CENTRAL BUSINESS SYSTEMS NEWSLETTER

Summer 2024

Top News

Stay ahead in tech with our newsletter! From cutting-edge innovations to expert insights, we're excited to bring you the latest trends and developments transforming the IT and cybersecurity landscape.

What Is Ransomware?

Most people have heard about the importance of protecting their business from a ransomware attack. But not everyone knows exactly what ransomware is.

Ransomware is a type of malicious software, or malware, that encrypts your data, rendering it unusable, or that prevents you from accessing your computer system entirely. It is called "ransomware" because the cyber criminals who perpetrate these types of attacks hold your data or system access hostage and demand a ransom payment from you to get it back.

Ransomware attacks are all too common; in fact, 24% of all data breaches involve ransomware, according to the Verizon 2023 Data Breach Investigations Report.

con't page 2

BUSINESSNEWS 2023 Best Places to Work Central Business Systems

#TechTrends #StayUpdated

What Is Ransomware? *cont'd*

How do Ransomware Attacks Happen?
Threat actors pull off ransomware attacks in a number of ways. The most common method is through phishing emails. Designed to look like legitimate communications from a reputable organization or a familiar person, these emails contain a malicious link or attachment. When you click or open it, ransomware is installed on your device and starts encrypting files on the affected system – and may spread to additional systems on the same network. You may also unwittingly download ransomware from compromised websites or ads, or it may enter your system through infected software applications. Cyber criminals can also insert ransomware by exploiting network vulnerabilities.

Some ransomware attacks encrypt files, while others lock you out of your device completely. Another common subset of ransomware attacks, known as scareware, involves fake warnings and demands for payment to fix non-existent issues.

Should You Pay the Ransom?
Ransomware attacks are followed by a note demanding payment for a decryption key or to unlock your system. This leaves you with a horrible choice to make: Pay off the criminals and (hopefully) get your valuable data back or lose access to your system and/or data and risk public exposure of your data, which may be highly sensitive. Although many law enforcement agencies advise against it, many companies feel they have no choice but to pay the ransom. Unfortunately, making the payment is no guarantee that the thieves will unlock your system or deliver the decryption key, and even if they do, your data may still be at least partially corrupted or unusable. Further, victims who pay up are often targeted for future ransomware attacks.

Protect Your Business against Ransomware Attacks
It's best to avoid getting attacked in the first place. A strong defense against ransomware attacks should include several elements:

- Cybersecurity education for your entire team is one of the most effective ways to guard against ransomware attacks. Everyone should receive regular training and reminders about common and emerging threats and the dangers of clicking on links from unknown sources, visiting unsecured websites, and how to recognize phishing emails.
- Back up your data regularly and store these backups in a secure off-site location, so your data can be accessed in the event of a cyber attack or other emergency.

#CyberSecurity #Ransomeware

What Is Ransomware? *cont'd*

How do Ransomware Attacks Happen?
Threat actors pull off ransomware attacks in a number of ways. The most common method is through phishing emails. Designed to look like legitimate communications from a reputable organization or a familiar person, these emails contain a malicious link or attachment. When you click or open it, ransomware is installed on your device and starts encrypting files on the affected system – and may spread to additional systems on the same network. You may also unwittingly download ransomware from compromised websites or ads, or it may enter your system through infected software applications. Cyber criminals can also insert ransomware by exploiting network vulnerabilities.

Some ransomware attacks encrypt files, while others lock you out of your device completely. Another common subset of ransomware attacks, known as scareware, involves fake warnings and demands for payment to fix non-existent issues.

Should You Pay the Ransom?
Ransomware attacks are followed by a note demanding payment for a decryption key or to unlock your system. This leaves you with a horrible choice to make: Pay off the criminals and (hopefully) get your valuable data back or lose access to your system and/or data and risk public exposure of your data, which may be highly sensitive. Although many law enforcement agencies advise against it, many companies feel they have no choice but to pay the ransom. Unfortunately, making the payment is no guarantee that the thieves will unlock your system or deliver the decryption key, and even if they do, your data may still be at least partially corrupted or unusable. Further, victims who pay up are often targeted for future ransomware attacks.

Protect Your Business against Ransomware Attacks
It's best to avoid getting attacked in the first place. A strong defense against ransomware attacks should include several elements:

- Cybersecurity education for your entire team is one of the most effective ways to guard against ransomware attacks. Everyone should receive regular training and reminders about common and emerging threats and the dangers of clicking on links from unknown sources, visiting unsecured websites, and how to recognize phishing emails.
- Back up your data regularly and store these backups in a secure off-site location, so your data can be accessed in the event of a cyber attack or other emergency.

