TECH ASSETS

New Reading

As we find articles across the web that would be of interest to our clients, we add them to our Flipboard Magazine — *Tech 4 Every 1.* Check out some of the new articles collected just for you:

Patches Pitched to Address Cyber Hacking Risks Created by Intel Chip Flaws

Questions You Need to Ask About Your Cloud Storage and Backups

IoT - "Internet of Things" Basics for Small Business

Dear Aunt Sadie, Please Step Back From The Net Neutrality Ledge

https://flipboard.com/@assetbc/tech-4-every-1-bnunrt2vy

To make it easy to access, we also hyperlinked it in our email signatures.

February 2018

This monthly publication provided courtesy of Ellen Bailey, President of Asset Business Computing.

Our Mission:
Asset Business Computing works diligently to help our clients achieve IT productivity, protection, and peace of mind.

If You Think Your Business Is Too Small To Be Hacked… Then You're Probably A Cybercriminal's No. 1 Target!

In a world of rampant cybercrime, hackers thrive on the blind faith of their targets. Despite high-profile digital security breaches showing up in the news nearly every week, most people assume they're safe from attack. The thinking goes that while Fortune 500 corporations like J.P. Morgan, Sony, Tesco Bank, and Target have lost millions of dollars of data breaches in recent years, *my* business is far too small to justify a hacker's attention… right?

Wrong. In fact, it's quite the opposite. According to StaySafeOnline.org, attacks on small businesses now account for over 70% of data breaches, a number that appears to be on the rise. Close to *half* of small businesses have been compromised, ransomware attacks alone have skyrocketed a whopping 250% since 2016, and incidents of phishing have followed suit, as reported by Media Planet.

Owners of small businesses might be excused for erroneously believing themselves safe. After all, the hundreds of little guys paying out thousands of dollars in digital ransoms each and every day are a lot less newsworthy than, say, the CIA's recent hacking by the mysterious Shadow Brokers, or the 143 million sensitive customer records stolen in the recent Equifax fiasco. The lack of visibility of the more frequent, smaller-profile incidents plaguing the country can easily lull us into a dangerous false sense of security.

But why would a team of hackers zero in on a small-town operation when they

Continued on pg.2

Continued from pg.1

could be targeting a giant like Google? Well, which building is a petty thief more likely to target — the bank in the center of a busy downtown, packed with security guards and high-tech theft prevention equipment, or the house in an affluent part of the city, which the owners always keep unlocked while they're on vacation? Make no mistake — these hacker gangs aren't boosting a couple flat screens and a box of jewelry. They're gutting small businesses with ransoms that stretch to the very edge of their means, as much as $256,000 for a single attack, according to one TechRepublic analysis.

Of course, any small business owner will struggle to afford the security measures implemented by giant corporations. However, there is a balance to be struck between affordability and vulnerability. With just a little research, it's actually quite easy to find an array of robust and comprehensive digital security solutions to protect your company. Such programs can turn your business from low-hanging fruit into an impenetrable fortress.

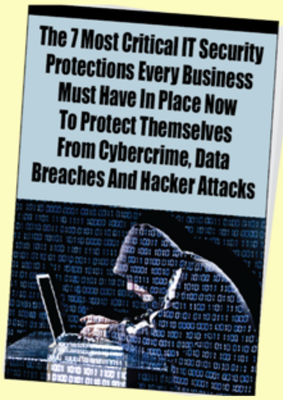
Even if you've somehow managed to make it through the past few years without a data breach, statistically, you can be confident that hackers *will* come for your business one day. With that in mind, it's important to be prepared. Just because you haven't had a life-threatening illness in the past two years doesn't mean you shouldn't have a wide-reaching health insurance policy. Just because your car hasn't broken down since you bought it doesn't mean you shouldn't regularly change the oil and invest in car insurance.

> "Cyber security isn't something you purchase to check off a box and give yourself an imaginary peace of mind. Instead, it's an investment in your company's future, the safety of your customers, and the longevity of your livelihood."

And just like your car, your network security requires regular maintenance and upkeep to stay effective. If you grab your security software from the bargain bin, install it and forget it, you're only marginally safer than you were before installing the barrier in the first place. Cyber security isn't something you purchase to check off a box and give yourself an imaginary peace of mind. Instead, it's an investment in your company's future, the safety of your customers, and the longevity of your livelihood.

If your business isn't too small to attract the attacks of hackers — and we guarantee it isn't — then it's certainly precious enough to protect. Cybercriminals *will* come for your business one day, but equipped with a set of up-to-date, powerful security protocols, you can rest easy knowing they'll go away empty-handed.

