**Ransomware**

Ransom malware, or [ransomware](https://blog.malwarebytes.com/threats/ransomware/), is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

**Types of ransomware**

There are three main types of ransomware, ranging in severity from mild to extremely dangerous. They are as follows:

1. **Scareware-** It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you’ll likely continue to be bombarded with pop-ups, but your files are essentially safe.

A legitimate cybersecurity software program would not solicit customers in this way. If you don’t already have this company’s software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you wouldn’t need to pay to have the infection removed—you’ve already paid for the software to do that very job.

1. **Screen lockers -** When lock-screen ransomware gets on one’s computer, it means that they will get frozen out of their PC entirely. Upon starting up their computer, a full-size window will appear, often accompanied by an official-looking police department seal saying illegal activity has been detected on one’s computer and they must pay a fine. However, the police would not freeze someone out of their computer or demand payment for illegal activity. If they suspected someone of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.
2. **Encrypting ransomware-** Encryption ransomware snatches up one’s files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get a hold of your files, no security software or system restore can return them to you. Unless you pay the ransom—for the most part, they’re gone. And even if you do pay up, there’s no guarantee the cybercriminals will give you those files back.

**Targets of ransomware attacks**

Ransomware can spread across the Internet without specific targets. But the nature of this file-encrypting malware means that cybercriminals also are able to choose their targets. This targeting ability enables cybercriminals to go after those who can — and are more likely to — pay larger ransoms. Four target groups and how each may be impacted:

* **Groups that are perceived as having smaller security teams**- Universities fall into this category because they often have less security along with a high level of file-sharing
* **Organizations that can and will pay quickly**- Government agencies, banks, medical facilities, and similar groups constitute this group, because they need immediate access to their files and may be willing to pay quickly to get them.
* **Firms that hold sensitive data**- Law firms and similar organizations may be targeted, because cybercriminals bank on the legal controversies that could ensue if the data being held for ransom is leaked.
* **Businesses in the Western markets**- Cybercriminals go for the bigger payouts, which means targeting corporate entities. Part of this involves focusing on the United Kingdom, the United States, and Canada due to greater wealth and personal-computer use.

## Ways to prevent a ransomware attack

Ransomware is a profitable market for cybercriminals and can be difficult to stop. Prevention is the most important aspect of protecting one’s personal data. To deter cybercriminals and help protect ourselves from a ransomware attack, we can keep in mind the following points:-

1. **Do use security software**- To help protect your data, install and use a trusted security suite that offers more than just antivirus features. Use reputable antivirus software and a firewall. Maintaining a strong firewall and keeping your security software up to date are critical. It’s important to use antivirus software from a reputable company because of all the fake software out there.
2. **Do keep your security software up to date**- New ransomware variants continue to appear, so having up-to-date internet security software will help protect you against cyberattacks.
3. **Do update your operating system and other software**- Software updates frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
4. **Don’t automatically open email attachments**- Email is one of the main methods for delivering ransomware. Avoid opening emails and attachments from unfamiliar or untrusted sources. Phishing spam in particular can fool you into clicking on a legitimate-looking link in an email that actually contains malicious code. The malware then prevents you from accessing your data, holds that data hostage, and demands ransom.
5. **Never click on unverified links-** Avoid clicking links in spam emails or on unfamiliar websites. Downloads that start when you click on malicious links is one way that your computer could get infected
6. **Never use unfamiliar USBs-** Never insert USBs or other removal storage devices into your computer if you do not know where they came from. Cybercriminals may have infected the device with ransomware and left it in a public space to lure you into using it.
7. **Avoid giving out personal data-** If you receive a call, text, or email from an untrusted source that asks for personal information, do not give it out. Cybercriminals planning a ransomware attack may try to gain personal data in advance of an attack. They can use this information in phishing emails to target you specifically. The aim is to lure you into opening an infected attachment or link. Do not let the perpetrators get hold of data that makes their trap more convincing. If you get contacted by a company asking for information, ignore the request, and contact the company independently to verify it is genuine.
8. **Do back up important data to an external hard drive**- Attackers can gain leverage over their victims by encrypting valuable files and making them inaccessible. If the victim has backup copies, the cybercriminal loses some advantage. Backup files allow victims to restore their files once the infection has been cleaned up. Ensure that backups are protected or stored offline so that attackers can’t access them.
9. **Do use cloud services**- This can help mitigate a ransomware infection, since many cloud services retain previous versions of files, allowing you to “roll back” to the unencrypted form.

**Responding to a ransomware attacks**

In the event of a ransomware attack, simple steps to follow to minimize damage are-

### Isolate your computer- If you experience a ransomware attack, the first thing to do is to disconnect from any networks and the internet. Disconnecting in this way, isolates your computer and minimizes the chance of the ransomware infection spreading to other computers.

### Never pay the ransom- Do not pay any ransom demanded by the cybercriminals carrying out the ransomware attack. Like a real-life hostage situation, it is best not to negotiate with cybercriminals. Paying the ransom will not guarantee the return of your data — after all these individuals have already manipulated your trust. Caving in and paying also encourages this sort of crime. The more people that pay the ransoms, the more popular ransomware attacks become.

