Russian ransomware attacks are on the rise - here’s how to protect your business from cyber-attacks

Submitted by: Key Loans & Mortgages Limited t/a KIS Finance
Wednesday, 23 February 2022

In a joint review of cybercrime trends led by the UK, USA, and Australia, it was found that the number of sophisticated ransomware attacks originating from Russia, or being carried out by Russian speakers, has been on the rise over the last year.

Last October, the UK’s cyber agency GCHQ also stated that UK ransomware incidents had doubled.

This threat is now being highlighted in Government after Chief of the Defence Staff Admiral Sir Tony Radakin told the Cabinet earlier this month that the UK needs to be ready for a wave of Russian based cyber attacks over its defence of Ukraine.

According to the National Cyber Security Centre (NCSC), the top sectors often targeted in ransomware attacks are:

- The NHS
- Universities and schools
- Businesses (including SMEs)
- Charities
- Law firms
- Councils

For example, at the start of February KP Snacks (makers of McCoy’s crisps and Hula Hoops) suffered a ransomware attack resulting in a supply disruption which is expected to last until the end of March at the earliest.

Ransomware is a type of malware that employs an encryption software to the user’s device in order to hold their information at ransom. The information or data is encrypted so that the user can’t access or read their own files or databases. The criminals then demand a ransom (payment) in order to release the information back to you.

This type of attack can be crippling for organisations and businesses that hold and rely on large customer databases.

In light of this growing threat, Holly Andrews, MD at KIS Finance (https://www.kisbridgingloans.co.uk/) and personal finance and fraud expert has provided her tips for businesses on how to protect themselves from ransomware attacks.

“Most ransomware attacks happen via unsafe websites, text message links, or email attachments that are sent to an employee of the company or organisation. This means that every company and organisation that uses email services is a potential target.

Once the attachment or link has been clicked on, it activates the malware which then infiltrates the user’s device and encrypts the any data or information held. These criminals are smart and their attacks are usually targeted to a specific person that has access to important files and databases.

There isn’t one single method that can be used to prevent ransomware attacks, so you need to implement good cyber security practices across your business in order to mitigate the risk and potential losses if you do fall victim to an attack.”

1. Educated your employees

Your employees should be your first line of defence against ransomware attacks so it’s vital that everyone on your team is educated on how to identify cyber threats. Your employees should know never to open email attachments from an unknown source or to download files or software from anywhere that isn’t a known and trusted source.

It’s also important to keep your employees updated on all the latest threats and any new tactics that these criminals are using so they know what to keep an eye out for.

2. Keep anti-virus software up to date

Just having anti-virus software in place isn’t enough; it needs to be regularly updated in order to be effective.

Make sure that every device in your company or organisation is regularly updated with the latest anti-virus and anti-malware software. Having software that updates automatically and runs regular checks will give you the greatest level of protection against any potential threats.

3. Limit access

In order to limit the risk of ransomware threats, it’s important that you limit access of important files to those who really need it. Giving employees access to databases and files that they don’t need only widens the risk as criminals have more targets for their attack.

4. Backups are essential

It’s absolutely essential to have backups of important files and documents. This is especially the case if your business can’t operate without them as backups will allow you to still have access to your data

in the event of a ransomware attack, lessening the impact on your business.

Backups should be stored either offline, or in a system that is entirely separate from your business' operating systems.

5. Have a response plan

Although taking these safety measures will mitigate the risk of an attack, nothing is 100% bulletproof and there's still a chance that a ransomware attack can happen. In which case, setting out a response plan ahead of time will ensure that you can respond quickly to a threat.

Make sure that all of your employees know who should be alerted in the case of an attack and what steps they need to take after a breach.

[ENDS]

Notes to journalists/editors:

Comments provided by Managing Director at KIS Finance, Holly Andrews. If you would like to use these comments then a link back to KIS Finance is required to credit the source.

KIS Finance fraud guides - https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/

About KIS Finance:

KIS Finance are an independent finance broker specialising in bridging finance, development finance, commercial mortgages, equity release, and secured loans. Their team of advisors have considerable experience across multiple different areas of the finance sector, as well as insurance and compliance.

KIS Finance are also very invested as a company in fraud awareness and prevention and keeping their clients safe from financial fraud and scams.

Contact:

Phoebe Griffits
phoebe@kisfinance.co.uk
01884 669099

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Key Loans & Mortgages Limited t/a KIS Finance

Copyright © 1999-2026 ResponseSource, Northburgh House, 10 Northburgh Street, London, EC1V 0AT, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com