Avast Business

Ransomware survival:

Jigsaw

With 120 million new ransomware samples in 2015 alone, it is one of the fastest growing threats on the web. Jigsaw is the newest and most advanced version of ransomware – hijacking your computer and deleting files until you pay up. Prevention is key to avoiding these attacks. Welcome to ransomware survival!

How does Jigsaw get in?

Businesses are 80% more likely to get hit by ransomware; educate your employees, users, or customers on how to spot it before it becomes a problem.

Email

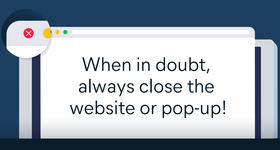
Malicious emails are some of the most common ransomware entry points. What to look for:

- A malicious link
- Suspicious or vague subject lines
- An attachment with malicious code inside disguised as a .pdf, Word, Excel, or .zip file

Website

Sometimes a webpage can be a point of entry. Watch out for:

- Links that point to ransomware
- Images that link to ransomware
- Pop-ups or banner ads



What happens when you are infected with Jigsaw?

72hrs You typically have 72 hours to pay the ransom, usually in Bitcoin.

1hr Every hour and at start-up, Jigsaw deletes files to pressure you into paying up.

1-1K The rate at which files are deleted is exponential, from a single file to a thousand files at a time.

Why Bitcoin?

Bitcoin is a digital currency that supports peer-to-peer transactions without the need of a bank or credit card company.

The payment cannot be tracked, making it harder for the police to get involved or banks to freeze payments.

There is no supervision of your payment and therefore no guarantee.

The good news: we can protect you!

As your security partner, we understand what's needed to protect your business against the latest threats. We let you focus on what you do best, your business, and we worry about your security.

We can protect you in four important ways:

1

We've got your back

With an effective backup of your files, you keep control of your data regardless of it being held for ransom. It's easy to recover without having to pay a dime.

2

Filter spam, attachments, URLs, social media links and websites

90% of all SPAM email links to malware. We help eliminate spam from the inbox, we then scan attachments, attached archives, and encrypted email streams to remove threats. We scan for hidden threats on websites, in the URL of any sites visited, and in links exchanged in social networks.

3

Remove vulnerabilities

Ransomware and malware take advantage of software imperfections. This is why maintaining the latest versions of software and operating systems is essential. We keep things up to date, so you can focus on running your business.

4

Use multi-layer protection

Simply relying on one approach to protect yourself isn't enough – our multi-layer security system combines best-in-class technology to prevent, detect, and eliminate most threats.

Trust us to protect your business.

Contact us today to find out how we can protect your business against ransomware and other threats!

#securitysimplified