



The McAfee Safety Series

# Ransomware Security Guide



# Table of Contents



**Protecting what's precious** **3**

**What is ransomware?** **4**

Who do hackers target with ransomware attacks? **5**

What does ransomware look like? **7**

Can smartphones get ransomware too? **9**



**Ransomware prevention** **10**

Best defenses against ransomware **11**

What to do if you're the victim of a ransomware attack **14**



**You're your own best defense** **15**

**About McAfee** **16**



## Protecting what's precious

Ransomware. Arguably one of the most malicious attacks hackers have in their bag.

One reason why, it can feel personal. Ransomware targets some of the most precious and important things you have on your devices, like your photos, files, and financial records too—and holds them for ransom. Still, even if you pay, there's no guarantee that you'll get them back.

Yet you absolutely have ways you can protect yourself.

Ransomware affects everyone. From individuals to businesses to governmental bodies of all sizes, hackers target them all. Often, they do it for the money. Other times, they do it out of spite—simply to hurt and harm others. And on a yet larger scale, ransomware attacks target businesses and portions of critical infrastructure, such as the Colonial Pipeline attack that made headlines in 2021.

Whatever ends they have in mind, hackers have made ransomware a rising form of attack that costs people and organizations billions of dollars worldwide.

Hackers know what you value, and ransomware gives them a way to exploit it. Yet there's plenty you can do to protect yourself, and that's what we'll focus on in this guide.

We'll start with what ransomware looks like and how it works, followed by the straightforward things you can do to prevent it, along with the steps to take if the unfortunate ends up happening to you or someone you know.

Without question, your data is precious and important. Let's protect it.



## What is ransomware?

Ransomware attacks effectively hold information hostage, promising its release only if a ransom is paid.

More specifically, it's a type of malware. It infects a network or a device and then typically encrypts the files, data, and apps stored on it, digitally scrambling them so the proper owners can't access them, often using sophisticated methods of cryptography that are nearly impossible to undo.

And as a name implies, the hacker then demands a ransom for release—often in the form of cryptocurrency because it's so difficult to trace. However, paying that ransom may or may not restore the encrypted information. A hacker could figuratively take the money and run, leaving the victim with an unusable batch of scrambled data. In fact, some estimates show that only 8% of victims who pay the ransom actually recover their data.<sup>1</sup>

Additionally, a hacker could use ransomware to further steal files and data and then post them online for all to see, a practice known as doxing. For individuals, doxing could damage their identity, privacy, or even reputation. For businesses and organizations, doxing could expose customer data, trade secrets, or other information that could not only compromise their operations but other people as well.

Clearly, a ransomware attack can get quite ugly—which makes it good to know you can go a long way toward preventing them.

## Who do hackers target with ransomware attacks?

Ransomware can affect anyone. An attack can target a person at home, or it can target some of the largest organizations out there.

Organized hacking groups tend to go after bigger game, so to speak, like major corporations, government agencies, and even critical infrastructure. Given the scope of these attacks and their potential impact, organized hackers will demand ransoms that can run well into the millions of dollars.

A few recent examples of large-scale attacks include:

- **JBS Foods, May 2021:** Organized ransomware attackers targeted JBS's North American and Australian meat processing plants, which disrupted the distribution of food to supermarkets and restaurants. Fearing further disruption, the company paid more than \$11 million worth of Bitcoin to the hacking group responsible.
- **Colonial Pipeline, May 2021:** In an attack that made major headlines, a ransomware attack shut down 5,500 miles of pipeline along the east coast of the U.S. Hackers compromised the network with an older password found on the dark web, letting the hackers inject their malware into Colonial's systems. The pipeline operator said they paid nearly \$4.5 million to the hackers responsible, some of which was recovered by U.S. law enforcement.
- **Kaseya, July 2021:** As many as 1,500 companies had their data encrypted by a ransomware attack that followed an initial ransomware attack on Kaseya, a company that provides IT solutions to other companies. Once the ransomware infiltrated Kaseya's systems, it quickly spread to Kaseya's customers. Rather than pay the ransom, Kaseya' co-operated with U.S. federal law enforcement and soon obtained a decryption key that could restore any data encrypted in the attack.




That's not to say that hackers show little interest in attacking individuals. While the potential ransom payout is far lower with individuals, hackers can cast a far wider net for victims and rack up ransom money in volume. Hundreds of successful attacks at hundreds of dollars each quickly add up.

Moreover, these ransomware attacks require relatively low levels of effort. Small-time hackers and hacking groups can find the tools they need to conduct such attacks by shopping on the dark web, where ransomware is available for sale or for lease as a service (Ransomware as a Service, or RaaS). In effect, near-amateur hackers can grab a ready-to-deploy attack right off the shelf.

