Customer Information - IT Security Recommendations
Poppy IT Services - January 2017

Poppy IT Services
www.poppyits.com

Ransomware is a major threat to your business

What exactly is it?
Ransomware is a criminal moneymaking scheme that is usually installed by clicking deceptive links in an email, instant message or website. All your important documents, pictures, etc will then be silently encrypted, making them unusable. Finally, a message is displayed demanding a ransom payment for the unlock key. This is something you really do not want to experience first-hand.

Am I already protected?
Because ransomware typically gains initial access by human deception, anti-virus protection alone is unlikely to block such attacks. You may already be very wary of what you click on, but even the informed user can be duped in the right circumstances.

What happens if I get hit?
Paying the ransom is one option, but not advisable - apart from being very complicated (payment in 'bitcoin' digital currency), the recovery key is often not forthcoming or does not work.
An infected PC with access to shared folders, such as another PC, network hard drive or file server, will usually result in those files also being encrypted.

To be clear, encrypted effectively means 'lost'. In most cases the only realistic option is to remove the malicious software and then restore your files from a recent backup.

Is this actually happening?
Yes. We have experienced three or four ransomware incidents with business customers. Cleaning infected computers and restoring data from backups takes time, which is an unwelcome expense & loss of productivity.

What can be done to mitigate the risk?

a) **Prevention is better than cure :** minimise vulnerability with a layered approach (see below)

- Keep Windows & other software up to date (security patches)
- Minimise malware infections with business-grade anti-malware protection
- Block access to dangerous web links, based on trust ratings & content types.
- Consider restricting staff access to personal email & social media sites
- Email security - business-grade spam & content filtering
- Custom settings - eg. prevent programs running from default folders, show file extensions, etc.
- Avoid use of mapped drives to shared network folders
- User education - raise awareness & recognition likely threats

b) **Be prepared for the worst** : a rock-solid backup solution is your only safety net

- Regular backups of critical data
- Test & verify that the restore process works

How can we help protect you?

PoppyIT has a the following services available, to address this layered approach:

- Workstation CarePack - ensures software updates are applied (Patch Management)
- Managed Antivirus - business-grade anti-virus/anti-malware protection (Bitdefender)
- Web Protection - block dangerous links / enforce web usage policy
- Hosted Exchange Email, with options for Email Security with or without Email Archiving (1 or 10 years)
- Managed Backups - local &/or cloud backups with central management & alerts

Most of our business customers take the Workstation CarePack & Managed Antivirus, which provides a standard platform for us to provide effective support & management. Many also have the hosted exchange email, providing large mailboxes, shared calenders/contacts and centralised management of email footers/signatures.

Customers that I have spoken to about the ransomware threat have generally opted to add Web Protection and Managed Backups. Several Hosted Exchange email customers have added Email Security / Archiving.

Further Information

Please contact us to discuss your specific situation and get further details of service that will reduce the likelihood of your business being hit by ransomware.

Poppy IT Services
020 3773 3356