THE ABCs OF MALWARE

A Small-Business Owner's Guide to Understanding, Preventing, and Budgeting for Online Attacks

SUNDOG

YOUR STRATEGIC IT PARTNER

THE ABCs OF MALWARE

TABLE OF CONTENTS

Viruses aren't the only thing you need to worry about

Every day, hackers invent new ways to wreak havoc for personal gain

You regularly update your antivirus software and everyone working in your office is trained to treat emails with suspicion and to avoid unsecured Wi-Fi networks; that should be all it takes to protect your office from a cyberattack, right? That may be more than most companies are doing, but it's not nearly enough to keep you safe.

From front-page attacks like ransomware to less obvious "grayware," there are several types of malicious software (malware) programs and each one requires a unique defensive strategy. This is especially true for small businesses, which according to Verizon's 2020 Data Breach Investigations Report, account for almost one-third of cyberattack victims.

> *At Sundog, we believe avoiding malware is just as feasible for an office of 5 as it is for an office of 500.*

You don't need a computer science degree to follow some basic cybersecurity best practices, and you don't need to hire a full-time technician with a six-figure salary to enjoy enterprise-level security. By the end of this eBook, you'll have a fundamental understanding of how hackers target small- and mid-sized businesses with malware and how to stop them from succeeding. Let's get started

5 Telltale signs of malware infections (besides sluggishness)

Noticing one of these red flags could save you thousands of dollars

For decades, you've been trained to look for a virus when your computer performed more poorly than usual. But as more sophisticated malicious software programs are released, hackers have made it harder to notice when something is amiss. Here are some lesser-known signs your computer has been infected:

1. Your security software is mysteriously disabled.
2. Filenames have changed for no reason.
3. Unknown apps or browser toolbars have appeared.
4. A web page you've never visited before loads when you open a new browser window.
5. Your email contacts are receiving strange messages from you.
6. You've been getting suspicious pop-up ads or security warnings on your computer.

If you notice any of these signs, shut down your computer immediately and contact an IT professional to stop the malware from spreading further.

Now, if you subscribe to managed IT services, unlimited tech support is included in your service. But for businesses that still rely on the break-fix model, malware prevention is going to be especially important.

Tips for avoiding the most common malware attacks against small businesses

Insight from Sundog technicians, who spend 7 days a week in the IT security trenches

The best way to protect your small business from malware attacks is to be aware of the threats they pose. Many people tend to downplay the dangers of malware, making it easy for cybercriminals to gain access to their systems and data. Let's take a look at some common types of malware and how you can avoid them.

Trojans

What are they?

Trojan horses are programs that hide their true purpose, thus appearing benign to unsuspecting users. For instance, an application may advertise itself as an antivirus program but secretly send sensitive data to cybercriminals without the user's knowledge.

How you can avoid them:

Since Trojan horses are disguised as seemingly harmless apps, a cautious mindset is your best defense. In other words, be careful when installing free software, even if it comes from trusted websites or app stores. It's also a good idea to forbid employees from installing software that isn't approved by your IT department on the devices they use for work.

Viruses

What are they?

Similar to the behavior of their biological counterparts, computer viruses replicate and spread to other devices. They can infect programs, files, and inboxes, and spread via infected flash drives, websites, and email attachments.

How to avoid Viruses

Because viruses can't hide behind the guise of a useful program, they are usually distributed within documents attached to emails. In addition to regularly reminding your employees to be wary of attachments, deploying a high-end spam filter and email-based anti-malware software, ideally with monthly audits from an IT staffer, will help you keep computer viruses at bay.

Worms

What are they?

Worms are malware that spread themselves without the need for any human action. They are standalone programs that exploit network security holes and, unlike viruses, worms don't need to be opened or installed to work. They hog a surprising amount of computing resources as they spread from victim to victim, but worms are most dangerous when they're programmed to deploy viruses, ransomware, and trojans along their journey.

How you can avoid them:

Because worms spread via deeply rooted hardware and software vulnerabilities, the most effective thing to do is to install vendor-issued updates and patches for apps, operating systems, and firmware.

Continued use of outdated software could land you in the same scenario as the thousands of victims of the WannaCry ransomware cryptoworm. Although Microsoft had patched the vulnerability that made WannaCry possible before the ransomware attack was launched, many organizations failed to update their Windows computers, which led to their files being encrypted and their operations grinding to a halt.

Ransomware

What is it?

Ransomware is set apart from other types of malware by its use of extortion and encryption. When a computer or server is infected, all of its files are rendered unreadable until victims pay hackers a fee to return everything to normal. Ransomware dates back to the early '90s, but has become exponentially more effective and costly for businesses. In March 2021, in fact, insurance company CNA Financial was forced to pay cybercriminals $40 million to regain control of its network.

