

3 WAYS TO PROTECT YOUR ONLINE BUSINESS FROM CYBERATTACKS IN 2021



3 WAYS TO PROTECT YOUR ONLINE BUSINESS FROM CYBERATTACKS IN 2021



*2020 was bad for cyberattacks.
Experts predict 2021 will be worse.*

Two out of every five businesses have had sensitive customer data stolen from hackers within the last year.

Cybercriminals targeted e-commerce with domain spoofing, ransomware, and breaches. The thieves breached business databases, stole customer credentials, and reused the stolen data to hack into other business accounts. The first tip sounds very simple, but it is often overlooked.

1. Don't store customer data


While it's tempting to store passwords and credit card numbers to make it convenient for customers to buy more goods and services down the road, you're leaving them and your business wide open to identity theft.

Many companies fail to do this correctly. The criminals are often successful because a Harris Poll shows up to 75 percent of people recycle or use the same passwords for all of their online accounts. The criminals also sell the bank and credit card information on the dark web.

Provide a secure online payment gateway. The best tip for businesses is to use special software such as Red Maple's StagedPayTM (now Clever Division) that safeguards credit card information by locking-it up in separate vaults. This simple solution stops hackers from getting complete information and committing more fraud and theft. In addition, Clever Division helps ensure you follow the steps for PCI DSS compliance.

2. Educate your employees

Offer your workers training in cybersecurity, especially those working from home and using their own devices to access your business servers. Criminals are taking advantage of businesses that have not set up security protocols for employees working remotely. New research shows 28% of people admit to using their personal, unsecured devices for work-related activities instead of their work-issued devices, creating new opportunities for cyberattacks.



Let us help you protect your company from cybercrime.
+ 1-830-280-0400 • info@redmaple.com

So far, that exposure has led to more than [one-quarter of businesses](#) paying exorbitant fees from malware infections, ransom ware and breaches. Take steps as well to provide credit card payment security to your customers.

3. Backup your data

Ransomware is the fastest-growing cybercrime against retailers, according to [Cybercrime Magazine](#).

The criminals will hold your most important information hostage until you pay a ransom – and even then, there's no guarantee they'll release the data later. That's why experts recommend you back up your data and computer once a week at minimum, preferably once every 24 hours. In fact, all sensitive information must be backed up daily. Invest in an off-site backup system and provide a hard drive or flash drive for employees to save their files. Backups are cheap insurance that allow you to restore your critical information, keep your customers and stay in business.

BACK UP TIP: To help you track your information, set up a consistent system for naming all files. In the event of a breach, all employees can easily access their files and minimize work interruptions.

By all accounts, cybercrime is expected to grow worse. By the end of 2021, Cybersecurity Ventures estimates global cybercrime will cost \$6 trillion a year or \$16.4 billion every day. By 2025, cybercrime is projected to cost the world \$10.5 trillion every year or some \$28 billion a day. That's why online retailers need to take the risks seriously by preparing for attacks, planning to recover, and educating their employees to prevent future attacks.

Red Maple can help you take the necessary steps today to protect your customer's valuable information with their patented solution called StagedPay (now Clever Division). They offer a variety of Microsoft Dynamics 365 solutions [Learn more](#), [get a quote](#) or [schedule a demo](#).

FAQs



What is the likelihood of a retailer being a victim of ransomware?

According to cybersecurity experts nearly half of all retailers will be hit by ransomware.



How much does a ransomware attack cost a retailer?

According to the Sophos Cybersecurity report, the average ransom retailers pay is almost \$150,000.



How can [Clever Division](#) protect us from a cyberattack?

Clever Division provides several layers of security for your clients. Their credit card information is not stored in its entirety anywhere on your site, so thieves do not have access to their information in the event of a data breach.



Let us help you protect your company from cybercrime.

+ 1-830-280-0400 • info@redmaple.com