### Start ransomware removal- To rid your computer of ransomware, we can follow the following simple steps:

### Step 1: Disconnect from the internet- First up, disconnect from the internet to stop the ransomware spreading to other devices.

### Step 2: Run a scan using internet security software- Use the internet security software you have installed to run a scan. This will help to identify any threats. If it detects any risky files, they can be removed or quarantined.

### Step 3: Use ransomware decryption tool- If your computer gets infected with encryption ransomware, you will need to use a [ransomware decryptor](https://noransom.kaspersky.com/) to decrypt your files and data so that you can access them again. Various companied that produce internet security software continually research the latest forms of ransomwares and create ransomware decryptors to counter new threats.

### Step 4: Restore files from backup- If you have backed up your data externally or on cloud storage, restore a clean backup of all your files on your computer. This allows you to revert to a version of the software that is malware free.

### ****1. Ryuk, 2019 and 2020****

Like most infections caused by ransomware, Ryuk is spread mainly via malicious emails, or phishing emails, containing dangerous links and attachments. The ransom amount to be paid to release an entire system can exceed USD 300,000, making Ryuk one of the most expensive ransomware in history, well above the average.

According to the FBI, Ryuk's attacks have already caused more than USD 60 million in damage worldwide since this type of ransomware gained prominence in 2018 after stopping the operations of major newspapers in the United States. More than 100 companies suffered attacks.

In 2020, for example, EMCOR Group (engineering and industrial construction company) and Epiq Global (legal services company) suffered incidents involving Ryuk.

An interesting fact is that Ryuk's ransom notes contain contact emails with the end @protonmail.com or @tutanota.com. The victim needs to send a message to find out how much they must pay for the decryption key.

### ****2. SamSam, 2018****

SamSam ransomware was identified a few years ago, more precisely in late 2015. But it was in 2018 that it gained much more prominence after infecting the city of Atlanta, the Colorado Department of Transportation and the Port of San Diego, in the U.S., abruptly stopping services.

In the same year, two Iranian hackers were accused of using SamSam against more than 200 organizations and companies in the U.S. and Canada, including hospitals, municipalities and public institutions. A loss of USD 30 million is estimated as a result of the attacks.

Just the city of Atlanta spent more than USD 2 million to repair the damage. Hancock Health, an Indiana hospital, paid a ransom of USD 55,000. To spread, this type of ransomware often exploits vulnerabilities in Remote Desktop Protocols (RDP) and File Transfer Protocol (FTP).

A curious fact about SamSam is that the victim is asked to make a first payment for a first key, which would unlock only a few machines. It would be like a sign of honesty.

“With buying the first key you will find that we are honest”, says the ransomware message. Would you believe that?

### ****3. WannaCry, 2017****

One of the most devastating ransomware attacks in history in terms of loss volume was caused by WannaCry, launched in 2017. The estimated value at the time was USD 4 billion in losses. The amount required to release each machine was around USD 300.

WannaCry spread via email scams, or phishing. Worldwide, more than 200 thousand people and companies were affected, such as, for example, FedEx, Telefonica, Nissan and Renault. WannaCry exploits a vulnerability in Windows.

By the way, even today there are phishing emails claiming that you were infected by WannaCry, demanding ransom payment. But they’re plain emails, with no files. Pay attention!

### ****4. Petya, 2016****

Petya is a ransomware that started to be propagated in 2016, via emails with malicious attachments. Since its launch, it's estimated that different variations of Petya have caused more than USD 10 billion in financial losses.

Petya acts by infecting the boot record of machines that use the Windows system. That is, it blocks the entire operating system. To unlock, you need to pay a ransom of around USD 300 per user.

This type of ransomware affected different organizations in the world, such as banks and companies in the areas of transportation, oil, food and health. Let us cite as an example the National Bank of Ukraine, Mondelez (food company), Merck (pharmaceutical company) and Rosneft (oil company).

**There are a few dos and don’ts when it comes to ransomware.**

1. Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
2. Restore any impacted files from a known good backup. Restoration of your files from a backup is the fastest way to regain access to your data.
3. Do not provide personal information when answering an email, unsolicited phone call, text message or instant message. Phishers will try to trick employees into installing malware, or gain intelligence for attacks by claiming to be from IT. Be sure to contact your IT department if you or your coworkers receive suspicious calls.
4. Use reputable antivirus software and a firewall. Maintaining a strong firewall and keeping your security software up to date are critical. It’s important to use antivirus software from a reputable company because of all the fake software out there.
5. Do employ content scanning and filtering on your mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
6. Do make sure that all systems and software are up-to-date with relevant patches. Exploit kits hosted on compromised websites are commonly used to spread malware. Regular patching of vulnerable software is necessary to help prevent infection.
7. If traveling, alert your IT department beforehand, especially if you’re going to be using public wireless Internet. Make sure you use a trustworthy Virtual Private Network (VPN) when accessing public Wi-Fi like Norton Secure VPN.