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information

Claim Your FREE Copy Today at

www.assetbusinesscomputing.com/cybercrime

4 Sneaky Ways Cybercriminals Used Phishing In 2017

Cybercriminals were more active in 2017 than ever before, with a staggering array of high-profile hacking incidents in the news each month. Here are four of the ways hackers used phishing to penetrate some of the most secure networks in the country last year.

Shipping Info Scam: Last July, an Internet security company called Comodo outlined a phishing strategy that was zeroing in on small businesses. Hackers sent phishing e-mails out to more than 3,000 businesses with the subject line "Shipping information." When the recipient clicked the tracking link in the body of the e-mail, it downloaded malware to their PCs.

WannaCry: This widespread ransomware exploited a weak point in the Windows operating system to infiltrate networks across the country. Once it was in, the malware locked users out of their files and demanded a hefty ransom to retrieve their data.

The Shadow Brokers: Last April, the ominously named Shadow Brokers released a huge number of classified tools used by the NSA, including Windows exploits, which hackers then used to infect businesses throughout the world.

Google Docs Phishing: In May, hackers sent out false Google Docs editing requests to over 3 million individuals. You know how the story goes — when recipients clicked the link, phishers gained access to their entire Gmail account.

SmallBizTrends.com 08/29/2017

What Makes You Stand Out

Whenever I work with the sales team of any organization, there is one specific question I like to ask that will tell me how skilled their salespeople are and how good their training has been. I always make sure to ask the question in a private setting.
"I have spoken to your top three competitors, and each of them have told me why I should do business with them. I would like to know why I should do business with you, instead. I want you to give me a two-minute commercial on what makes your company better than your competitors."

You would be amazed at how many times I get *awful* answers to that question. With this in mind, I think it would be advisable for all companies to spend some time thinking about and carefully answering the following questions.

1. What's your competitive advantage?

2. What are several ways your customer service stands out?

3. Are there ways you can sell value instead of selling price?

4. What makes you special?

5. What will make your clients tell their friends about you?

6. How can you deliver more than you promised to your client?

7. Is there anything you do better than your competition?

You can take all seven questions and roll them into a single inquiry: *What differentiates you from your competitors?*

For example, there is a financial planner who has each client's car detailed while he is conducting their annual review. I know a realtor who has an enormous lunch delivered to her clients when they move into the house they bought from her on their move-in date. I even know a remodeling contractor who has his employees clean up the worksite every day to show the respect they have for the client's home. When the job is done, he gives the client a giant ShopVac to reinforce the message. Would a plumber who put booties over his shoes before entering your home impress you? It sure impressed me.

Every business owner needs to ask themselves what they could do that would make them truly stand out from their competition.

Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

TECH TIP

by

Joshua Bagwell

MALVERTISING

What is malvertising? It’s the practice of inserting malicious code into ads that you see on both legitimate and not-so-legitimate websites. Websites make money by selling advertising, but most do not create or even have any control over which ads are displayed on their website. They farm this out to a third party that will display ads relevant to the viewers browsing history. The malicious code isn’t inserted by the third-party ad generator, but by the advertiser supplying the ads.

Every day a large number of ads are submitted to the various advertising networks globally, making it very difficult for the advertising networks to check each ad thoroughly. This automation makes online ads vulnerable to malvertising. Often advertisers work on a complaint based system waiting until a complaint is lodged against an ad or ads from a specific group before performing a deep analysis. In addition, it is very difficult to identify exactly which ad is malicious because the ads on a webpage constantly change. This means that one visitor may be infected, but the next ten, who visit the same webpage, won’t be infected.

Ways to prevent these infections are the same as preventing other malware infections. First, keep your system up-to-date including the operating system, browsers, browser plugins (Java, Adobe Reader, etc.), AntiVirus, and if your router/firewall does content filtering, make sure that’s updated too. Also, user training is essential. Finally, since malicious ads will display a popup ad trying to get you to click on them, using software that blocks ads, such as AdBlocker, is a good approach.

> *“There are two types of people who never achieve very much in their lifetimes. One is the person who won't do what s/he is told to do. And the other is the person who does no more than s/he is told to do.”*
>
> **~ Andrew Carnegie**

“To be fair, we were due for a correction.”

Do This BEFORE You Throw Out That Old Computer

If you’re throwing out your old computers or servers, it’s important to realize the risks. Not only are components used in digital equipment not safe for landfills, but they often contain a lot of confidential data. Instead of throwing equipment in the dumpster, find a local recycling facility to safely dispose of e-waste. And when you do, remove and destroy the hard drives inside.

LifeHacker.com 11/23/2017