THE ABCs OF MALWARE

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

OKLAHOMA
TECHNOLOGY SOLUTIONS
SOLVING YOUR TECHNOLOGY PROBLEMS

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 WiFi 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 programs and each one requires a unique defensive strategy. This is especially true for small businesses, which according to Verizon's 2018 Data Breach Investigations Report, account for 58% of cyberattack victims.

At Red Earth Systems, we believe avoiding malware is just as feasible for an office of five 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 an 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 (beyond sluggishness)

Noticing one of these red flags could save you thousands

For decades, you've been trained to look for a virus when your computer performed more poorly than usual. But as new types of advanced malicious software 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. An unrecognized webpage pops up when you open a new browser window
5. Your email contacts are receiving strange messages from you

If you notice any of these signs, shut down your computer immediately and contact an IT professional about stopping the malware's spread.

Now, if you subscribe to managed IT services, unlimited tech support is included in your service. But for businesses that still rely on the "call IT repairmen after something breaks" model, malware prevention is going to be especially important.

Tips for avoiding the most common malware attacks against small businesses

Insight from Red Earth Systems technicians, who spend 7 days a week in the IT security trenches

Full disclosure, the majority of cyberattacks are made possible by users who circumvent security software and hardware. “Phishing” (sometimes called social engineering) is when hackers disguise themselves as a trustworthy source, such as a bank employee, and ask for private information, such as a credit card expiration date.

So, the best way to avoid almost any type of malware is employee training. But beyond that, there are some more black-and-white solutions.

Trojans

What are they?

Trojans are programs that seem benign to unsuspecting users, but hide their true purpose. They accounted for 41% of all infections in 2017 according to Comodo’s Global Malware Report. In one example, the Google Play store recently expunged a fully functional barcode scanning app that was secretly forwarding sent and received text messages without the user’s knowledge.

How to avoid trojans

Since Trojans are disguised as seemingly harmless apps, a cautious mindset is your best form of defense. In other words, be careful when installing free software, even if it comes from a trusted source like the Google Play store. Forbidding employees from installing software that isn’t approved by your IT department is a good place to start.

Viruses

What are they?

Viruses were some of the first malicious programs ever created. When a file is opened that is infected with a virus, that virus can spread itself to other files and computers. Applications and documents that are infected can be altered, stolen, or destroyed. Viruses aren't as popular as they once were, but in 2017 they were detected in 190 countries, with US individuals and businesses being the most common targets.

How to avoid Viruses

Because viruses can't hide behind the guise of a useful program, they are usually distributed as documents attached to emails. In addition to regularly reminding your employees to be wary of attachments, you should have a high-end spam filter and email-based antimalware software, ideally with monthly audits from an IT staffer.

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 to avoid worms

Because they spread via deeply rooted hardware and software vulnerabilities, the most important thing to do is install vendor-issued updates and patches for apps, operating systems, and firmware. In a horrific real-world example, Microsoft patched the vulnerability that made the WannaCry possible before the ransomware attack was released. The malware was so immensely successful only because so many people failed to update Windows.

Ransomware

What is it?

Ransomware is set apart by its use of extortion and encryption. When a computer or server is infected, all its files are rendered unreadable until victims pay hackers a fee to return everything to normal. Ransomware actually dates back to the early '90s, but has become exponentially more effective, with 22% of infected small businesses immediately going out of business.

How to avoid ransomware

Because it is based on unbreakable encryption, there's usually no recovering from a ransomware attack unless you have robust and secure backups stored somewhere safe from the spread of infection. Many off-the-shelf antimalware programs contain so-called ransomware protections, but struggle to recognize never-before-seen threats. Cloud-based backup services are inexpensive and ensure your data is always accessible regardless of the latest advancements in ransomware infections.

Grayware

What is it?

Grayware programs don't actively alter, steal, or destroy information, but still manage to cause problems. This type of malware slows down your computer, reveals your private information, and floods your computer with ads. In the summer of 2017, a grayware application was found on 250 million computers. All it did was change a web browser's default search engine, but it could've granted remote access to the computers it was installed on.

How to avoid unwanted applications

These unwanted applications often come installed on new computers or bundled in free software packages. Take the time to periodically factory-reset company-issued devices. Windows 10 includes a user-friendly "Refresh" feature that wipes everything from a computer except its documents and critical applications. Anyone should be able to wipe a mobile device, but an IT provider can do it in a fraction of the time.

$2.3 Million worth of mistakes prove malware isn't 'fake news'

Small businesses make for lucrative targets

Construction company - $588,000

In 2009, a general contractor in Maine that employed fewer than 50 employees lost more than half a million dollars over the course of seven days. A trojan had been installed on a company computer that recorded the username and password for the company's bank account login. If the company in question had a "no free software policy," none of this would've happened.

Communications and safety solutions provider - $180,000

In 2012, an employee at a Missouri business clicked on an email attachment containing a virus. That infection exposed enough information to enable hackers to add 26 "employees" to the payroll, and wire each of them between $5k and $9k, which they then transferred to an unknown number of people in Ukraine. All because the company had an inadequate spam filter in place.

City Municipal Court - $25,000+

To date, the Conficker worm has infected well over 15 million computers, caused $9 billion in damages, and continues to elude security researchers. In one case, Conficker shut down a city's judicial court system for several days. Although costs associated with hundreds of slowed computers wasn't calculated, the city was forced to pay $25,000 in emergency cyber security consulting fees. Several patches had been released at the time of infection, but they just weren't installed.

Law firm - $743,000

In early 2017, a firm with only 10 attorneys was hit by a strain of ransomware that demanded $25k in payments. The firm paid the ransom, but the tools to remove the malware didn't work. Hackers demanded another $18k, and this time the firm was able to regain access to its files. The entire process took almost three months and cost the firm an estimated $700k in lost business. With basic backups, the firm could've skipped the ransoms and restored everything in a matter of days.

State welfare office - Potentially $798,000

Also in 2017, one of Maine's health and human services offices contracted IT work from a third party. An employee of the contractor posted over 2,000 records containing names, addresses, and social security numbers to a free website that optimizes datasets and does not protect uploaded information. No lawsuits have been made public yet, but that "grayware" could cost the state of Maine almost $800k based on the current $380 average cost per breached HIPAA record. All because someone thought a free app was a good place to upload SSNs.

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. Budgeting 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. 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 the location and industry of your business. For example, Kapersky Lab estimates that the average sma ll-business data breach costs $117,000, but that number could be 10x higher if you are in the healthcare industry.

So even if you experience incidents only every other month -- which we assure you is woefully optimistic -- you could justify an annual cybersecurity budget of almost $700,000 (6 events x $117,000)!

This is why Red Earth Systems provides managed IT services rather than break/fix contracts. We charge a flat monthly fee and 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 money than the costs of potential data breaches.

THE ABCs OF MALWARE

24-hour 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 around-the-clock security you'll never be totally safe.

We offer cutting-edge cybersecurity solutions designed to protect you against new and old malware threats. With our expertly configured antivirus software, firewalls, advanced intrusion prevention systems, and data backup solutions, you'll never need to worry about the financial impact of a data breach again.

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

Want to see the Red Earth Systems approach to your cybersecurity firsthand? Schedule your free consultation today!

Phone: **405-622-5080** Email: **contact@oktechsol.com**

OKLAHOMA TECHNOLOGY SOLUTIONS
SOLVING YOUR TECHNOLOGY PROBLEMS

www.oktechsol.com