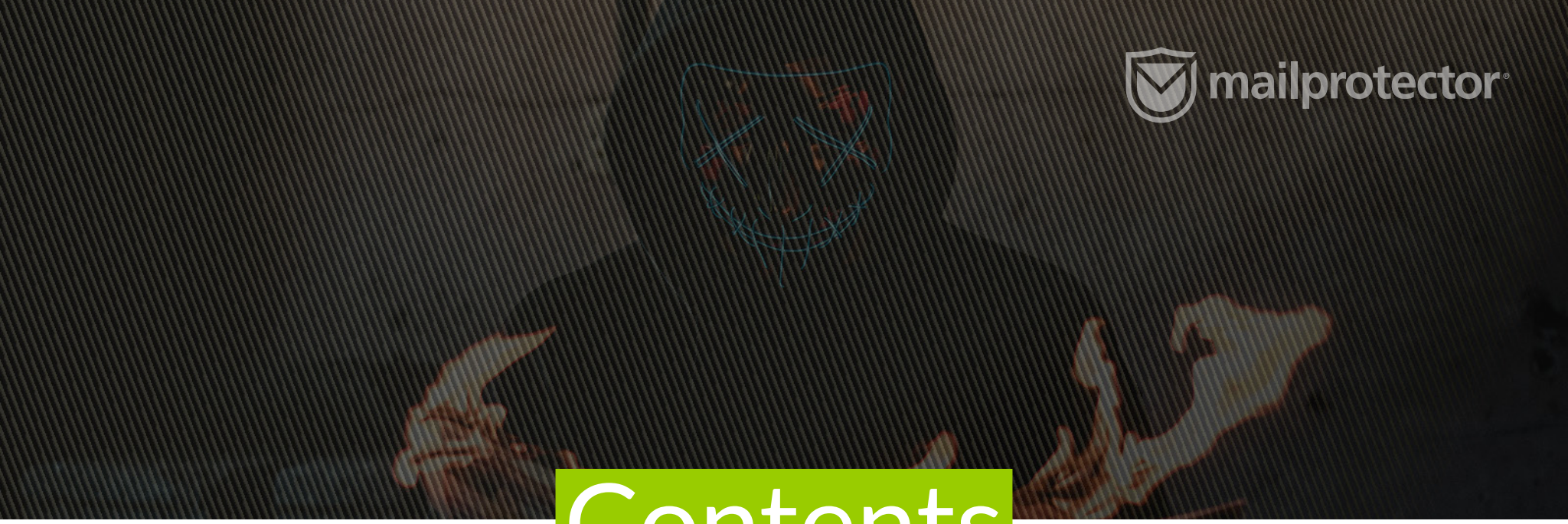
mailprotector

Preventing Ransomware Attacks

Ransomware examples and suggestions for how to improve your organization's cyber-resiliency



Contents

INTRO

Forget the Mafia

Cyberhackers represent the **new wave of organized crime**. Now infamous hackers like REvil and Darkside are creating process and software for wealthy benefactors to deploy in an "as a Service" model. These pirates of the web are making their way into the IT infrastructure of companies everywhere, gaining access and locking systems down until a ransom is paid.

While ransomware has been around since 1989, it has surged in popularity as an easy way for cybercriminals to make money.

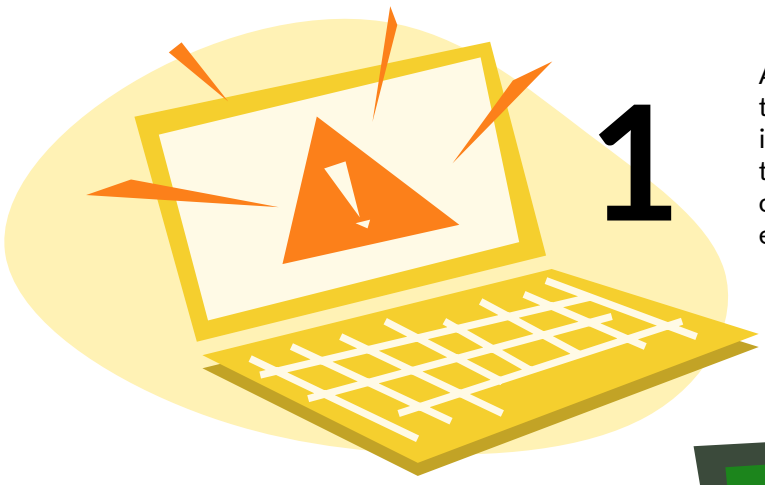
Recently, cyberattackers have been targeting societal infrastructure like ferries and gas lines because the more people impacted, the faster a ransom will be paid. **No one is immune,** as attackers are looking for one thing: money. Even the White House, FBI and intelligence agencies galore are sitting up and taking notice – with activity that is even drawing comparisons to the way our country mobilized against terrorism after the 9/11 attacks.

