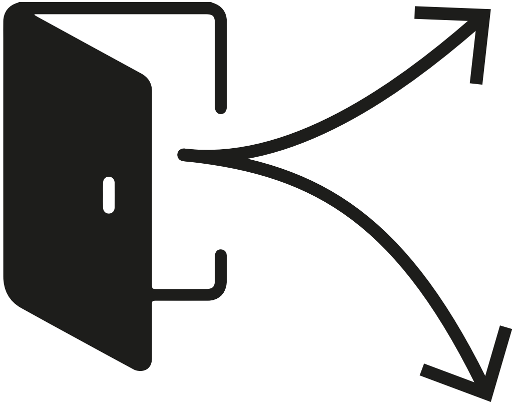
AVG Business

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

Website

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

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

When in doubt, always close the website or pop-up!

What happens when you are infected with Jigsaw?

72:00

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

00:60

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

1-1000

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.

Bitcoin is mostly available on the dark web.

Don’t give ransomware a chance Prevention is the best protection

By backing up regularly, educating your customers, and using multi-level protection you can protect your customers' business against ransomware. Not all antivirus solutions are able to scan files to a level that can actually prevent a ransomware attack. Make sure your antivirus software is able to scan .zip files, metadata, content and behavior.

Protect your customers' business in 5 simple steps:

1. Backup files to an external drive
2. Educate employees on what to watch for
3. Implement policies to manage ransomware
4. Update all software to the latest versions
5. Use multi-level AV protection

Trust AVG to protect your customers' business

AVG Internet Security and AntiVirus Business Edition utilize a multi-layered approach to detecting and eliminating ransomware. When a file passes successfully through one level of testing, it is handed off to another layer. AVG proactively identifies new malware samples and our advanced algorithms shorten scanning times!

Don't let your customers' business be held to ransom!

ASBIS®
www.asbis.com

#securitysimplified

The Online Security Company™
Devices. Data. People.™