RANSOMWARE rescue

HOW TO RECOGNIZE AND AVOID A DATA HOSTAGE SITUATION

Warning!

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

THREATS SEEM INNOCENT WHEN THEY ARRIVE LOOKING LIKE…

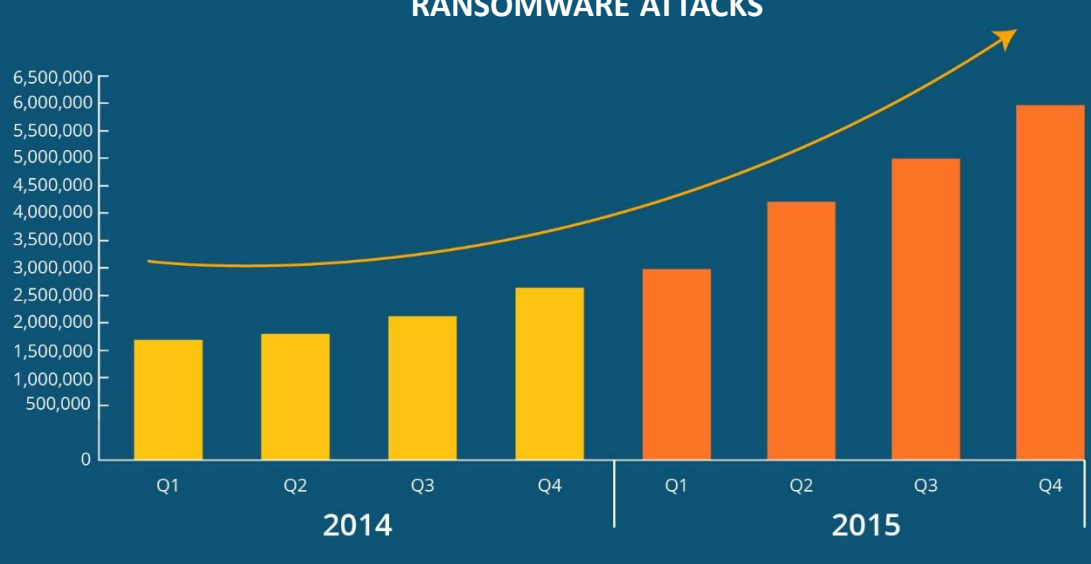
EMAIL

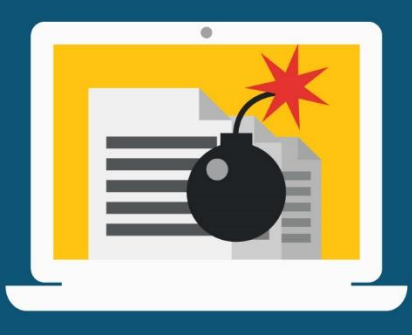
Internet downloads

PDF's

..BUT ON 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 systems and applications.
- ☑ Disruption to your regular operations.
- ☑ Financial loss.
- ☑ Harm to your organization's reputation.

PROTECT YOURSELF AND YOUR COMPANY

CHECK ALL OF YOUR EMAILS CAREFULLY BEFORE OPENING THEM!

SAFETY CHECKLIST:

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

CHECK YOUR BACKUP

Ensure your critical files are being backed often, preferably offsite, in case you 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 IMMEDIATELY, with lots of details!

BEWARE OF POPUPS

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

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.