What Is Ransomware? *cont'd*

- Firewalls and antivirus software should be installed and updated regularly. These programs can sometimes block ransomware entirely or detect and mount defenses against an attack in its early stages, thus containing the damage.
- Monitor your system on a 24x7x365 basis, to identify any suspicious activity, and have a response plan in place that is ready to be activated in the event of various scenarios.
- Update all software as soon as updates become available from the manufacturer. Software companies continually update their products, shoring up various vulnerabilities with security enhancements and patches.

ARTICLE FROM WIRED MAGAZINE

Ransomware Is 'More Brutal' Than Ever in 2024 | By Jordan Pearson, Wired Magazine

As the fight against ransomware slogs on, security experts warn of a potential escalation to "real-world violence." But recent police crackdowns are successfully disrupting the cybercriminal ecosystem. Today, people around the world will head to school, doctor's appointments, and pharmacies, only to be told, "Sorry, our computer systems are down." The frequent culprit is a cybercrime gang operating on the other side of the world, demanding payment for system access or the safe return of stolen data. The ransomware epidemic shows no signs of slowing down in 2024—despite increasing police crackdowns—and experts worry that it could soon enter a more violent phase.
"We're definitely not winning the fight against ransomware right now," Allan Liska, a threat intelligence analyst at Recorded Future, tells WIRED.

Link to entire article: https://www.wired.com/story/state-of-ransomware-2024/

We're excited to announce we have openings for service technicians and IT engineers (Levels 1, 2 and 3). If you or someone you know is passionate about technology and committed to client service, we would love to connect. Come join Central, which Long Island Business News named among the Best Places to Work in 2023, and make a difference with your skills and expertise! Send resumes to Tom Drago at tdrago@centraldigitalsolutions.com.

#CyberSecurity #ITjobs

Join Family Service League on Saturday, September 7th, 2024 at Belmont Lake State Park in West Babylon, NY for a day of fun, fitness, and family!

Choose between a 1.5 mile or 5K walk or bike ride through the beautiful park. Whether you're walking, riding, or cheering on, there's something for everyone!

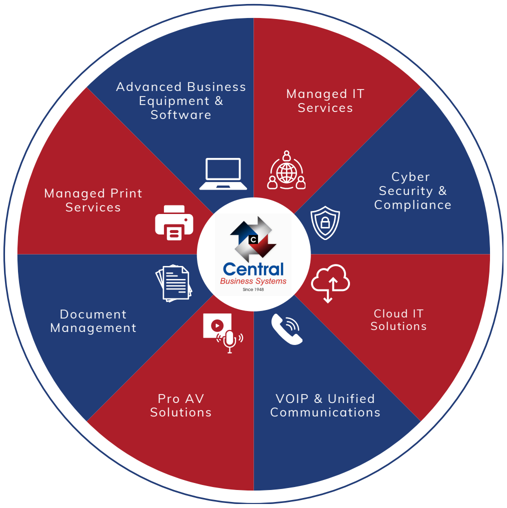
🕘 Starts at 9:00 AM
🍏 Healthy snacks
🧎 Wellness activities
👪 Fun for the whole family!

Don't miss out on this chance to support a great cause while enjoying a day in nature. For details: https://fundraise.givesmart.com/vf/WALK2024

Experience the Power of Integration with Central Business Systems!

As your one-stop technology partner, we're here to streamline your operations and drive efficiency throughout your entire organization.

With our integrated approach, we offer:



Advanced Business Equipment & Software
Managed IT Services
Cyber Security & Compliance
Cloud IT Solutions
VOIP & Unified Communications
Pro AV Solutions
Document Management
Managed Print Services
Central Business Systems

Hyakuman Kai Award

Sharp recognizes only a select group of dealers across the US with its prestigious Hyakuman Kai award. As a continued recipient, this award speaks to our mission at Central Business System's to deliver top-tier technology and industry-leading multifunctional products to businesses in the Long Island, Brooklyn, Queens, and NYC areas, helping them maximize growth and potential. We take immense pride in being a Sharp dealer and wholeheartedly commend Sharp's well-deserved reputation as one of the industry's best.

(631) 249-1990
team@centraldigitalsolutions.com
centraldigitalsolutions.com

Businessnews 2023 Best Places to Work
Central Business Systems