Is your company is leaving itself vulnerable? In this eBook, **we feature 5 ransomware attacks** and offer ways to keep your users safe and resilient.

WHAT IS RANSOMWARE?

Ransomware comes in all forms these days. In its most basic sense, ransomware is a form of malware put into place by cyber criminals to steal information and hold it for ransom. Once they find their way into an organization's network, hackers block the organization's access through encryption. While they don't always deliver on the promise to return the network back to its pre-attack state, the ploy is that hackers will deliver an encryption key once the ransom is paid. This will allow the organization to go back to operation as usual.

HOW DO RANSOMWARE ATTACKS TYPICALLY PLAY OUT?



An employee clicks a link and unknowingly take actions which allow malware to be installed. Immediately after losing access to their computer, a message shows a list of demands, offering system restoration in exchange for payment.

The ransomware quicky spreads to other employees and systems connected to the network, allowing threat actors to block access to vital systems and instantly bringing normal operations to a screeching halt.

Infected companies (scrambling to find a solution) realize the damage is too extensive and technologically advanced to be undone. They may choose to lose their data and existing hardware, or pay exorbatant fees to regain access to their systems. Most pay.

COMMON RANSOMWARE TACTICS

Another prominent cybercriminal, REvil, uses a tactic called "triple extortion." Here are some quick definitions around the different levels of ransomware attacks:

- ***Traditional Ransomware***
  Breaches a network, then encrypts sensitive data so it is no longer accessible to the data owners. Attackers demand ransom in exchange for the decryption key.

- ***Double Extortion***
  Takes on the look of a traditional ransomware attack, but in this case, sensitive data is threatened to be released to the public in exchange for a ransom payment.

- ***Triple Extortion***
  Uses the same tactics as traditional and double extortion, but it expands its extortion threat to customers, partners and third parties.

Despite national defense and intelligence agencies ramping up their efforts to snuff out ransomware attacks, they have gained popularity as **a hacker's tactic of choice because they are so lucrative**. In the next few pages, you'll learn about recent ransomware attacks, and we'll close our eBook with ways to prevent ransomware attacks.

CASE 1 OCTOBER 28, 2020

UVM Medical Center

WHAT HAPPENED?

The University of Vermont Medical Center represents another phishing attack example in a long list of recent cyberattacks.

During the fall of 2020, employees at the University of Vermont Medical Center started having trouble logging in to their business-critical systems. Suspecting a cyberattack, IT administrators promptly shut down their network. With further investigation, they found a text file on a network computer that read, “We encrypted your data, if you wanna get the key to unencrypt it, contact us.”

Rather than contacting the cyber attackers, administrators immediately contacted the FBI (rather than the attackers themselves).

“Even if you contact them, even if you pay them, you have no guarantee they’re gonna deliver anything,” said Senior VP of Network IT Doug Gentile. “Of course we have standard procedures for if systems go down, but being down for two to three weeks is beyond what we ever expect. It was stressful for people.”

The hospital estimates that the phishing attack cost them almost $50 million in lost revenue.

WHAT WAS AFFECTED?

A hospital employee took their company-issued laptop on vacation and opened what they thought was a personal email from their homeowner's association, later clicking a fraudulent link that opened the door for a hack. Malware was then transferred to the employee's computer. When they returned from vacation, the laptop connected to the hospital network and released into the hospital's network.

Once they discovered the error, hospital officials put up a page designed to keep its patients informed on the breach.

While critical systems were locked down, shockingly no patient data was determined to have been breached.

Popular phishing attack examples include spear phishing (targeted email phishing), vishing (phone call phishing), smishing (text phishing) and pharming (directing traffic to a fraudulent website). Because of the ransom associated, cybercriminals continue to evolve their tactics. However, spear phishing attacks are by far the most popular phishing tactic right now.