Once the ransomware is on your computer, it will encrypt your data or lock your operating system. Once the ransomware has something to hold as ‘hostage,’ it will demand a ransom so that you can recover your data. Paying these ransoms may seem like the simplest solution. However, this is exactly what the perpetrator wants you to do and paying these ransoms does not guarantee they will give you access to your device or your data back.

### Do not open untrusted email attachments

Another way that ransomware could get onto your computer is through an email attachment.

Do not open email attachments from senders you do not trust. Look at who the email is from and confirm that the email address is correct. Be sure to assess whether an attachment looks genuine before opening it. If you’re not sure, contact the person you think has sent it and double check.

Never open attachments that ask you to enable macros to view them. If the attachment is infected, opening it will run the malicious macro, giving the malware control over your computer.

### Only download from sites you trust

To reduce the risk of downloading ransomware, do not download software or media files from unknown websites.

Go to verified, trusted sites if you want to download something. Most reputable websites will have markers of trust that you can recognize. Just look in the search bar to see if the site uses ‘https’ instead of ‘http.’ A shield or lock symbol may also show in the address bar to verify that the site is secure.

If you’re downloading something on your phone, make sure you download from reputable sources. For example, Android phones should use the Google Play Store to download apps and iPhone users should use the App Store.

### Avoid giving out personal data

If you receive a call, text, or email from an untrusted source that asks for personal information, do not give it out.

Cybercriminals planning a ransomware attack may try to gain personal data in advance of an attack. They can use this information in phishing emails to target you specifically.

The aim is to lure you into opening an infected attachment or link. Do not let the perpetrators get hold of data that makes their trap more convincing.

If you get contacted by a company asking for information, ignore the request, and contact the company independently to verify it is genuine.

### Use mail server content scanning and filtering

Using content scanning and filtering on your mail servers is a smart way to prevent ransomware.

This software reduces the likelihood of a spam email containing malware-infected attachments or links from reaching your inbox.

### Never use unfamiliar USBs

Never insert USBs or other removal storage devices into your computer if you do not know where they came from.

Cybercriminals may have infected the device with ransomware and left it in a public space to lure you into using it.

### Keep your software and operating system updated

Keeping your software and operating system updated will help protect you from malware. Because when you run an update, you are ensuring that you benefit from the latest security patches, making it harder for cybercriminals to exploit vulnerabilities in your software.

### Use a VPN when using public Wi-Fi

Being cautious with public Wi-Fi is a sensible ransomware protection measure.

When you use public Wi-Fi, your computer system is more vulnerable to attack. To stay protected, avoid using public Wi-Fi for confidential transactions, or use a secure VPN.

### Use security software

As cybercrime becomes more widespread, ransomware protection has never been more crucial. Protect your computer from ransomware with a comprehensive internet security solution like [Kaspersky Internet Security](https://usa.kaspersky.com/internet-security).

When you download or stream, our software blocks infected files, preventing ransomware from infecting your computer and keeping cybercriminals at bay.

### Keep security software updated

To benefit from the highest level of protection that internet security software has to offer, ensure you keep it updated. Each update will include the latest security patches and maximize ransomware prevention.

### Backup your data

Should you experience a ransomware attack, your data will remain safe if it is backed up. Make sure to keep everything copied on an external hard drive but be sure not to leave it connected to your computer when not in use. If the hard drive is plugged in when you become a victim of a ransomware attack, this data will also be encrypted.

Ransomware attacks can be deployed in different forms. Some variants may be more harmful than others, but they all have one thing in common: a ransom. Here are seven common types of ransomware.

* **Crypto malware**. This form of ransomware can cause a lot of damage because it encrypts things like your files, folders, and hard-drives. One of the most familiar examples is the destructive 2017 WannaCry ransomware attack. It targeted thousands of computer systems around the world that were running Windows OS and spread itself within corporate networks globally. Victims were asked to pay ransom in Bitcoin to retrieve their data.
* **Lockers**. Locker-ransomware is known for infecting your operating system to completely lock you out of your computer or devices, making it impossible to access any of your files or applications. This type of ransomware is most often Android-based.
* **Scareware**. Scareware is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the problems. Some types of scareware lock your computer. Others flood your screen with annoying alerts and pop-up messages.
* **Doxware**. Commonly referred to as leakware or extortionware, doxware threatens to publish your stolen information online if you don’t pay the ransom. As more people store sensitive files and personal photos on their computers, it’s understandable that some people panic and pay the ransom when their files have been hijacked.
* **RaaS**. Otherwise known as “Ransomware as a service,” RaaS is a type of malware hosted anonymously by a hacker. These cybercriminals handle everything from distributing the ransomware and collecting payments to managing decryptors — software that restores data access — in exchange for their cut of the ransom.
* **Mac ransomware**. Mac operating systems were infiltrated by their first ransomware in 2016. Known as KeRanger, this malicious software infected Apple user systems through an app called Transmission, which was able to encrypt its victims’ files after being launched.
* **Ransomware on mobile devices**. Ransomware began infiltrating mobile devices on a larger scale in 2014. What happens? Mobile ransomware often is delivered via a malicious app, which leaves a message on your device that says it has been locked due to illegal activity.