

## Don't Wait! Apply These 3 Steps to Protect Your Small Business Against Cyber Criminals

Dec 13, 2017 by Brian Hughes In Technology Trends 1

299 Shares

[Twitter](#) 154
 [Facebook](#) 101
 [Google+](#)
[Print](#)

[LinkedIn](#) 50
 [Pinterest](#) 1
 [Email](#)



Think the biggest threat to your small business is a competitor offering lower prices or newer products? Think again. The biggest threat to your business might come from where you least expect it. **Malware**, including an especially pernicious form known as **ransomware**, can cripple small businesses. Ransomware is a type of malware that locks down computers until money is paid to “ransom” the computer’s contents. Twenty-two percent of businesses with less than 1,000 employees that experienced a ransomware attack in the last year had to stop business operations immediately and 15 percent lost revenue, reports [CNN](#). Yet many small businesses continue to be woefully under prepared.

### Advertisement

### Cyber Attacks and Malware Don't Discriminate: Why Small Businesses are at Risk

When most of us think about cyber attacks, we think about serious security breaches at major corporations like Equifax, FedEx, and Target. [Equifax](#), for example, recently disclosed it had been hit by two major hacking incidents in March and May, exposing personal and financial data on 143 million U.S. consumers. Earlier this year, the global WannaCry and NotPetya cyber attacks hit major corporations like FedEx's TNT shipping unit. [Target](#) fell victim in 2013 after hackers installed malware on Point of Sale (PoS) systems at retail locations across the country, intercepting more than 110 million transaction records.

Attacks on major corporations can leave millions of consumers vulnerable to identity theft and financial compromise. It's no wonder that the recent Equifax breach, for example, continues to make headlines on the nightly news. Unfortunately, these attacks can also lull small business owners into a false sense of complacency. We fall victim to our own confirmation bias: if we only hear about major attacks, small businesses must not be targeted, right?

Not so fast! Malware can strike any business, anywhere. [According to data](#) compiled by Enigma Software Group (ESG), the creators of SpyHunter, there were more than 1.5 million infections in all 50 states in the first six months of 2017. The highest infection rates were in New Hampshire, Colorado, Virginia, New Jersey and Oregon. There's no clear pattern or reason for why some states have higher infection rates. "Regardless of where you live, it's always important to stay vigilant for infections all the time," says ESG spokesperson Ryan Gerding.

### SUBSCRIBE

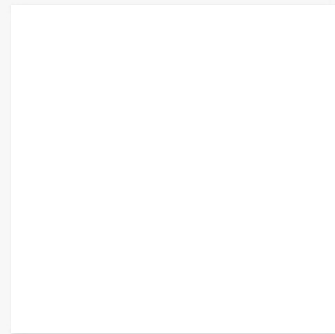
Follow @SmallBizTrends



Subscribe to our Newsletter

### ADVERTISEMENT



### POPULAR

Popular	Comments	Tools
---------	----------	-------

- 
- 
- 
- 

[View All](#)

- "Thanks for posting this useful tool."

[Dave](#)
- "It is now possible to have a business even if you don't have a lot of startup..."

[BizEpic](#)
- "Another way to get inspired is to attend events and listen to successful people..."

[BizEpic](#)
- "Networking is really important. No business is an island. You cannot survive alone."

[Aira Bongco](#)
- "Thanks for the ideas. The key is to get people talking about your brand or at least..."

[Aira Bongco](#)

[Do You Qualify for a Small Business Loan?](#)

299 Shares

[Twitter](#) 154
 [Facebook](#) 101
 [Google+](#)

[LinkedIn](#) 50
 [Pinterest](#) 1
 [Email](#)

## 3 Ways to Protect Your Small Business Against Cyber Criminals

Could your business recover from a ransomware attack? On average, small companies lose over \$100,000 per ransomware incident due to downtime. That's not even taking into account the potentially catastrophic loss of client trust in your company. While larger corporations have the financial and legal [resources](#) to bounce back from an attack, most small businesses don't.