Such RaaS attacks have a flip side, though. Because the ransomware kits are available online, the keys to decrypt those attacks are online as well. Potentially, a victim could decrypt the data themselves, provided they know which key to use. However, the risk is that decrypting information with the wrong key can make the issue worse.

Put plainly, attempting to handle a ransomware attack on your own falls into the category of "don't try this at home." That calls for the services of a professional security specialist who can help you assess the risk and take the proper steps in return.



Hundreds of  
successful attacks  
at hundreds of  
dollars each  
quickly add up.

## What does ransomware look like?

The more things change, the more things stay the same.

A typical ransomware attack on a computer or smartphone today follows a format that dates back decades. The first documented ransomware attack occurred in the late 1980s when malware-loaded floppy disks plagued members of the medical research community. Known as “PC Cyborg,” the malware would lie in wait until the user rebooted their computer for the 90th time and then presented them with a digital ransom note.

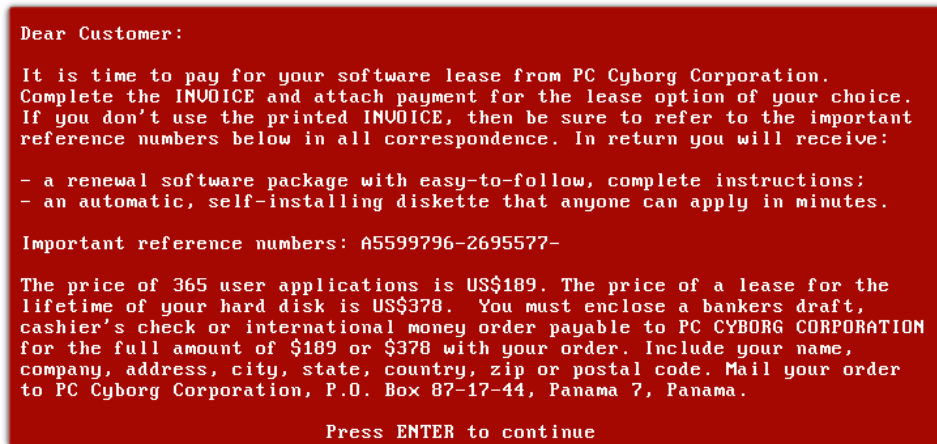


Figure 1. Early example of ransomware – Source, Wikipedia

From there, PC Cyborg would encrypt the computer’s files and victims could only unencrypt them if they paid a fee. Of course, this was long before cryptocurrency, let alone before the internet established itself in our homes and offices. Thus, the payment method: a cashier’s check or money order sent to a post office box in Panama.

Skip ahead nearly 30 years to 2017’s “WannaCry” attacks, and the digital ransom note of today works in much the same way—although with a few new wrinkles.



Figure 2. Example of the WannaCry ransomware, 2017

## SECURITY GUIDE

Once again, a window dominates the screen and announces the attack. A description of what's happened and how to pay the ransom follows, just like before. The newer elements include a couple of countdown timers that further ratchet up the urgency, along with demanding Bitcoin as a form of payment. No more cashier's checks and no more post office boxes. This attack exploits the anonymity of the internet and takes steps to shield the identity of the crook.

Otherwise, the way a ransomware attack looks and feels remains much the same as it did at the start. Yet when you consider how much of our personal, financial, and professional lives we keep on our computers and smartphones today, the stakes are far higher than they ever were. That aspect of ransomware attacks has most certainly changed since the days of PC Cyborg.

**DOOPS, YOUR IMPORTANT FILES ARE ENCRYPTED**

**IF YOU SEE THIS TEXT, THEN YOUR FILES ARE NO LONGER**

**HAVE BEEN ENCRYPTED. PERHAPS YOU ARE BUSY LOOKING**

**FILES, BUT DON'T WASTE YOUR TIME. NOBODY CAN RECOVER**

**DECRYPTION SERVICE.**

**WE GUARANTEE THAT YOU CAN RECOVER ALL YOUR FILES SA**

**NEED TO DO IS SUBMIT THE PAYMENT AND PURCHASE THE C**



## Can smartphones get ransomware too?

Yes. Although it can take different forms.

Some mobile ransomware will encrypt files, photos, and the like on a smartphone, just as it can on computers and networks. Yet other forms of mobile ransomware don't have to encrypt data to make the phone unusable. The "Lockerpin" ransomware that has struck some Android devices in the past would change the PIN number that locked the phone, and other forms of lock screen ransomware would simply paste a warning over the home screen with a "pay up, or else" message.

