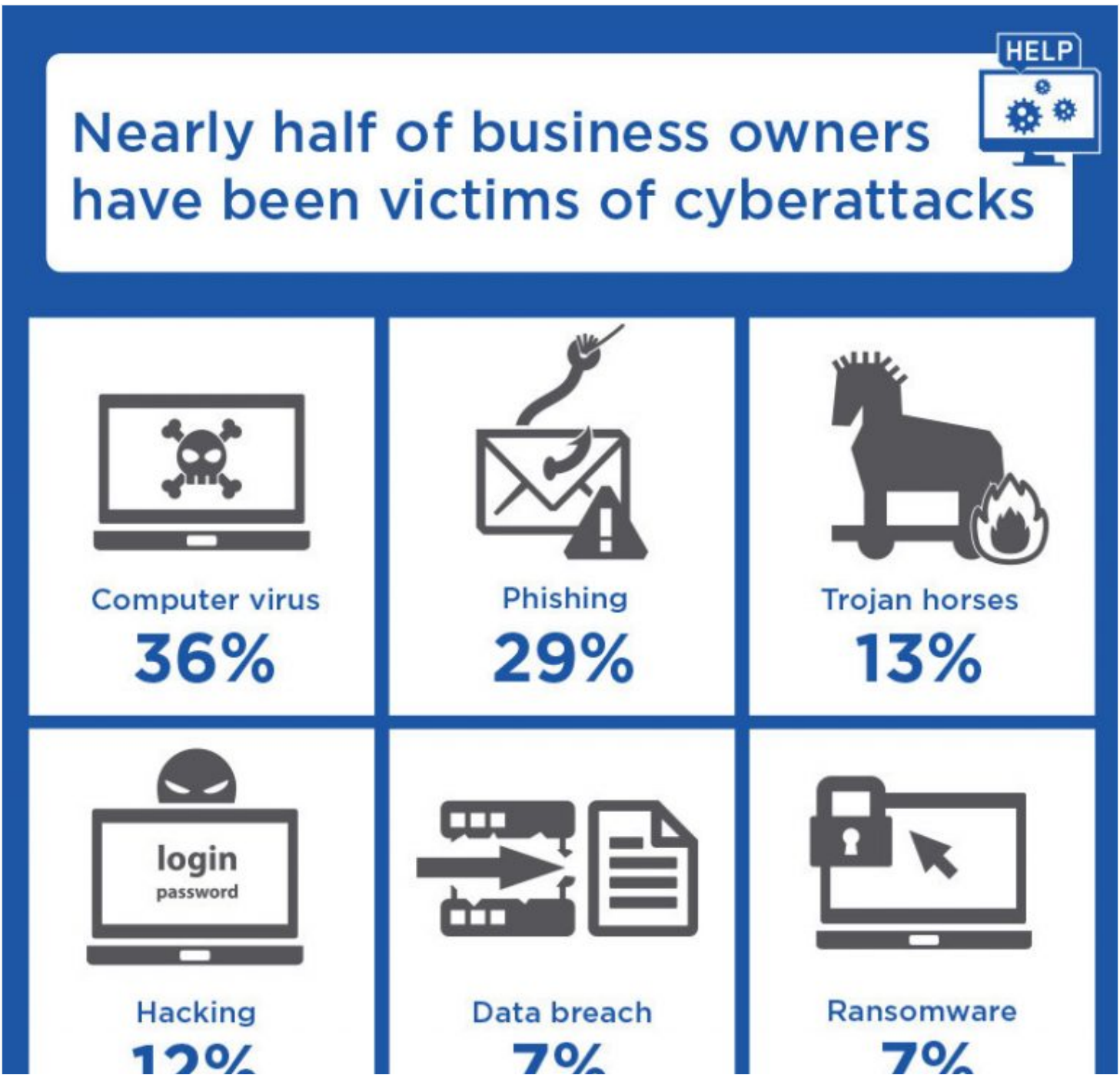
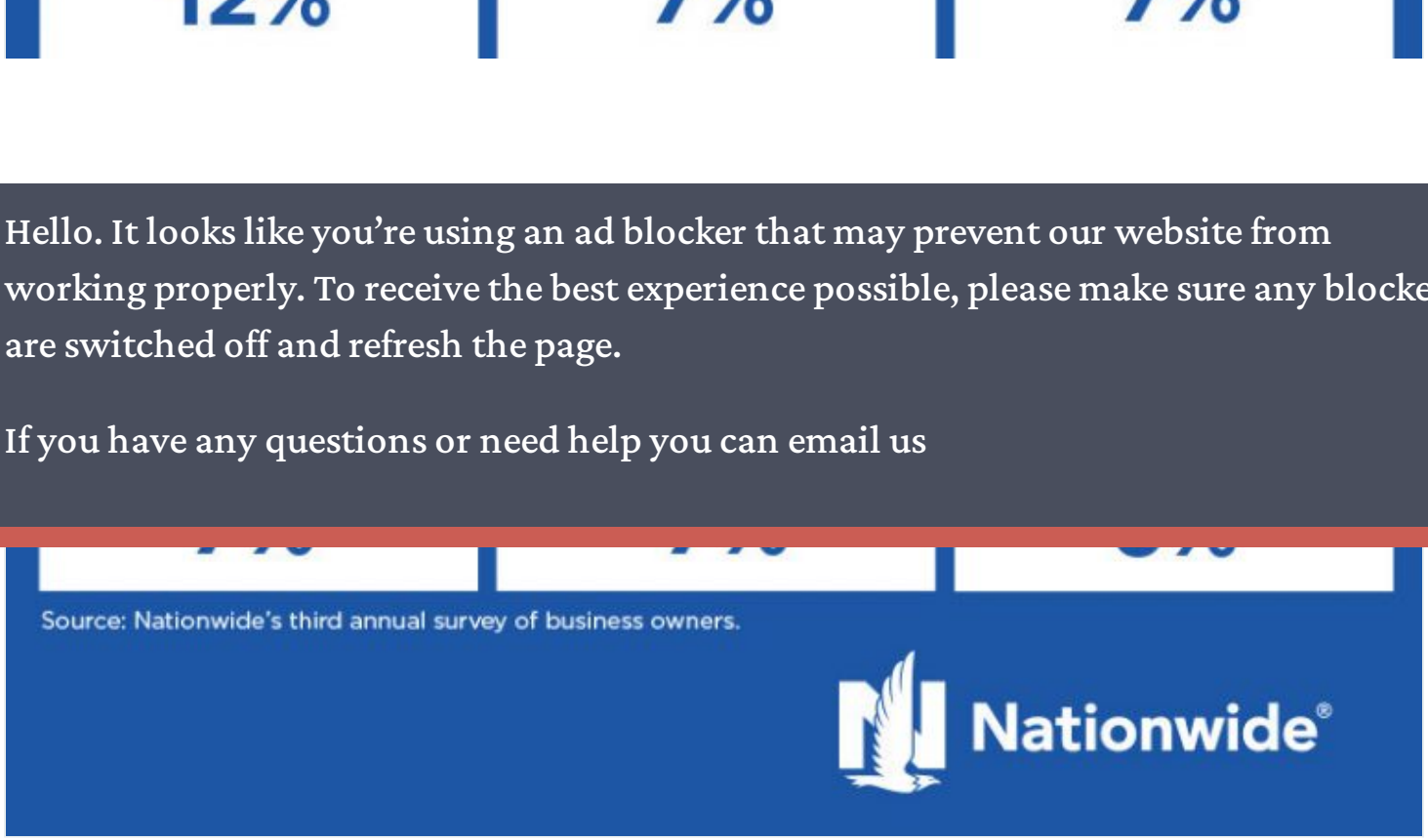
Breach

