Why Small Businesses Must Deal With Emerging Cybersecurity Threats



September 2, 2020 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Companies worldwide have made work from home (WFH) arrangements for employees while still trying to focus on acquiring customers. While most have been able to keep running, there's a lurking crisis waiting to happen. Cybersecurity threats are becoming more dangerous as criminals take advantage of the crisis by monetizing stolen identities, installing viruses and malware and hijacking passwords and digital funds.

According to Accenture's 2020 Cybersecurity Report, organizations that lead in implementing best practices are

four times more effective in stopping attacks, three times better at fixing breaches and two times better at reducing a breach's impact. The authors say the most prepared companies do three things – invest for operational speed, drive value from investments and sustain what they have.

I spoke with Dr. Oren Eytan, former head of the IDF cybersecurity unit and CEO of Odix, to get his thoughts on how to improve online business security. And he cautioned that, "Hackers are constantly developing new and more complex malware variants to circumvent conventional security solutions."

Here are common threats you'll see, along with suggestions for protecting your business.

Longer passwords prevent ID theft

Nearly 40 million Americans have filed for unemployment benefits since March. Unfortunately, scammers in the U.S. and abroad are taking advantage of overwhelmed state unemployment systems. This year, hackers will use stolen identities to collect at least $26 billion in fraudulent payments, according to Congress's estimate. The Labor Department thinks that in a best-case scenario, 10 percent of unemployment payments will constitute waste and abuse.

"In the age of social and mobile, your digital identity is your life," Dr. Eytan says, adding that as a result of the expansion of these outlets, "A long, easy-to-remember password is essential to securing one's online profile, financial accounts and preventing ID theft."

Consider combining keywords, phrases, names, dates and events that only you would know. For example, "briansdogbunny20" or "love20starbucks" or "proud77armyvet" are all easy to remember and extremely difficult for an unauthorized individual to guess. Other examples of longtail passwords are

“feedmycat730pm” or “fianceweddingMay2021.” You should also change passwords once or twice a year for extra security.

Related: It’s Time to Stop It With the Terrible Passwords

Malware helps criminals stay quiet

Malware is a silent threat to small businesses and individuals. Malicious software can be programmed to partially control a computer or device. Last year, there were 9.9 million malware attacks, according to SonicWall’s 2020 cybersecurity report. More than a third (37 percent) of newly detected malware hide in Microsoft Office and Adobe PDF files. Google’s Transparency Report sheds some light on where malware originates.

Although there are lots of products on the market to help fight against malware, Eytan warns they aren’t all the same. “While antivirus and anti-malware solutions are commonplace among computer users, these solutions often fall short of addressing newer and ever-more complex malware strains,” he says. “Polymorphic malware can automatically change their code in order to evade signature-based detection most antiviruses use.”

Work-from-home employees may access company resources through unsecured devices and networks. Businesses should implement measures to protect their data while enabling workers to collaborate online. Nearly two-thirds (62 percent) of cybersecurity professionals believe their firm’s cybersecurity team is understaffed, according to a 2020 report by Information Systems Audit and Control Association (ISACA).

In one particular case, hackers exploited the coronavirus crisis by renaming their malware “Coronavirus Finder,” which supposedly detected nearby people infected with Covid-19. In reality, the criminals used the mobile app to gain access to people’s bank card details and intercept text messages and

two-factor authorization codes.

Related: 5 Best Practices for Remaining Malware-Free

Cryptojacking is an emerging threat

Cryptojacking has been on the rise ever since cryptocurrencies became more valuable. Cryptojacking is the unauthorized use of a computer, laptop, server or smartphone to mine cryptocurrencies and steal from users. Unfortunately, hackers also divert your hardware's computing capacity and electricity for their purposes.

They typically entice victims to visit a fake website, install a virulent app and/or click a false link that secretly installs malicious code on your device. According to a 2018 report by Cyber Threat Alliance (CTA), in 2018 there was a "459 percent increase in illicit cryptocurrency mining malware detections since 2017." Cryptos are a new asset class that even Wall Street investors find valuable, so cybercriminals are incentivized to steal digital funds.

The pandemic should make companies and individuals vigilant of online scams. The hardest-hit state for fraudulent jobless claims is Washington state. So far this year, the state has lost $650 million in benefits to criminals (although officials said they've recouped $350 million). The huge loss comes from 200,000 claimants being red-flagged, although many are innocent people whose lives have been turned upside down thanks to fraudsters triggering slow investigations from state bureaucracies.

Consumers should delete unnecessary apps, browsers and software to prevent malicious code from operating in the background. You should only visit credible websites. As a sidenote, adult sites are notorious carriers of malware and viruses. Scams and cyberattacks are proliferating worldwide. By following safe IT practices, you can protect your personal

and business assets from being stolen.

loading…

https://www.entrepreneur.com/article/354862