Even with billions of smartphone users around the world, smartphone ransomware isn't as prevalent as ransomware that targets other devices and networks. There are a few reasons for this.

- Apple's iOS operating system "sandboxes" applications on their mobile devices, which limits the resources that apps can tap into. Moreover, Apple requires all iOS apps to be sold in its App Store, which has measures in place to root out malware as part of the company's app submission process.
- Likewise, Android has similar measures in its app submission process. However, third-party app stores likely have no such measures in place, which counts as one more good reason not to use them because they can harbor apps with malware in all its forms, including ransomware.
- That's not to say that legitimate app stores are completely free of malicious apps. They do sneak through, and you can [find out how you can shop for apps safely with a look at this blog article](#).

So as far as your household goes, whether it's your network, computers, or smartphones, they can all benefit from malware and ransomware protection. The simple fact that they're connected makes them subject to attack.

Yet the good news is this: you can put protections in place rather easily, which we'll cover next.





## Ransomware prevention

Some of ransomware prevention comes down to avoiding human error.

Like so many other types of malware, ransomware ends up on networks and devices because someone clicked a bad link, downloaded a sketchy file, reused a password that was hacked, or had a momentary lapse in judgement. These mistakes can get made in several ways:

- **Downloads from malicious sites**, where bad actors direct you to the site and trick you into downloading malware.
- **Falling victim to a phishing attack**, whether via an email, direct message, text, or some form of electronic message, bad actors will embed links or attachments to trick you into installing ransomware onto your device.
- **Exploiting security loophole**, which may include attacking out-of-date apps or an operating system that's missed a crucial security update. It can also include abusing stolen or hacked password that hasn't seen an update in some time. Additionally, using the internet without the protection of a firewall can expose devices to attack.
- **Shopping in un reputable app stores**, like the third-party app stores mentioned before—where hackers inject ransomware into otherwise innocent-looking apps.
- **Trusting an imposter**, such as social engineering attacks where the hacker poses as someone the victim knows and gets them to either download malware or provide the hacker access to an otherwise password-protected device, app, or network.

Looking at this list, it's little surprise that professional IT vendors say that spam and phishing emails account for 57% of the ransomware attacks they've come across, followed by human error at 27%.<sup>2</sup> Without question, good habits, thinking twice, and going online with a critical eye can help you avoid a ransomware attack.

The rest of ransomware prevention comes down to taking a proactive stance.

## Best defenses against ransomware

Putting security measures in place and protecting your data round out your best possible defense.

Start with online protection software, which offers several features that can help you avoid falling victim to a ransomware attack, such as:

- Safe surfing features that warn you of malicious downloads, attachments, and websites.
- Strong antivirus that spots and neutralizes the latest malware threats with the latest antivirus technologies.
- Vulnerability scanners that help keep your device and its apps up to date with the latest security measures.
- A firewall that helps prevent intruders from accessing the devices on your network—and the files on them.

As you can see, several of these measures help prevent some of those human errors mentioned above. From there, you can take several other steps that round out your proactive stance.



Ransomware prevention comes down to taking a proactive stance.



## **Back up your data—and secure it too**

Because ransomware attacks your data, keeping a backup for restoration is a must. A reputable cloud storage solution [secured with a strong and unique password](#) offers one option. Likewise, you can back up your files on an external disk or drive, making sure to keep it disconnected from your network and stored in a safe place—because ransomware is often cagey enough to search for backups on a network or device and encrypt those as well. So while backing up your data can't prevent an attack, it can ease the damage.

## **Be careful where you click**

As mentioned, mistakes can lead to ransomware. Don't respond to emails and text messages from people you don't know and only download applications from trusted sources. This requires a sharp eye because hackers go to great lengths to make their emails and messages look legitimate, like they're from a business, brand, or friend you know. Check out our blog here for several [ways you can spot phony websites and links](#).

## **Only use secure networks**

Sometimes the convenience or need to use a public Wi-Fi network is just too much to pass up. Yet because they are public, they can expose you to threats from bad actors who may be lurking around on them. When using public Wi-Fi, consider using a VPN like [McAfee® Secure VPN](#) that provides you with a secure connection to the internet no matter where you go.



### **Don't use unfamiliar USB storage sticks**

Just as hackers once spread malware by passing along infected floppy disks, they now inject malware into storage sticks and other external storage devices. Recent reports<sup>3</sup> call out instances of hacker groups mass mailing infected USB drives to consumers, sometimes posing as a retailer or government agency. If you find or receive a stray USB drive, don't use it, and dispose of it in a way that no one else can unwittingly use it.

