HOW TO PROTECT YOUR SMALL BUSINESS FROM CYBERCRIME

WWW.3POINTS.COM
Cybercrime is becoming its own incredibly lucrative industry, and if you don’t take the proper precautions, your business could be the target of a cybercrime. By 2021, cybercrime will cost the world $6 trillion annually; that's more than the GDP of Japan, the world's third-largest economy.

If the global economy is to remain healthy, then this is a dangerous and unsustainable trend. Curious about how you can better prepare your business to deal with the realities of cyber crime? We have a few helpful insights.

**HUMAN ERROR IS FATAL**

The best malware protection software won't survive contact with an employee that doesn't know the basics of cybersecurity. Statistics show that human error is responsible for a staggering amount of lost data, with either a mistake or loss/improper disposal behind 30% of data loss incidents. An even greater proportion of cybercrimes could be averted with proper training and knowledge on the part of employees.

“90 percent of the internet’s data was created in the last two years. To a cybercriminal, it’s like being a miner in an ever-expanding gold mine.”
- Redcode.net
Human error can come in many shapes and sizes. One of the most common instances of human error is falling prey to a malicious email. A Symantec report says that in July 2017, 55% of all email was considered spam, and that 1 in 359 were malicious. As individuals comb through their inboxes, the normal, mundane spam and mountain of business emails can provide cover for a small number of malicious emails that can open up your network to nasty threats like ransomware.

To make matters worse, phishing is becoming more clever by the day. You may remember one widespread phishing incident earlier this year, when millions received a fake link to a Google Doc, seemingly from someone on their contacts list. If you received that link from someone you haven’t spoken with in seven years, you probably weren’t fooled, but think about the hundreds of thousands who assumed they’d been sent another work-related file from a colleague.

Another source of human error is general negligence towards cybersecurity in the office. This can be on the part of regular employees or management. Failure to properly password protect workstations and important files is a terrible habit to develop, but can be observed in a large number of organizations. Training employees to properly lock down their workstations when they’re away is a great step towards preventing malicious threats from inside your business. Implementing dual authentication policies is a great way to deter hackers. Requiring employees to regularly change and randomize their passwords is another great deterrent.
It seems so intuitive, but your business should take steps to protect itself from old school cyberattacks - and many businesses don’t have a proper firewall in place. Protecting your internet and server activity from outside threats is crucial, and easy to do with the proper procedures and knowledge.

Whether you work with an outside technology provider or an in-house IT staff, it’s important to properly communicate all firewall updates and put several levels of redundancy in place. You should also prioritize which data is most important to your company and take extra precautions to protect it.

The key, however, may be to move beyond thinking of firewalls as an adequate protective measure. After all, cybersecurity is an arms race. When ancient engineers built walls, their enemies invented siege engines. As cybersecurity becomes more sophisticated, cybercriminals become more conniving.
90 percent of the internet's data was created in the last two years. To a cybercriminal, it’s like being a miner in an ever-expanding gold mine. Twitter alone has already generated more text than all the books in the world combined. All of that data generation is creating so much noise that it’s nearly impossible for human cybersecurity professionals to actually isolate and address threats; like focusing in on a single voice in a crowded party.

THE FUTURE OF CYBERSECURITY

Automation is the undeniable future of cybersecurity. The incredible data explosion of the last few years has happened alongside rapid improvements in technology, including breakthroughs in the development of effective artificial intelligence.

In 2016 there were one million unfilled cybersecurity positions around the world. It's becoming more apparent that there just aren’t enough qualified human beings to properly address the world’s cybersecurity needs, and there’s not enough time to train the requisite army of analysts. The logical solution? Let computers do the dirty work and free up existing professionals to make more important high-level decisions.

Artificial intelligence can comb through massive amounts of data, identifying threats as effectively as humans. It can work around the clock with no
holidays or breaks and identify trends and anomalies that would elude the attention of human analysts. And due to the major labor shortage in the field, they aren’t taking any jobs.

“62% of cybersecurity professionals believe we are less than 12 months away from a cyberattack that utilizes a weaponized form of artificial intelligence...”

Utilizing artificial intelligence will also help the cybersecurity jump forward and get ahead of cybercriminals; right now, cybersecurity can sometimes feel like a desperate race to stave off cyber crime rather than an active war against it.

Artificial intelligence will also be necessary to fight off hackers in the near future. 62% of cybersecurity professionals believe we are less than 12 months away from a cyberattack that utilizes a weaponized form of artificial intelligence, and there’s simply no way human technicians could effectively fight such an attack.

The good news for small businesses is that while the automation of cybersecurity is still absolutely essential, there’s still time to prepare. The deadliest cyberattacks are carried out between nation-states or against larger enterprises; while cybercrimes against small businesses are still incredibly common, your business has a window to effect proper cybersecurity measures.
CONCLUSION

As a business owner, you have a responsibility to take cybersecurity seriously. It’s an ethical obligation to yourself, your clients, and your employees. Cybercrime isn’t something anyone wants to think about, but it’s a very real threat to the integrity of any business. If you’re serious about making your business a hacker’s nightmare and ensuring the security of your data, don’t hesitate to get in touch. The 3Points team has experience with cybersecurity and a mission to help Chicagoland businesses leverage technology to reach their full potential.
Locations:

1100 Jorie Boulevard, Suite 100
Oak Brook, IL 60523

7820 Graphics Drive, Suite 106
Tinley Park, IL 60477