RANSOMWARE RESCUE

HOW TO RECOGNISE AND AVOID A HOSTAGE SITUATION

WARNING

Be on the alert for ransomware – viruses designed by cyber-thieves to lock you out of your computer until you pay a ransom.

THREATS SEEM INNOCENT WHEN THEY ARRIVE AS…

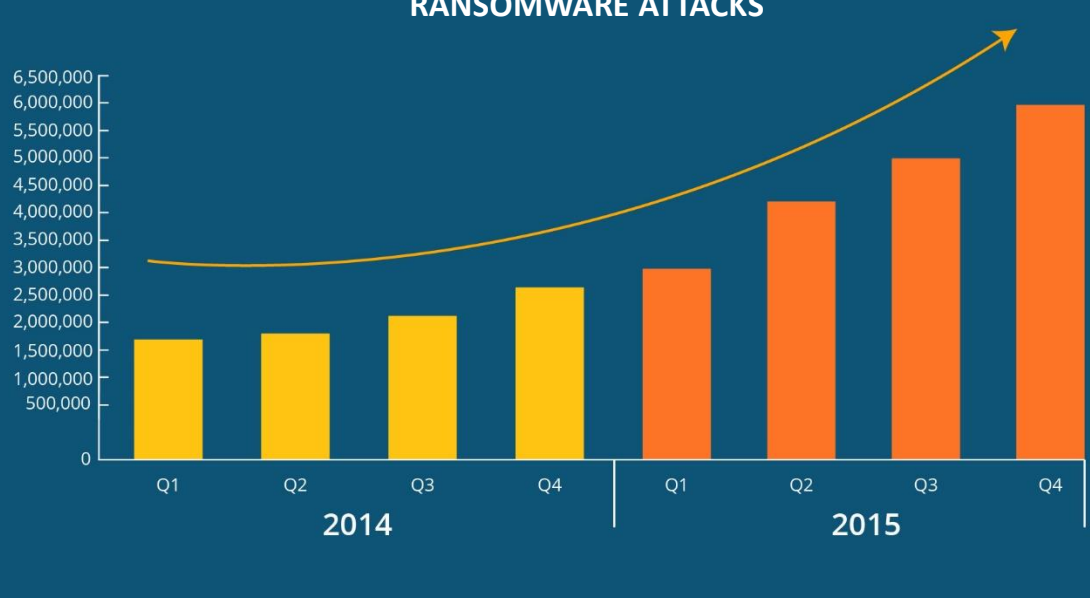
Email

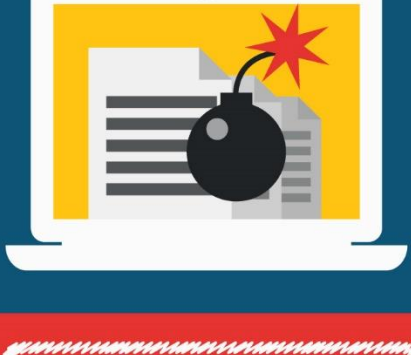
Internet Downloads

PDF's

…BUT ONE CLICK CAN LET AN INFECTION INTO YOUR ENTIRE NETWORK

RANSOMWARE ATTACKS





A RANSOMWARE INFECTION MEANS

- ☑ Temporary or Permanent Data Loss.
- ☑ Little or no access to your systems or applications.
- ☑ Disruption to your regular operations.
- ☑ Financial loss.
- ☑ Harm to your organizations reputation.

PROTECT YOURSELF AND YOUR COMPANY

CHECK ALL OF YOUR EMAILS CAREFULLY BEFORE YOU OPEN THEM

SAFETY CHECKLIST:

- ☑ I know the sender of this email.
- ☑ It makes sense that it was sent to me.
- ☑ The attached link or PDF is something that I can verify is safe.
- ☑ The email doesn't threaten to close my accounts or my cards if I don't provide information
- ☑ This email if from someone I trust, it doesn't just look like someone I trust.
- ☑ Nothing seems 'odd' about this email, its contents or sender.

YOUR RANSOMWARE PREVENTION KIT

UPDATE!

Keep on top of updates for your antivirus and other applications.

Don't say no to familiar updates!

STAY VIGILANT

If it sounds too good to be true, it is.

Stick with trusted sites and don't fall victim to scams (like "You're a Winner!" banners). Be aware of email attachments: ransomware commonly comes in the form of a bogus shipping receipt or invoice

CHECK YOUR BACK UP

Ensure your critical files are being backed up often, preferably offsite, in case you do get infected. Files saved to an attached USB drive or another location on your network are still vulnerable!

LISTEN TO YOUR ANTIVIRUS

If you get a warning from your antivirus about a possible threat,

Don't dismiss it. Report it to your support team, with lots of details!

BEWARE OF POP UPS

Immediately close popups that ask you to update your account information or install applications you did not specifically request.

BOOKMARK

Hackers often create pages with names very close to commonly used sites (Gogle.com, for example). Save your most used or sensitive websites to avoid typing the wrong address and ending up somewhere you don't want to be.

If you think you've been infected, DON'T FEED THE HACKERS!

Unplug your computer from the network and call your IT service provider immediately.

Created by the security experts at Quintech
Computer Systems Ltd
www.quintech.co.uk