### **Update your passwords**

Ensure that your passwords are strong and unique, for your accounts, your lock screens, and for your internet router too. Many people utilize the same password or variations of it across all their accounts. Therefore, be sure to diversify your passcodes to ensure hackers don't get access to several accounts with a single stolen password. You can also [employ a password manager](#) to create and securely store your passwords for you, which you can find in comprehensive online protection software.

### **Get ransomware coverage**

Just as large organizations invest in cybersecurity insurance, you can cover yourself as well. [Select McAfee plans offer \\$25,000 in ransomware coverage](#), which comes with expert support that can help you determine the severity of a ransomware attack, learn what immediate steps you can take, and determine what your options are. In short, with ransomware coverage, so you don't have to go it alone.

## What to do if you're the victim of a ransomware attack

Getting hit with a ransomware attack can feel like the floor has dropped out from under you. Immediately you think of the potential loss at hand—all your files, photos, and information. The most important thing you can do is to act quickly and take the following steps:

- **Isolate the infected device.** Disconnect your device from your network to prevent any possible spread to other devices. If you can't disable Wi-Fi (and a cellular data connection if your device has one), power it down. Check your other devices for signs of an attack and run a security scan on them to see if they've been affected. If they show signs of ransomware, disconnect them as well.
- **Don't pay the ransom.** Paying a ransom is no guarantee that the hacker responsible will restore your data. The reasons are many. Some hackers may be unsophisticated and rely on a pre-packaged ransomware kit that they don't fully understand. Others may simply walk away once they have your money, as they really have no incentive to restore the data at that point. And let's face it, they don't have a reputation to preserve. There's no such thing as a "nice" hacker.
- **Work with an expert.** Rather than pay, get help from a reputable and knowledgeable source. An expert can help you assess the damage and advise you on next steps and recovery options. Note that some ransomware attacks may inject other malware packages that sit dormant for some time, so removing ransomware and decrypting files may not be enough. Extra steps may be called for. Again, guidance from our [ransomware coverage experts](#) or our [TechMaster service](#) can show you the way forward.
- **Report the ransomware attack to authorities.** Ransomware is a crime. File a report with law enforcement. (Likewise, many insurers will require a police report if you plan on filing a claim associated with a ransomware attack.) If you ended up paying a ransom or believe that the attack removed data from your device, report that as well. Also consider reporting to the appropriate governmental cybercrime agency, such as the [FBI's Internet Crime Complaint Center](#) in the U.S. The information you provide could help officials track down the hackers responsible for these attacks and provide intelligence that can help prevent others from falling victim.
- **Evaluate your backups.** Take a good look at your storage and backup systems and ensure that everything is in order. Do they have the files you need? Are there files missing that you'd like to recover? Is everything ready for downloading onto a fresh device? Share this info with the expert who's assisting your recovery, as it may influence the steps you'll need to take.

Finally, once you've recovered from the attack, work with your expert to find out what went wrong. Was it a bad link, a sketchy download, a fault in your software somewhere? With that information in hand, you can shore up your defenses and help see to it that doesn't happen again.



## You're your own best defense

You can significantly reduce the risk of a ransomware attack.

A combination of preventative measures and playing things smart can help keep hackers at bay. Further, a sound data backup plan gives you a path to recovery should ransomware or try to do harm to your files and photos.

So much of your defense revolves around you. Hackers count on people who fail to keep their protection up to date. And they also count on people to take the bait—clicking on links without thinking twice or not making sure that someone is who they really say they are when communicating online.

And they most certainly count on people failing to securely back up their data on a regular basis. In fact, nearly the entire basis of a ransomware attack hinges on that.

Put up your best defense and securely back up those precious and important files.

For more about staying safe and getting the most out of life online, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

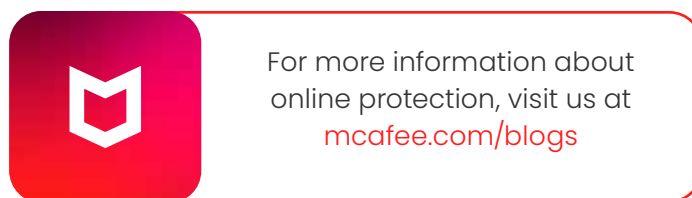
Visit us any time!

<https://www.mcafee.com/blogs>

## About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

[www.mcafee.com](http://www.mcafee.com)



1. <https://www.forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back>
2. <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/>
3. <https://www.zdnet.com/article/fbi-cybercriminals-are-mailing-out-usb-drives-that-will-install-ransomware/>