HOW HAS THE HOSPITAL REBOUNDED?

UVM Medical Center is now regularly training and testing its employees with simulated phishing attacks to drive further phishing awareness. They are also blocking personal email on employee computers, restricted access to the network, and invested in software that defends against phishing attacks.

There are two great ways to prevent phishing attacks. We detail both in our article, Select the Best Phishing Protection Solution for Your Users.

CASE 2: MAY 8, 2021

Colonial Pipeline

WHAT HAPPENED?

At this point, everyone in the IT community is familiar with the recent Colonial Pipeline cyberattack. In addition to a big ransom payment of $4.4 million, this ransomware attack ultimately resulted in a **temporary closing of the pipeline**, which is a critical part of U.S. petroleum infrastructure. In fact, the Colonial Pipeline supplies nearly half of the Eastern United States with fuel, as it stretches 5,500 miles and transports 2.5 million barrels per day. While the cyberattack on Colonial Pipeline was not the first of its kind, it certainly was one whose grimy tentacles reached millions. **Here's how it went down:**

APR 29

Hackers identifying themselves as "DarkSide" entered the Colonial Pipeline network via VPN using a single compromised password from an unused account that was likely purchased on the dark web. Several days are spent downloading critical business information.

MAY 7

Colonial Pipeline IT employees receive a ransom note demanding cryptocurrency. News of the ransomware attack is escalated internally, then externally, leading to the pipeline being shut down for the first time in its 57-year history as a precaution.

MAY 8-12

Options are explored and eventually a $4.4 million in ransom is paid.

MAY 12

The pipeline is turned back on and the FBI begins to deal with the aftermath.

Outside of Colonial Pipeline allowing itself to be vulnerable to outside threats due to lack of proper IT security protocol, the attack was planned and orchestrated by a growing enemy; organized cyber criminals.

What was always a dishonest money maker for cyber criminals has become big business as hackers have graduated to attacking infrastructure. As seen with Colonial Pipeline, **the more people an attack effects, the larger the motive an organization has to pay hackers** and move on.

Ransomware is a profitable and trending crime for many organized cybercriminals. CrowdStrike reported over 1,400 ransomware and data extortion incidents in 2020. Just since the Colonial Pipeline attack in late April, attacks have been made on government agencies, a Florida water system, schools, health care institutions, the meat industry and even a ferry service to Martha's Vineyard. Such assaults have caused FBI director Christopher Wray to draw comparisons to the government response taken after the September 11 terrorist attacks.

WHAT DATA DID DARKSIDE STEAL?

In addition to Colonial Pipeline, cyber criminals calling themselves "DarkSide" have been very active lately, most recently attacking the European subsidiaries of Toshiba. In another ransomware attack of a large US-based manufacturing company, DarkSide **published a list** of what was stolen.

The list includes data related to:

- ***Accounting***
- ***Finance***
- ***Human Resources***
- ***Employee Confidential Data (photos, taxes, benefits)***
- ***Marketing***
- ***Budgets***
- ***Taxes (sales tax compliance, property, income, franchise taxes)***
- ***Payroll***
- ***Banking Data***
- ***Arbitration***
- ***Scans***
- ***Insurance***
- ***Reconciliations***
- ***Reports (monthly bank inventory, monthly financial, claims reports)***
- ***Audits (DHG, insurance audits)***
- ***B2B clients config data***
- ***Confidentiality 2020***
- ***2020, 2021 Business Plans***
- ***2019, 2020, (2021 YTD) years closing (full dumps)***

DarkSide concluded the list by saying in addition to the list above, **they also stole "a lot of other sensitive data."** "Other sensitive data" might include things like embarrassing email conversations hackers can now use to compromise the company's brand.

CASE 3 MAY 31, 2021

JBS

WHAT HAPPENED?

Cybercriminals are keeping their sights aimed high as Brazilian-based JBS S.A., the world's largest meat processor, was attacked with ransomware on May 31, 2021. JBS joins other giants, Wendy's, Molson Coors, and E & J Gallo Winery as those recently attacked in the food industry. JBS is one of the largest beef importers to the United States and Canada.

The FBI is attributing the attack to Russian-based cybercriminals, REvil. For financial gain, REvil (pronounced R-eevuhl and short for Ransomware Evil) threatens to post stolen information to their "happy blog" for the world to see.

