Ransomware 101

Keeping Your Organization Safe

CCS Technology
BRING. IT. ON.

ccstechnologygroup.com

Ransomware 101

Any kind of virus is scary. The idea of the technology you use turning on you is unsettling at best. As we come to rely more on computers, smartphones, tablets and the cloud, a single cyber attack can be devastating.

And yet, there is one form of cyber attack that stands out. Ransomware is singularly chilling. When this malware finds its way onto your device, it demands payment . . . or you lose your files. Forever.

While ransomware may seem like a new form of cyber attack, it's actually been around for a while. In fact, the first known ransomware attack happened in the 1980s.

Attack Number One

It was 1989, well before email or Instagram. The average PC user wasn't logging into the internet, so the delivery method of that first ransomware attack may seem low-tech by today's standards. It came on floppy disks.

20,000
of them!

The disks were distributed to users in 90 different countries, each labeled as a product of the PC Cyborg Corporation. No such company exists, but no one was counting on name recognition to get recipients to use the disks. They were counting on the content.

The disks included software designed to detail a person's risk of contracting AIDS. In those days, AIDS was both terrifying and mysterious. New information was welcome, especially if it promised some measure of protection. The attack played on a common fear.

The software included a legitimate risk assessment tool, as well as a virus. After the user rebooted their computer a set number of times, they would be prompted to turn on their printer. At that point, a literal ransom note would print, along with instructions for paying the ransom (or "licensing fee") in exchange for decryption software.

It was a deviously creative plan, and it set the stage for modern ransomware.

The Modern Threat

Today's ransomware is fundamentally the same as that first attack, though there are some notable differences. The delivery method, for example, has changed. We'll cover that in more detail in a bit.

Keeping your organization safe may seem like a tall order. There are so many clever ways a cyber criminal can infiltrate your network. Not only that, but ransomware attacks are alarmingly common. There's a ransomware attack on a business once every 40 seconds. And we're not just talking about large corporations. 40% of ransomware attacks target companies with fewer than 100 employees.

"There's a ransomware attack on a business once every 40 seconds."

– Kaspersky Security

And yet, the best cybersecurity is really just strict adherence to some basic strategies. In other words, it seems complex, but it's not.

If you're serious about protecting your company – and you should be – there's a two-pronged approach that will stop most ransomware dead in its tracks. You need solid employee education, and you need the right technical tools.

Employee Education

The vast majority of ransomware relies on a single potential weakness in your network – the user. As a recent article from the Harvard Business Review observed, "no matter the size or the scope of a breach, usually it's caused by an action, or failure, of someone inside the company." This is particularly true for ransomware.

Ransomware can only find its way into your system if it's invited. Without an open door, it can't touch you. The trick is to make sure your people know how to avoid inadvertently inviting ransomware onto your network.

Let's look at three key areas.

Phishing

Phishing emails are the modern day equivalent of the same strategy the AIDS Trojan used. Even if you're not familiar with the term "phishing," you're likely aware of this type of attack. The user receives an email with a link. Click that link and malware makes its way onto your system.

The thing about phishing emails is that they *only work* if the user clicks on the link, opting to download something. If the recipient doesn't do that, nothing happens. Unfortunately, about 30% of all phishing emails work. Innocent users take the bait, clicking on malicious links.

The success of phishing comes down to a lack of employee education. If your people know and understand the danger of suspicious downloads, they'll be far less likely to fall for them.

Social Media

Email isn't the only delivery vehicle for phishing. Phishing via social media is up by an overwhelming 500%.

Here's a common scenario. Attackers create fake social media accounts on sites like Facebook and Twitter. The newest variation is a fake account that appears to represent the customer service department of a trusted company. Attackers then watch for complaints from real customers, promptly messaging them with "fixes" . . . which are, of course, loaded with dangerous links.

Make sure your employees know of this tactic. If you or any member of your staff is having issues with a product or service, make sure you initiate conversation with the vendor. Don't trust anyone who initiates conversation with you without first verifying the authenticity of the account.

