Published: March 13, 2017

Updated: April 21, 2021

The 4 Cyber Attacks Business Owners Need to Watch Out For

Michael Kelly

Data Breach (Https://Sba.Thehartford.Com/Tag/Data-Breach/)

With COVID-19 pushing customers online to shop more than ever before, protecting your business and customer data is a must. By educating yourself on some of the most common cyber threats, you can begin to take action to protect your company and customers. Here are the four cyber-attacks you need to know about in order to protect your small business.

1. Phishing

According to the Federal Bureau of Investigation (FBI), the amount of phishing scams increased in 2020 (_wp_link_placeholder), with 241,342 compared to 114,702 in 2019. Phishing strategies involve a malicious user who poses as a trustworthy source (e.g., your bank). Typically, they'll send you an email where they create a false emergency and request that you click a link to go to their website to resolve the issue. Once there, you're prompted to enter sensitive data, such as your:

- Bank username and password
- Account number

Feedback

- Social Security number.

In recent years, it has become easier for phishers to launch attacks against unsuspecting business owners thanks to social media. This is because most business owners, vendors and employees put their information on the web for anyone to gain access. This allows phishers to create highly personalized emails and websites that resemble those of the sources they're posing as. This helps increase the chances of duping business owners and their employees.

The FBI also recently found an increase in government impersonator schemes during COVID-19. For these, criminals are reaching out to people via email, social media or phone calls and pretending to be from the government.

2. Drive-By Download

"Just don't click anything and you'll be okay" is the mantra many business owners use when they accidentally stumble onto a suspicious looking website. Unfortunately, drive-by downloads make it possible for websites to upload malicious software to computers without you even clicking on anything. Simply visiting the website initiates the attack. Drive-by downloads are often combined with phishing emails.

3. Malware

Malware is a broad term used to describe malicious software that can damage your computer and gain access to sensitive data. There are several different types of malware that you need to be aware of:

- Adware is a form of malware that is often bundled with free or pirated versions of software and is designed to launch advertisements, or pop-ups, when your computer is using a web browser.

- Spyware is designed to spy on your activities and monitor things such as keystrokes and websites you have visited in order to steal passwords. It can also change your computer's security settings.

- Trojan horses appear as normal files or computer applications. Once downloaded, they give a malicious user access to your computer and information —including your passwords and bank account numbers.

4. Point-of-Sale Hacking

This is one of the more high-profile cyber attacks that hackers can launch against your small business. This strategy involves a hacker remotely scraping the credit card information stored on your point-of-sale device. Typically, this information is stored on a PoS device for only a microsecond before it becomes encrypted. That microsecond is just enough time for hackers to grab the vital credit card information and transfer it to one or more remote servers.

It is rarely just one credit card number that hackers steal. More often, hackers will gain access to a point-of-sales device and scrape credit card information for months before being detected.

So, how do hackers gain access to your point-of-sale device? They can physically break into it, but if your point-of-sale system is linked to your computers, then they can hack into it using any of the three cyber-attacks listed in this article.

You Know the Dangers. Now Learn How to Protect Your Business

Your small business is a bull's eye for many hackers. Learn everything you need to keep it—and your customers—safe from a cyber-attack by downloading your free copy of How to Safeguard Your Business from a Data Breach. (http://pages.mail.thehartford.com/SBA_eBook_Data-Breach/) This eBook provides information on cyber security that only the experts know about.

It'll help teach you:

- The everyday mistakes you and your employees make that expose your business to a data breach
- Best practices that you and your employees can turn into habits to greatly improve your business's cyber security
- How to create a data breach response manual and train your employees to defend against cyber attacks
- Which law enforcement agencies to contact in the event of a breach

Leave a Reply

Disclaimer: Comments are subject to moderation and removal without cause or

Feedback