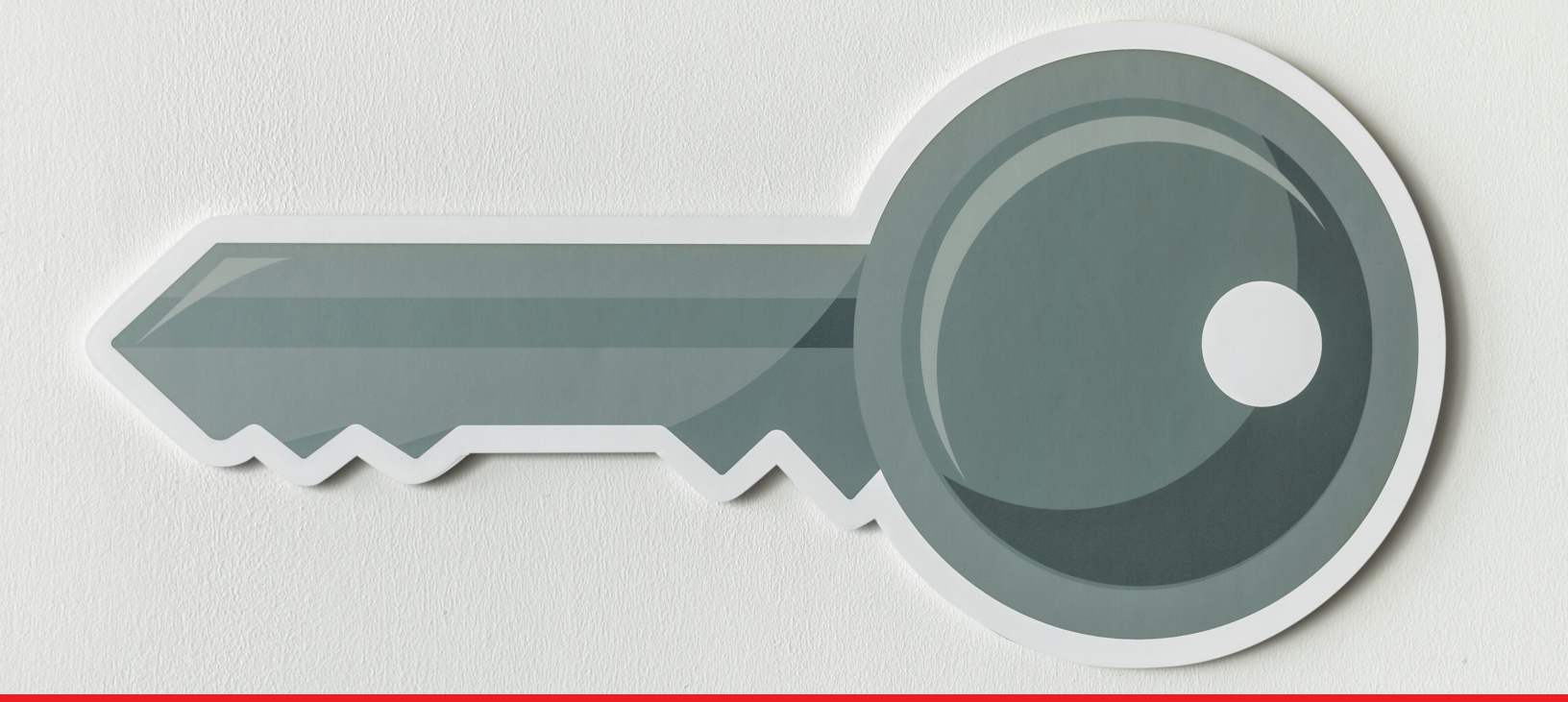
RANSOMWARE EXPLAINED



RANSOMWARE EXPLAINED

Ransomware attacks have become a normal occurrence in the last few years and the criminals behind it are so polished that in some cases they even have mini-call centers to handle your payments and questions.

In 2018, about 70% of ransomware attacks targeted small businesses with an average demand of $116,000, according to a report from Beazley Breach Response Services. Ransomware attacks have increased 11 percent from the past year, with 206.4 million attacks, according to recent SonicWall research.

WHAT IS RANSOMWARE?

The business model is as old as the earliest kidnapping. Ransomware stops you from using your PC, files or programs. The attackers hold your data, software, or entire PC hostage until you pay them a ransom to get it back. Obviously, knowing that you are dealing with criminals, there isn't a guarantee you will ever get your data back just because you meet their demands.

HOW DO I GET RANSOMWARE?

There are several ways that ransomware can infect your computer and network. It often spreads through malicious spam emails, which are unsolicited and may contain malicious attachments or links. Unfortunately, an employee may unintentionally download or click on these traps. Other times, the emails use social engineering to trick people into opening the attachments or clicking the links, because they believe it's from a trusted institution, another coworker or even boss.

HOW DOES RANSOMWARE AFFECT MY BUSINESS?

Ransomware can be very critical to small businesses because they have less to spend on cybersecurity software and staff training. If a business does not have a full back up system in place, this typically leads to paying the ransom, only to find out that they took your money and ran. Or if you refuse to pay, they destroy your data, and it causes massive business interruption. This could lead to starting your business from scratch or putting you out of business. It's this willingness to pay, which makes smaller businesses such an easy target.

CONSIDERING THE EPIDEMIC OF RANSOMWARE ATTACKS, NOW IS A GOOD TIME TO GET SMART ABOUT PROTECTING YOUR BUSINESS. HERE ARE 5 STEPS YOU CAN TAKE IMMEDIATELY:

1

BACKUP YOUR DATA

Your staff may fall victim to a sophisticated phishing message or scam and expose your network to the biggest risks out there, unintentionally. Clicking on a fake link or entering sending information to a fake email address, that is spoofing the original sender, are just some of the security disasters waiting to happen.

2

EDUCATE YOUR EMPLOYEES

People remain the biggest source of security breaches. Employees unwittingly open malicious emails or go to corrupted sites and expose their employers' networks and infrastructures to malicious software. By learning how to spot malicious emails, your end users will stay one step ahead of cybercriminals.

3

PATCH AND UPDATE YOUR SOFTWARE

Hackers love security flaws, also known as software vulnerabilities. Which is why software updates and patches are very important. They cover the security holes to keep hackers out. Updates can add new features to your devices and remove outdated ones.

4 **LIMIT USER'S RIGHTS AND PRIVILEGE**

To minimize the impact of a potential attack, it's important for your business to make sure that employees only have access to the information that is needed for them to execute their day-to-day duties. This helps limite the potential of a ransomware attack spreading throughout your network.

5 **TURN ON TWO-STEP AUTHENTICATION**

Two-factor, or multi-facdtor, authentication can use anything from a text message to your phone or a biometric like your fingerprint, to provide enhanced account security. This adds a second level of authentication to accoun logins.

KNOWING HOW TO AVOID RANSOMWARE IS KEY TO SECURING YOUR INFORMATION SYSTEM INFRASTRUCTURE.

Tech Rage IT | 1511 E State Rd 434, Suite 2001 | Winter Springs, FL 32708 | 407-278-5664
www.TechRageIT.com