Passwords

Remarkably, there are still a lot of folks out there using painfully ineffective passwords. In a recent survey, 17% of users were actually using the password "123456." That's not just an invitation for cyber attack. That's a neon sign with a laser light show and door prizes.

"40% of ransomware attacks target companies with fewer than 100 employees."

– Infosecurity Group

Instruct your employees to use strong passwords, and encourage them to change them often.

Technical Tools

In addition to employee education, there are some things you can do on the technical side of your network to protect your company from ransomware attacks. Like employee education, these aren't particularly difficult to execute. But don't be fooled by their relative simplicity.

These are crucial steps to keeping your network safe.

Software Updates & Upgrades

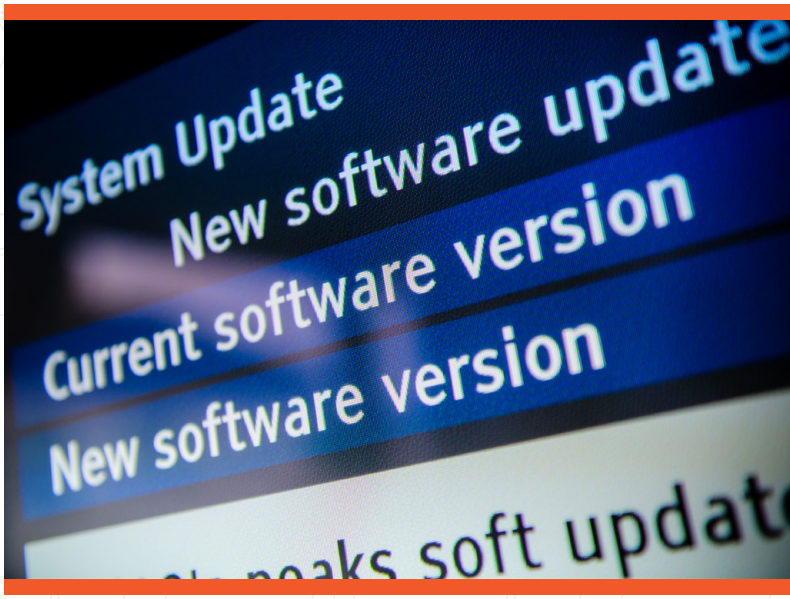
In June of 2017, the Petya ransomware virus made worldwide headlines, infecting an estimated 16,500 machines. Ready for the painful twist? Microsoft released patches to address the vulnerabilities Petya exploited in May.

Too many companies have a casual, relaxed attitude about updates and upgrades. Yes, it's inconvenient to reboot your machine so the OS can update. Yes, it's expensive to upgrade from the old version of a program to the new (current) version. And yes, it's extremely important to do both anyway.

Software developers do their best to outpace cyber criminals. When they find holes in their products, they address them. But if you don't update and upgrade appropriately, you'll remain vulnerable.

Backups & Business Continuity

Even thorough security measures aren't a guarantee that you won't fall victim to a ransomware attack. After all, it just takes one employee clicking on a malicious link. Just one out-of-date program. It can happen, even if you're cautious.



Because the threat is very real, your protection should include a worst-case-scenario plan.

Ransomware is engineered to hold your data hostage. That can ruin a business – unless you have recent backups and a solid business continuity plan. If you're prepared, even a successful attack won't unravel your company's stability.

A word of caution here, though. Business continuity isn't something we advise doing on your own. But, that's a perfect lead-in to our final technical tool . . .

Cybersecurity Partner

A cybersecurity partner should be a part of your ransomware defense plan. Particularly if you don't have an internal IT department. There's no substitution for expertise. Working with the pros makes protection much easier to manage.

A well-qualified cybersecurity partner can even handle employee education on your behalf.

CCS Technology Can Help

Ransomware is a serious threat. That's why we recommend a serious, proactive response. The individual parts aren't all that complex, but each piece is important.

If you're looking for ways to shore up potential security holes in your network, the experts at CCS Technology are here to help. We have years of experience helping small businesses just like yours. We know what it takes to stop ransomware.

Plus, we're just a phone call away. Let us know how we can help you.