"Trust is the foundation for our business," says [Brandon Lewis](#), the President of Win More Patients. "Any attack could compromise our integrity with clients. When it comes to protecting our business, we leave nothing to chance."

You shouldn't, either. Here's the good news: you don't have to spend a small fortune on cyber security to protect against common threats, like ransomware. Most ransomware gets on a computer when the user clicks on a bad link in an email or downloads something with a malicious code. Proper threat education coupled with up-to-date security programs can help reduce the risk of an attack. Here's how to get started:

### Assess Your Threat Risk

Bring Your Own Device (BYOD) culture is great for productivity, but not great for hacking risks. If you have not done so already, establish a company-wide policy that regulates which data employees can access and what happens if an employee's device is lost, stolen or compromised. Finally, consider how sensitive data is stored and accessed. Take additional steps to secure data stored in the cloud.

### Protect Your Network

Hackers use tools to search for unprotected networks and computers. Once a computer is identified, the hacker takes over the computer and uses it to launch a full-scale attack. Assess your existing network protections. Do you have a software firewall as well as anti-virus and anti-spyware programs in place? If you aren't sure about the best ways to protect your network, consider hiring a specialized contractor on a project basis to harden network security protocols.

### Educate Your Team

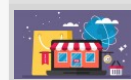
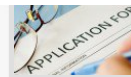
Human error is a major contributing factor to ransomware attacks. Do your employees know how to identify a threat, such as a suspicious email? Do they know what to do if they click on a bad link? With the threat landscape changing rapidly, your company's security policies must keep pace. Put all security policies in writing, including detailed steps employees should take in the event of a potential breach. Require employee signatures to confirm understanding and enforce compliance.

### Bottom Line

Ransomware attacks are costing small businesses big money. Don't wait until your company is a victim and it's too late to take action. Take steps now to shore up your business's cyber security and protect your most valuable asset: client trust.

Photo via [Shutterstock](#)

1 Comment ▼

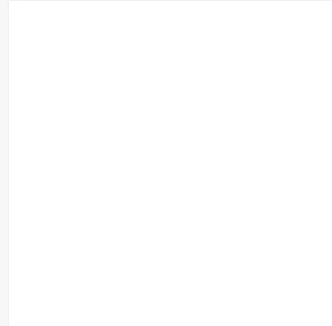


Marketplace



Research Your Business

### ADVERTISEMENT



### EDITOR'S PICKS



**Are Samsung S9 and S9+ Priced for Your Small Business Budget?**



**Dropbox Now Integrated with Google Cloud**



**1 in 5 Businesses Will Abandon Their Mobile App by 2019**

**BRIAN HUGHES**



Brian is a seasoned digital marketing expert who loves to write about subjects that help small businesses grow their brands and increase their rankings online. He accomplishes this through his agency [Integrity Marketing & Consulting](#), which he founded in 2011.

**One Reaction**



*Aira Bongco*

December 15, 2017 at 12:25 am

Small businesses should be more active in their cyber security. They have to understand that it is not optional and protection is necessary to operate a business.

Reply

**LEAVE A REPLY**

Your email address will not be published. Required fields are marked \*

Name \*

Email \*

Website

**Post Comment**

Follow @smallbiztrends



**About Small Business Trends**

Founded in 2003, Small Business Trends is an award-winning online publication for small business owners, entrepreneurs and the people who interact with them. It is one of the most popular independent small business publications on the web.

Together with hundreds of expert contributors, Small Business Trends brings you the news, advice and resources you need. "Small business success... delivered daily."

**Contact**

- Advertise
- Magazine Advertising
- Contact Us
- Looking for Writers
- Support
- Privacy
- Terms

**More**

- Daily Tips
- Small Business News
- Small Business Press Releases
- Selling to Small Businesses
- Infographic Gallery
- Cartoon Gallery
- Small Business Spotlight

**About**

- Company
- Media Kit
- Announcements
- Editorial Calendar
- Resource Center
- Newsletter Archive
- Archives
- Trade Publications
- Newsletter

**Our Other Sites**

