TECHNOLOGY

Why Your Business Might Be a Perfect Target for Hackers

BY JOHN BRANDON @JMBRANDONBB

Think you're too small to catch the attention of hackers? Big mistake. Your company might be exactly what they want.

For many years, the average American small business was an unlikely target for a sophisticated cyberattack. Fewer Ìinancial resources and a relatively unknown brand worked in your favor to ward oÌf hackers. Not anymore.

The dam has broken for small companies when it comes to security. Jeremy Grant, an adviser at the Department of Commerce's National Institute of Standards and Technology, says in the past two years he has seen "a relatively sharp increase in hackers and adversaries targeting small businesses."

According to the security company Symantec, cyberattacks on small businesses rose 300 percent in 2012 from the previous year.

Smaller companies are attractive because they tend to have weaker online security. They're also doing more business than ever online via cloud services that don't use strong encryption technology. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick. If you have any Fortune 500 companies as customers, you're an even more enticing target--you're an entry point.

Worse, the laws safeguarding commercial bank accounts aren't as strong as those for personal accounts. Banks won't always reimburse businesses whose accounts get hacked, especially if a bank can prove its security meets federal guidelines, but the business's isn't up to snuÌf. (Individuals aren't expected to have strong security in place.)

Patco Construction, based in Sanford, Maine, learned this the hard way when hackers siphoned $588,000 from its bank account in 2009 and its bank refused to reimburse the full amount.

Patco sued the bank and finally won after two appeals. The court ruled that despite the bank's security, it should have caught the suspicious transactions.

So what can you do about the growing threat of hackers? First, put in place the best tech barriers you can afford, like a cloud-based security app. Then patch your biggest vulnerability: your people, says Chris Hadnagy, founder of security training firm Social-Engineer.

Teach employees not just to devise smarter passwords and spot sketchy emails but also to think critically about their online actions. "If you just want people to follow the rules--don't think, just do--you create an easy environment for [hackers]," he says.

IMAGE: MATTHEW HOLLISTER

FROM THE DEC. 2013/ JAN. 2014 ISSUE OF *INC.* MAGAZINE

@JMBRANDONBB

JOHN BRANDON | Columnist

John Brandon is a contributing editor at *Inc.* magazine covering technology. He writes the Tech Report column for Inc.com.

The opinions expressed here by Inc.com columnists are their own, not those of Inc.com.