10 Ways to Protect a Small Business From Hackers

Richard E. LaCross
LaCross Financial Advisors

537 Massachusetts Ave
#201
Acton, MA 01720

(978) 289-4150

https://www.lacrossfinancialadvisors.com/

–Devin Kropp

As a small business owner you have a lot on your plate, but you need to start educating yourself on another issue threatening businesses.

Identity thieves have branched out. They're not just after individuals anymore—businesses are the new target for hackers and fraudsters.

With their deep credit lines, multiple users, and many financial transactions, businesses make it easier for thieves to operate, since their erroneous charges typically go unnoticed for a longer time in the busy business setting. These crimes can happen right under your nose before there is even a whiff of the theft.

Take a Sacramento law firm that was fraudulently charged $70,000 after a group of thieves impersonated the company, moved in to the same building, and ordered computers, furniture, and other goods on the firm's company credit card. The fraudsters moved out of the building before the charges were ever discovered.

This growing threat puts many small-business owners at risk, especially if your business credit line is tied to your personal credit. Thieves that gain access to your business may compromise your personal accounts as well, which can be devastating.

A National Cybercrime Security Alliance study found that one in five small businesses fall victim to cybercrime each year, with 60% of those victims going out of business within six months.

There are two main ways that thieves steal businesses identities: impersonation and hijacking.

Impersonation

In this type of fraud, a thief impersonates your business to steal from the business itself or your customers. In both scenarios, fraudsters use phishing emails to gain personal information. As you may already know, phishing emails are fake emails created by fraudsters to either trick you into sharing personal information or install malware onto your computer.

When thieves are targeting a business, they send an email to someone within the company, perhaps the CFO, and pretend to be another person in the company. The fraudster may send a receipt that needs to be paid, but will attach a virus to the email. Once the email is opened, the virus automatically downloads and the fraudster can hack into the company system.

When attempting to defraud the customers of a business, thieves impersonate an email address from the company and send a phishing email to customers attempting to obtain their information.

Hijacking

The second kind of business identity theft is company hijacking. In these cases, a scammer uses your company's identity as a means to steal. Thieves change the registered contacts of your company, along with other details, such as address and phone number. They then purchase goods and services with the company account.

Some thieves may even use your company's identity to produce pirated products to sell for profit. Thieves are able to pull this scheme off by obtaining your business's tax identification number (which can easily be found), copying quality logos found on your website, or even duplicating business stationery. Sometimes they even produce a fake website identical to the real one, but they change the ".com" to another top-level domain, such as ".net."

The dangers

Clearly, identity theft can be detrimental to your business. A business can lose large sums of money and even go bankrupt due to hackers. If your personal account is connected to your business account, you can lose that money as well. Lastly, your reputation with consumers and customers can be damaged, and you may be viewed as unreliable and dangerous to do business with.

How to keep your business safe

But there are ways you can protect their business from fraud. You should:

1. Protect your business from fraud in the same way you would protect your personal accounts. This includes keeping your business's sensitive information in a safe place and verifying who you share that information with before doing so.
2. Educate all employees on business identity theft and tell them not to open suspicious emails or links.
3. Give sensitive information such as credit card numbers, customer information, and administrative passwords only to those who need it.
4. Make sure all employees are using secure usernames and passwords.
5. Monitor business credit reports. You can obtain these reports through the three major credit reporting agencies: Experian, Equifax, and TransUnion.
6. Set up two-factor authentication with your bank for wiring money.
7. Keep your computer software up to date. This includes the devices of employees that work from home.
8. Secure your wireless network. All businesses should have password protected Wi-Fi with a unique username and password. You should change the default name and password that came with the router to something more secure.
9. Register all versions of your domain name to keep them out of hackers' hands. This can be done through the registrar used to create the business's main site. Some popular registrars are GoDaddy, Register, and 1&1.
10. Set up Google Alerts for your business to keep an eye out on where your business name is popping up online.

Devin Kropp is a New York-based writer for Horsesmouth.