[Hyperlinks intentionally deactivated]

Pour lire la version française, cliquez ici

As the number one security threat to businesses, ransomware attacks jeopardize entire organizations. Phishing via malicious emails is like a knock on the door that if opened will let ransomware in. Awareness is key to preventing and minimizing risk.

Everyone. Every day.

Ransomware – What you need to know

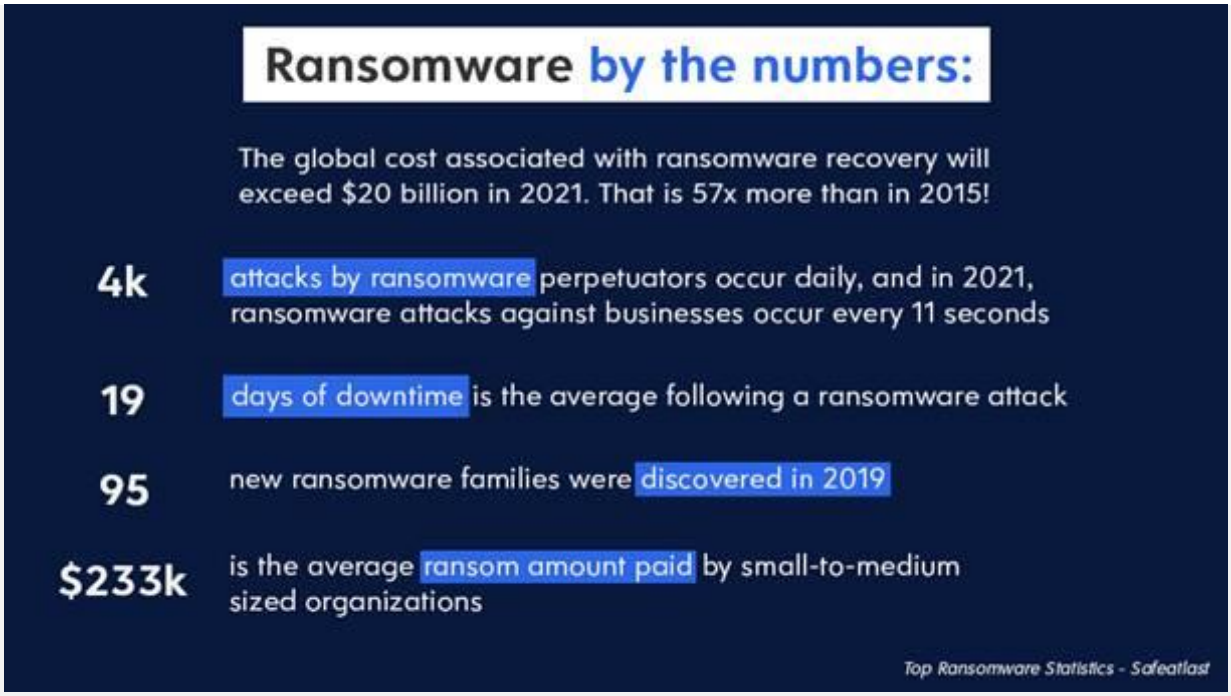
Ransomware was recently top news when an attack took the largest gasoline pipeline in the U.S. hostage. According to media reports, it was the biggest cyberattack on operations in U.S. history. Pipeline operations were shut down to contain the attack affecting delivery of gasoline and jet fuel on the U.S. Southeast Coast.

What is ransomware? Ransomware is a type of malware that holds systems and data hostage for payment. Cybercriminals usually go after businesses to get large amounts of money in the form of a ransom payment. There is also the threat of what could happen to the data that has been compromised – putting employees, customers, and the business further at risk.

Once ransomware gets in unnoticed, it can spread throughout systems infecting the entire organization. Says CISO Colin Anderson, “Ransomware can spread like head lice in a kindergarten.” Being aware of what comes in your email box is the first step to minimizing risk and protecting yourself against ransomware at work and at home. Here is what you need to know: Continue reading

Social Media Threats – Protect Yourself Online

Cybersecurity threats can also come through social media. Attackers use social media to capture information about individuals and companies to launch attacks. Find out how to protect yourself online here.



Did you know?

What's in a name
REvil, Nemty**,** NetWalker, DoppelPaymer, Maze – these may look like names of characters from a science fiction movie, and to be sure, these are some bad actors, but these are actually names for ransomware.

Identifying and classifying types of malware falls to researchers who create a name based on what is known about the malware and its functionality. By giving a name to the malware/ransomware, researchers are able to track and investigate to determine type, platform, and other important details. And, if the threat or vulnerability appears that it will have a big impact on the public, researchers may use special naming to attract media attention.

It is not always researchers who come up with names for ransomware threats or attacks. Cybercriminals themselves like to show off their creativity and put a name out there for recognition. REvil is one of those. Its name stands for Ransomware Evil and was inspired by the Resident Evil movie series (*Source: CSOonline*).

For more on cybersecurity, check out Cybersecurity Corner Online.