TECH ASSETS

FREE
IT SECURITY TRAINING

71% of data breaches occur in small and medium sized businesses. The common thread in the attacks point to the weakest link in your IT network — your employees. **95% of breaches are caused by human error!**

To minimize the "human impact", during the **month of October** we are offering IT Security Training for your employees. There is **NO COST** to you.

The training includes slides with text and engaging videos with a security quiz at the end. Topics include PII, internal/external threats, phishing, phone scams, passwords, Wi-Fi dangers, BYOD, and many more.

The one hour training can be stopped and started to accommodate the employee's schedule. The time investment is well worth it. And your company will benefit!

Call (937) 435-0500 today to schedule training.

October 2017

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.

Skimp On Data Protection And Pay The Price

We've said it time and again: today's cybercriminals are using more advanced technology than ever. And those malicious tools are becoming even *more* sophisticated at a breakneck pace. To top it all off, new software developments are enabling these criminals to cast wider and wider nets, targeting businesses that, before, would have flown under their radar. Companies small and large, of every type, are being infiltrated by vicious cyber-attacks across the world each and every day.

Even knowing this, business owners are tempted to cut costs and corners. When you've never had a breach, data security can seem like a distant concern, especially for a limited budget. But regardless of which digital barriers you put in place to protect your business, you can bet on one thing: one day, your security will be tested by an attack. Whether or not the hackers punch through could mean the difference between your company shutting down for good — as 60% of small businesses do in the six months following a cyber-attack, according to the *Denver Post* — and remaining solvent and secure in your position.

When you're struggling to stay afloat or simply wanting to be a savvy spender, you may think the best way to lock down your data is to put one of your staff on the task or to do it yourself.

And sure, your team can conduct hours of research searching for inexpensive security. And you'll almost certainly find something cheap with good reviews and a decent track record. You'll figure out how to install the software across your system, complete with firewalls, server protection, antivirus and maybe a bell and a whistle or two. Perhaps you'll even hold a meeting to

Continued on pg.2

Continued from pg.1

educate your staff on the do's and don'ts of cyber security. "Use intricately constructed passwords," you'll tell them. "Don't click suspicious links in your e-mail."

Then, after a few days of fiddling with settings and ensuring the security software is properly in place, you'll forget about it altogether. After all, it's already installed, and you've checked to make sure there aren't any gaps in the system. It's not something you need to constantly monitor.

A year later, your business has — miraculously — doubled in size. You're finally reaping profits. Best of all, a recent news story has brought your company into the public eye, and brand-new leads are contacting you every day. For the first time since the company's inception, you can breathe easy.

Then, one Monday morning, you log in to your computer.

"Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses," wrote the Securities and Exchange Commission in a 2015 report. "The reason is simple: small and midsize businesses are not just targets of cybercrime; they are its principal target."

For a second, everything seems to be normal, until an innocent-looking pop-up fills your screen. "Attention!" an eerie robotic voice barks from your speakers. "Your documents, photos, databases and other important files have been encrypted!"

Thinking it's a hoax, you click into your server drive. To your dismay, you really are locked out of everything. So, palms sweating, you read the rest of the pop-up. It provides instructions to install the deep web browser Tor as well as an address for you to visit. When you go there, you learn that in order to recover all your data, including the credit card information of your customers, you'll need to dish out $50,000 in Bitcoin.

A year ago, you couldn't afford adequate cyber security. Can you afford $50,000 in cash today?

Identical situations are unfolding every day, with people *exactly like you*. Back in April, CNBC reported that across the previous 12 months, *half* of all small businesses had been infiltrated by malicious hackers. "Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses," wrote the Securities and Exchange Commission in a 2015 report. "The reason is simple: small and midsize businesses are not just targets of cybercrime; they are its principal target."

Cheapo security solutions might be fine for a lone browser surfing the web at home, but they are shockingly inadequate resources on which to base the entire success of your company, your livelihood and the livelihood of your employees.

Frankly, it's irresponsible to lock your data behind a flimsy $5 firewall. Invest in robust cyber security solutions and secure the future of your company.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer network that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.assetbusinesscomputing.com/protect
or call our office at (937) 435-0500.

Over $25 Million In "Ransoms" Paid Out In Just The Last Two Years Due To Ransomware Attacks

According to a study presented by Google last July, ransomware victims have paid out more than $25 million in ransoms over the last two years. Ransomware is a viral program that, after infecting a system, encrypts all the local files, making them unlockable only with a private key held by the attackers. Attackers then demand exorbitant sums of Bitcoin in order to recover the data — or threaten to make it inaccessible forever. The strategy has proven highly profitable for cybercriminals, who have adopted it in droves. Just this summer, San Francisco's largest public radio station was hit by ransomware, forcing employees to rely on mechanical stopwatches and paper scripts in the aftermath.