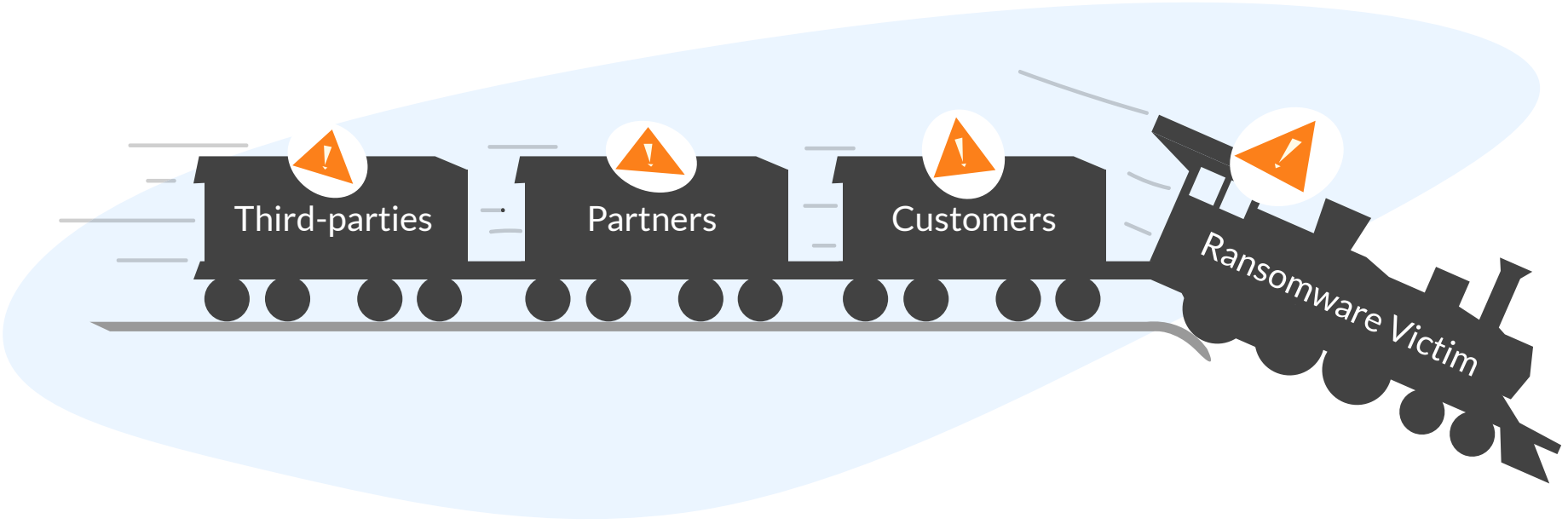
WHAT WAS AFFECTED?

The exact attack details were not made public but here's what we do know. REvil attacked servers that supported JBS's North American operations, while JBS reported that its backup servers were not affected. The cyberattack led to **the preventative shutting down of 84 facilities** in the U.S., Canada and Australia.

"The company took immediate action, suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation," JBS USA said in a statement.

THE TRIPLE THREAT

REvil reportedly used a tactic called “triple extortion” in its breach of the JBS servers, although customer and third parties have not been publicly identified. Triple Extortion ransomware attacks take down not only the original target of the attack, but other businesses and organizations associated with them as well. When this happens it severely, and often irreversably damages B2B relationships.



WHAT WAS THE RESOLUTION?

Once addressed, the attack seemed to cause minimal disruption, as meat has a 14-day window to move through the market. Since **the plants were closed for about a day or two**, the company can make up for lost time with extra shifts. The FBI has reached out to other major meat processors asking them to make up for missed production. JBS has not disclosed whether or not it paid the hackers.

WHAT HELPED JBS MINIMIZE DAMAGE?

JBS followed some IT industry best practices, particularly by having off-network backup servers. Solid email security also plays an enormous role in preventing ransomware attacks, particularly when you deploy an **easy-to-adopt encrypted email policy**. Keep reading to see some further recommendations we have compiled to help you keep your customers safe.

CASE 4: JUNE 1, 2021

FUJIFILM

WHAT HAPPENED?

Japanese multi-national conglomerate, FUJIFILM, detected **unauthorized access** to some of its servers on June 1, 2021. This activity ultimately resulted in a full-blown ransomware attack.