How you can avoid them:

Because ransomware is based on unbreakable encryption, there's usually no recovering from an attack unless you have robust and secure backups stored somewhere safe from the spread of infection. Cloud-based backup services are an inexpensive way to ensure your data is always accessible regardless of the latest advancements in ransomware.

Grayware

What is it?

Sometimes referred to as potentially unwanted programs, grayware programs don't actively alter, steal, or destroy information but still cause problems. This type of malware slows down your computer, reveals your private information, and floods your computer with ads.

The two most common types of grayware are adware and spyware. The primary goal of adware is to make money via advertising targeted to users. It may or may not collect and send data to a third party. Adware is often noticeable and may slow down a computer. Meanwhile, spyware's main purpose is to track and record information such as usernames, passwords, and credit card details, which will be sent to a third party. It normally stays hidden on victims' computers, silently running in the background to avoid detection.

How you can avoid them:

Grayware programs often hide behind deceptive software. So if you install such, you may unknowingly install grayware on your computer. Therefore, avoid downloading applications from illicit or third-party websites. And when downloading an app from official app stores or websites, always check the app permissions, number of downloads, user rating, and developer information to better ascertain the app's safety. Installing security updates regularly also significantly reduces the risk of grayware infections, as doing so patches bugs that may otherwise be exploited by cybercriminals to introduce new malware.

These stories prove malware isn't "fake news"

Businesses of all sizes make for easy targets

Still not convinced of the dangers that malicious programs pose to your business? Take a look at these four organizations that felt the effects of a malware attack:

Small Kentucky company

In 2020, a chief financial officer of a small company in Kentucky discovered that eight of their company's PCs were inaccessible due to a ransomware attack. The company ended up paying $150,000 to ensure business continuity.

Park Hill School District

The Park Hill School District in Missouri suffered a malware attack in March 2021. The cyberattack cut off access to several computers, forcing the school to cancel classes for a few days. Fortunately, the district was covered by technology insurance and did not find any personal data exposed.

Alaska court system

In April 2021, the Alaska court system became a victim of a malware attack. The court did not find any personal or confidential data, or credit card information stolen from its systems. Nevertheless, it vowed to upgrade its software and invest in better technology to protect themselves from future cyberattacks.

Irish state health services

A ransomware attack in May 2021 forced Ireland's state health services provider to shut down all of its IT systems and cancel outpatient services. Upon investigation, Health Service Executive (HSE) CEO Paul Reid discovered an attempt to access data stored on the HSE's central servers.

A formula for putting a dollar value on your security needs

Undeniable proof that cybersecurity solutions are worth the investment

Even without the information in this eBook, it's clear to most business owners that IT security services are nonnegotiable. However, figuring out how much to spend on those services isn't always as clear. Cybersecurity isn't something you want to skimp on, but we'll be the first to tell you that you shouldn't give an IT provider carte blanche either. Thankfully, there's a simple formula to make sure the funds you set aside for prevention never exceed the costs of a breach:

Annual Breach Costs = **Number of Incidents per Year** x **Potential Loss per Incident**

It's a simple equation, but the variables vary greatly depending on your business's location and industry. For example, software company AppRiver estimates that the average small-business data breach costs $149,000. So even if you experience incidents only every other month — which we assure you is woefully optimistic — you can justify an annual cybersecurity budget of almost $900,000 (6 events × $149,000)!

The cost of an annual breach is even higher in the healthcare industry. In fact, a single incident can cost a healthcare organization $7.13 million, which could be enough to shut them down for good.

This is why Sundog provides managed IT services rather than break-fix contracts. For a flat monthly fee, we'll take care of everything related to cybersecurity. Software vulnerabilities are patched before they cause a breach, your inboxes are kept free of malware, and your firewalls are top of the line — all for less than the cost of potential data breaches.

THE ABCs OF MALWARE

24/7 Malware protection doesn't have to cost an arm and a leg

Prevention is much cheaper than reparation

Knowing how to spot and avoid common types of malware can go a long way in protecting your business, but without round-the-clock security, you'll never be totally safe.

We offer cutting-edge cybersecurity solutions designed to protect you against existing and emerging malware threats. With our expertly configured antivirus software, firewalls, advanced intrusion prevention systems, and data backup solutions, you'll never need to worry about data breaches again.

All our solutions are installed, configured, monitored, and centrally managed by a team of certified professionals for less than the cost of hiring a single technician.

Want to see the Sundog approach to your cybersecurity firsthand? Schedule your free consultation today!

Phone: **(815) 991-2400** Email: **yourteam@sundogit.com**

SUNDOG

YOUR STRATEGIC IT PARTNER

www.sundogit.com