SBS Cyber Security

sbscybersecurity.co.uk

186 Cheetham Hill Road,
Manchester,
M8 8LW

M: 0161 827 1600

RANSOMWARE - WHY YOU SHOULDN'T PAY

03.03.17 - TITAN - North West Regional Organised Crime Unit

Ransomware is one of the biggest, current cyber threats. Your data is encrypted and criminals ask for digital currency to get everything back. But what should you do?

Ransomware is a form of malicious software which enables a criminal to remotely access your machine and encrypt, or lock files on your computer or mobile device.

Criminals then try to extort money from you in the form of digital currency to get your files back.

If you become a victim of ransomware, call the police on 101 and explain exactly what is happening. Often the electronic keys to unlock your files are publicly available and we can assist you by unlocking your files for you.

Paying the ransom just feeds the criminals hands and there's no guarantee you get everything back. Sometimes you may even get your files back but with another virus or piece of malware added on which will cause you further problems.

To stay safe, don't click on links or websites which you are unsure about, and follow the simple advice below:

SBS Cyber Security

sbscybersecurity.co.uk

186 Cheetham Hill Road,
Manchester,
M8 8LW

M: 0161 827 1600

DO YOU REALLY KNOW...

...HOW RANSOMWARE WORKS?

Ransomware is a form of malicious software (Malware) that enables cyber criminals to remotely lock down files on your computer or mobile device. Criminals will use ransomware to extort money from you (a ransom), before they restore your access to the files. There are many ways that ransomware can infect your device, whether it be a link to a malicious website in an unsolicited email, or through a security vulnerability in a piece of software you use.

UK

The UK was among the top 5 countries affected by ransomware in 2015

Symantec - Evolution of ransomware 2015

90,000

The estimated number of devices infected in one week by a single piece of ransomware

http://www.forbes.com/

£514

The average ransomware demand

Symantec - Ransomware & Businesses 2016

HOW TO PROTECT YOURSELF...

- Don't click on links, or open any attachments, you receive in unsolicited emails or SMS messages. The links may lead to malicious websites, and any attachments could be infected with malware.
- Always install software updates as soon as they're available. Whether you're updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Install anti-virus software on your computer and mobile devices, and keep it updated. Bear in mind that ransomware can often be picked up by visiting disreputable websites including illegal movie streaming websites and some adult sites.
- Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to isn't left connected to your computer as any malware infection could spread to that too.
- Don't pay extortion demands as this only feeds into criminals' hands, and there's no guarantee that access to your files will be restored if you do pay.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Get Safe Online
Free expert advice

TITAN
North West Regional Organised Crime Unit

mitigate xyone Cyber Security SOPHOS CYBER ESSENTIALS CYBER ESSENTIALS PLUS