Additionally, it's clear from the data that ransomware designers are constantly developing more and more ways to penetrate antivirus software. When antivirus identifies a specific malware program, the system usually scans for matching binaries. But modern ransomware is able to change its binary once it has been detected, allowing it to skate past many outdated defense systems.

TheVerge.com 7/25/2017

Are Your Clients Sucking The Life Out Of You?

Bad clients aren't just a nuisance, they're bad for business. They can take an inordinate amount of time to service. They may complain about irrelevant details, avoid paying their bills or drag payments out forever. They can be a huge emotional drain. Or, more often than we care to know, they can do all of the above.

Firing these bad apples can be an attractive option. But what if that client is buying a profitable product from you? What if they're 60% of your revenue? Firing them will eliminate a big headache, but it may also put you out of business.

Not all clients are created equal. When you're considering a "keep 'em or kill 'em" approach, take these steps first.

1 CONDUCT A CLIENT ASSESSMENT

Assess your problem clients, considering factors like their historical revenue, projected future revenue, their core values and other indicators. Keep in mind, if a client was the ideal client before, you may be able to nudge them gently back to their former selves.

2 REMIND THEM WHY THEY DO BUSINESS WITH YOU

To you, a problem client is nothing more than a pain in the neck. But to them, your business obviously has redeeming qualities that keep them working with you. Schedule a meeting with the client and explain the challenges you are facing with them. Ask them if they'll make the commitment to improve. It may be an awkward situation, and they may say no, but either way, the conversation can't make things worse.

3 MATCH PERSONALITIES

Sometimes, business difficulties are nothing more than a personality mismatch. If you're consistently having trouble with the same employee, ask the client if they can assign a new liaison from the company. Even if you're dealing with the boss, they may be willing to let you work with one of their employees or colleagues instead.

4 LAY DOWN THE LAW

This is one of the toughest parts of being a vendor, but it's critically important. You need to clearly outline the rules of what is or isn't acceptable. Meet with the client and tell them exactly what is wrong, exactly what they need to do to fix it and exactly what the consequences will be if they don't.

5 SET A STOP-LOSS

Once you've tried addressing the issues you're having with the client, put in place a deadline by which your suggested changes must be implemented. Plan and commit to the action you will take at that time, depending on what the client does.

6 GET OUT OF THE TRAP

If nothing fixes the problem, yet you decide to continue the relationship, you need to realize the problem is not the client's, but yours. There is something in your actions that indicates you are willing to be treated the way they are treating you.

MIKE MICHALOWICZ (pronounced mi-KAL- o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford- a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com/

TECH TIP

by

Joshua Bagwell

COMPROMISED EMAIL

Is your mailbox a honey pot just waiting for a hacker to gain access? Consider the things that could be done if someone gains access to your mailbox. They have access to all of the personal information that is sent back and forth on a daily basis. They have access to all of your accounts tied to your email address, because when you reset a password where does it send the password reset to? They have access to your email which includes your bank accounts, credit cards, online retailers and on and on. If you do your taxes online, they are able to reset that password allowing them to see even more information and open new accounts in your name.

Once someone has access to your email they also have access to all of your contacts as well, allowing them to send email out as you, possibly distributing malware or sending massive amounts of spam causing your email account to get locked.

Taking back control of your mailbox may be more difficult than you think. If the person has also changed your recovery options to send the password reset request to their email address, they will be able to gain access once again. They could also have configured your account to forward all incoming email to their email address. So all recovery attempts are emailed to them as well.

There are some things you can do to reduce the pain if your email account is compromised. Whenever possible, enable 2 factor authentications for online accounts. They will have your password, but will be missing the second item, preventing them from logging on. Change passwords often, and make them as difficult as you can. Some online accounts such as banks will also send a notification if it detects unusual logon attempts.

"The way we do anything is the way we do everything."

~ Martha Beck

"Tom, as your legal counsel I feel I'd be remiss if I didn't recommend against this one last time."

You Need To Be Tracking These Critical Numbers

If you're looking to expand your small business, you need to focus on the fundamentals. However, many small business owners fail to effectively track key numbers in their company, putting them at risk for financial instability. Insure that you have a firm handle on the daily, weekly and monthly financial data and trends within your organization. Pay special attention to your gross margin, net income, earnings and "defensive numbers" — gross wages as a percentage of sales and overhead as a percentage of sales. Your cash plus accounts receivable divided by accounts payable/current liabilities will quickly give you a picture of how much cash you have on hand at any time.