The global manufacturing giant says on Friday, June 4, it confirmed that the impact of the unauthorized server access was confined to a specific network in Japan.

While FUJIFILM has not elaborated on the nature of the attack, experts in the space are suggesting it might have been a Qbot attack, traditionally a banking trojan virus designed to steal personal information. **Cyber criminals initiate this virus using spam email campaigns**.

WHAT FUJIFILM OPERATIONS DID QBOT AFFECT?

The attack disabled emails, phone calls and prevented the company from accepting and processing orders. Preventatively and in order to determine the extent of the attack, FUJIFILM **shut down all networks and servers, and suspended all affected systems**.

FUJIFILM denied paying ransom because, based on their own findings of the attack, the hackers were unable to attain sensitive information. They decided to use backups to restore their operations.

KNOW WHEN TO HOLD 'EM OR FOLD 'EM

A note about denying ransom: Only in a situation where an organization is confident enough that sensitive data was not stolen can it ignore a ransom request.

Once the threat was isolated and FUJIFILM determined no additional risk to other networks, servers and equipment it restored backups and brought all systems back online.

FUJIFILM BOUNCES BACK

Thankfully FUJIFILM had their act together, so they were able to **isolate and eliminate the threat** to the point of not paying ransom. Like at FUJIFILM, so many attacks like this can be prevented with good email security.

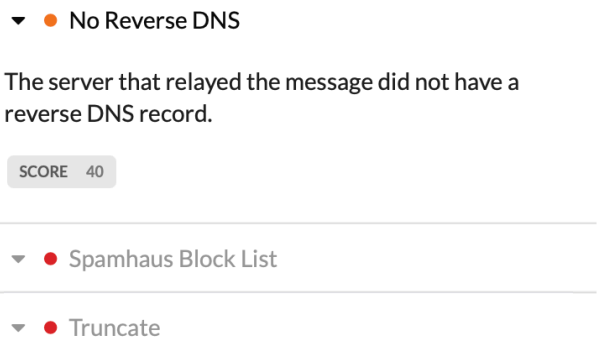
In fact, one of the popular malware methods used by REvil is a Qbot (or Qakbot). A Qbot makes its way into a network to steal sensitive data. Hackers activate a Qbot using email links and attachments. A good email filtering service that lets you preview content in a secure environment (such as CloudFilter from Mailprotector) allows users to see a lot of other information around the message. When certain details such as geographic origin are known, it becomes obvious that a message was sent with ill intent.

Staying protected: Mailprotector's CloudFilter email filtering tool helps individual users understand whether or not a quarantined message is safe, by revealing important analytics around data which is usually obfuscated by complex and hard to read message headers and delivery logs. When properly informed, most users will recognize the illegitimacy of a message and dodge the threat.

Obvious junk

SCORE: 540

DECISION: Quarantine spam



CASE 5: JUNE 3, 2021

Cox Media Group

WHAT HAPPENED?

At least nine Cox Media Group stations were targeted in a ransomware attack on June 3, 2021. Details of the attack have not been made public, as Cox Media Group hasn't made any comments to the public, however we can report on what happened as a result of the attack.

HOW WAS COX MEDIA GROUP AFFECTED?

Because the attack **crippled the live stream of the news broadcasts**, all TV stations had to either show replays of old news broadcasts or had to replace regularly scheduled broadcasts with national news broadcasts.

Two of the **affected stations told employees to stay home** as an extra precaution. Cox Radio Group radio stations were also taken down. Cox Media Group contacted employees shortly after the threat began by and asked to turn off company-issued devices and not access their Cox email. Many were **asked to delete social media posts** about the outages. This caused some frustration among Cox employees, who wanted to tell viewers why they were offline.

Due to the recent string of ransomware attacks that are affecting critical infrastructure, authorities at the U.S. Department of Justice, FBI and even the office of President Biden are getting involved. They have insinuated that they'll be using similar tactics to root out hackers as they do for terrorists.

CASE 6 JUNE 2, 2021

Massachusetts Steamship Authority

WHAT HAPPENED?

The Massachusetts Steamship Authority was attacked by hackers on June 2, 2021. Cyberattackers targeted the entity's website and booking system where passengers can schedule ferries to places like Martha's Vineyard and Nantucket. This marks another **infrastructure-related attack** following other recent malware hacks to Colonial Pipeline, JBS and Cox Media Group.

