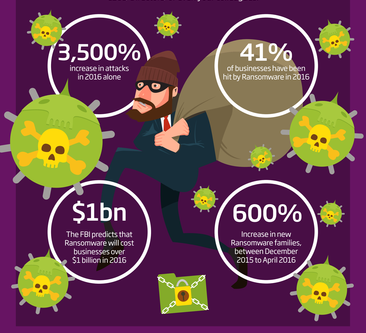
2016 has been dubbed the 'Year of Ransomware'...but why?

What is Ransomware?

Ransomware is a form of malicious malware. Most modern Ransomware viruses encrypt a user's files and demand money for their decryption – hence the name.

Why should I be aware of Ransomware?

Ransomware has existed for a long time, but it's seen a resurgence in 2016. Hackers are more targeted, using methods like spoofing to impersonate CEOs, Directors, or even your colleagues.



3,500%
increase in attacks in 2016 alone

41%
of businesses have been hit by Ransomware in 2016

$1bn
The FBI predicts that Ransomware will cost businesses over $1 billion in 2016

600%
Increase in new Ransomware families, between December 2015 to April 2016

Ransomware in the UK

Ransomware accounts for

25%

of all cyberattacks hitting businesses in the UK. This is a higher proportion than in any other country.

What's more,

54%

of UK businesses have experienced a Ransomware attack, and

37%

pay the ransom.

Top vehicles for Ransomware:

31%
Email Links

28%
Email Attachments

24%
Websites or Web Apps

At 59%, malicious emails are the most common way to distribute Ransomware. Other sources include websites, social media and infected USB sticks.

Hackers are spoofing CEOs and your colleagues, but they're also sending fake emails including:

Invoices | Shipping Confirmations | Overdue Bills | Tax Return Information | Fake Credit Card Reward Schemes

These fake emails are highly effective because they can lead victims to believe they're losing money.

But it's not just dodgy zip files and links that are hosting the viruses...

50%

Macro-activated infections (usually transmitted through an innocent-looking Word document) **have risen by 50%.** PDFs are also being used more to distribute Ransomware.

Should I pay the ransom?

You could, but **you shouldn't** for two reasons:

1 Paying gives the hackers the incentive to **carry out more attacks.**

2 There's no guarantee you'll get your files back – a third of the UK businesses who paid the ransom **never saw their files again.**

The average demand price has more than **doubled** since 2015.

Money isn't the only issue...

3.5% of businesses who've experienced a Ransomware attack said that there was a risk of people dying due to encryption (and loss) of patient information. Hospitals are easy targets due to outdated IT systems.

How can I prevent Ransomware?

Just 4% of businesses are confident that they can deal with the Ransomware threat. So how can you prevent it?

Be suspicious of emails

Email is the most common vehicle for Ransomware. Hackers are favouring 'spoofing', where they'll pose as your CEO or another colleague to gain your trust. Never click a link or open an attachment from an unknown source, and **always check the sender's email address and credentials.**

Back up your data

If you're unlucky enough to fall victim to a Ransomware attack, backing up your data means you'll be able to restore it without succumbing to the cyber criminals' demands. You can back up on cloud servers, on-premise servers, or as a last resort external hardware like USB sticks and hard drives.

Use a Ransomware-specific anti-virus solution

Ransomware is becoming more prevalent and more intelligent, but so are anti-virus solutions. **Sophos Intercept X** has been designed specifically to combat Ransomware at the point of entry and uses innovative tools to strengthen your system and ensure you never fall victim again.

Sources:
ESET, Malwarebytes, Osterman Research, Symantec, Tim Gurganus, Infoblox, CBR

Courtesy of TSG