware of limited order information

Do not open a file unless you're sure it's right

Do not click any links unless you're sure it's valid

What should I do if I'm concerned?

- Take a screen shot
- Let your IT support know
- Do not open, click links or forward the email

Contact the NCI team for swift assistance:
help@ncitech.co.uk or 01326 379 497

Recovery

I've been infected, is it too late? It may still be possible to save your data. Do you have a robust Backup process in place?

1

Unplug your PC/laptop from the network, and power supply.

2

If using Wifi, turn off your PC – it will break the link.

3

Contact IT support – there may be ways to de-encrypt the data or access the files

4

Data recovered from Backup – if you have a backup solution in place that is up-to-date and reliable then you should be able to swiftly resume work with little disruption.

5

My PC is locked down and I can't use it! – with a secure backup you will be able to resume work from an alternative device, and more readily so if you've backed data to the cloud.

6

If data is compromised, report the data breach to your customers and chief information officer.

Remember . . .

We are happy to help!

ncitech.co.uk

01326 379 497

sales@ncitech.co.uk