HOW WAS THE STEAMSHIP AUTHORITY AFFECTED?

First and foremost, the attack hampered the Steamship Authority's ability to schedule passengers for trips from June 2 until the booking website was operational again on June 12.

While the actual ships themselves were operational, **passengers could not schedule trips** over the phone or on the website. During the downtime, passengers could purchase tickets in person, but the Steamship Authority proposed people use cash. In the aftermath, the Steamship Authority waived cancellation and rescheduling fees for affected customers. They also temporarily extended its reservation hours to better accommodate customers.

6 Tips for Preventing Ransomware Attacks

Ransomware is a growing global crime with tentacles that are far-reaching. The IT community at large is increasingly looking to master how to prevent ransomware attacks for their own users.

Did you know?

Ransomware trojan viruses like Qbot (also called Qakbot) are programmed to steal personal information. This virus is initiated using spam email campaigns so it can be prevented by regular email encryption.

According to a recent TechCrunch article, "Ransomware attacks have been on the rise since the start of the COVID-19 pandemic, so much so that they have become the biggest single money earner for cybercriminals." One expert firm estimates that the quantity of ransomware attacks grew by more than 150% in 2020, and that the average ransom demand increased more than twofold to $170,000. The White House even went as far as to publish an open letter to US companies, urging organizations to "take ransomware crime seriously" and ensure "corporate cyber defenses match the threat."

Here are 6 recommendations we have compiled to help your organization prevent ransomware attacks so your users, and associates might never have to deal with one.

1. **Multi-Factor Authentication is a must.** This necessary electronic authentication method discourages hacking and ensures the safety of your users.

2. **Encrypt email to prevent unwanted visibility into your sensitive data.** Tools that are simple to use will be the most adopted by your community of users. The Bracket email encryption tool fits the bill perfectly.

3. **Back up data regularly and keep backups outside of the network(s) you manage.** There are some great Business Continuity and Disaster Recovery companies out there these days, such as Kaseya, Acronis, Veeam, Axcient and Datto.

4. **Keep the network(s) you manage up to date by running anti-virus and anti-malware scans.** Also, make sure you are regularly allowing updates on operating systems, software and applications.

5. **Educate your users on what to click and what not to click.** Organizations are only as secure as their least secure user. Educate users on what phishy email attachments and malicious links look like to prevent hackers from gaining access.

6. **Implement endpoint security.** Endpoint security, or endpoint protection, will safeguard end points, servers and mobile devices against security threats.

How can Mailprotector Help?

Stop ransomware and other email-based attacks in the cloud

CloudFilter™

Spam and malware are here to stay. Email-based threats to organizations and individuals continue to grow increasingly sophisticated as spammers innovate new tactics for evading spam and virus filtration systems. CloudFilter™ stops the junk and lets the good email through. Messages containing offensive, harmful, or policy violating content are held for user review, while good messages continue on their way. CloudFilter keeps users safe in an ever-changing email threat landscape and gives you confidence that your email infrastructure is **shielded from email-based threats**. And because there's nothing to install, you never again have to worry about updating definitions or following the latest email security trends.

Get the world's easiest to use encrypted email and file transfer

Bracket®

Email encryption has a reputation for being a pain to use. You have to create an account, download and install an app or plugin, open the app, sign in, and finally create and send your message. Then the recipient on the other end has to repeat all the same steps just to read the message. Bracket is so much easier to use. **It's even patented!** There's nothing to install or maintain. Email is encrypted from any client on any device, by wrapping the [subject] in brackets. Plus, with Bracket Share (included) you can safely send and receive files up to 1GB effortlessly. The encryption techniques Bracket employs to secure your email data are state of the art. Bracket is built on a globally distributed, multi-layer AES-256 encryption design with automatic key rotation, so you never have to wonder if your data is safe.

AND MUCH MORE...

Mailprotector gives MSPs everything they need to provision user-friendly, secure, and legally compliant email from a single vendor. Get in touch!

Since 1999, Mailprotector has poured itself into perfecting a secure, intuitive, and easily administered set of email security, compliance, and encryption solutions. These were developed in tandem with, and in consideration of, our global IT security partners and their base of users. Now you can have peace of mind knowing your users are secure and happy, while devoting time to other areas of your business.

mailprotector®

Learn more at mailprotector.com or email sales@mailprotector.com