One in three victims spent at least $50,000 to recover from a cyber attack, yet rebuilding reputation and customer trust can take more than a year.

Oct. 31, 2017





One company became a victim when a cybercriminal infected it with a ransomware virus, taking its servers hostage and holding them for ransom. Another business was attacked by an organized gang of cybercriminals that planned a complex social engineering scheme to steal customer credit card information by impersonating a third-party vendor and installing malware.

Such attacks are becoming more common and can potentially cripple a company's work and reputation — forcing them to pay hundreds to thousands of dollars. While both businesses experienced different forms of cyberattacks, they survived in part because having cyber coverage from Nationwide provided them with the necessary resources that enabled them to have quicker recovery time and fewer expenses than if they had to go it alone.

According to Nationwide's third annual survey of 1,069 business owners with 1-299 employees, more than 20 percent of cyberattack victims spent at least $50,000 and took longer than six months to recover. But 7 percent spent more than $100,000, and 5 percent took a year or longer to rebuild their reputation and customer trust.

"Cyberattacks are one of the greatest threats to the modern company," said Mark Berven, president of Property & Casualty for Nationwide, the No. 1 total small-business insurer[1] in the country. "Business owners are telling us that cybercriminals aren't just attacking large corporations on Wall Street. They're also targeting smaller companies on Main Street that often have fewer defense

mechanisms in place, less available capital to re-invest in new systems and less name

3. **Trojan horse:** 13 percent
4. **Hacking:** 12 percent
5. **Data breach:** 7 percent
6. **Ransomware:** 7 percent
7. **Issues due to unpatched software:** 7 percent
8. **Unauthorized access to company info:** 7 percent
9. **Unauthorized access to customer info:** 6 percent

Part of the problem facing a business' ability to recover from an attack is that a majority of owners are not prepared. In fact, 57 percent of owners do not have a dedicated employee or vendor monitoring for cyberattacks — and therefore, could be victims without even knowing it.

Further, most don't have a cyberattack response plan in place (76 percent), a plan in place to protect employee data (57 percent) or a plan to protect customer data (54 percent). Threats continue to grow as more companies are now frequently using new technologies such as the Internet of Things (37 percent) and Artificial Intelligence (24 percent) in a potentially unprotected environment.

While the vast majority of business owners *say* it's important to establish cybersecurity best practices recommended by the U.S. Small Business Administration, fewer report actually *following* those best practices:

1. **Protect** against viruses, spyware and other malicious code: 85 percent versus 65 percent
2. **Secure** your networks: 85 percent versus 58 percent
3. **Make** backup copies of important business data and information: 85 percent versus 59 percent
4. **Establish** security practices and policies to protect sensitive information: 83 percent versus 50 percent

5. **Control** physical access to computers and network components: 81 percent versus

For more information, visit Nationwide's blog page, take the cyber insurance quiz and review the cyber product pages for both Standard Commercial and Excess & Surplus/Specialty. You can also access more tips and resources during National Cyber Security Awareness Month.

Artificial Intelligence • Security • Small Business