

What's New

IS YOUR CYBER SECURITY AT RISK?

FREE LUNCH & LEARN SEMINAR March 15, 2018 12 noon

Learn from an experienced IT Security expert about:

1. A *SHOCKING* truth of bank fraud that could wipe out your company's bank account, yet most businesses are not aware of.
2. The #1 security threat to your business that antivirus, firewalls and other security protocols are defenseless against.
3. Why firewalls and antivirus software give you a false sense of security – and what it *REALLY* takes to protect your organization against new threats and today's sophisticated cybercrime.

Lunch provided; **RSVP NOW** by phone or email below.



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

February 2018



This monthly publication provided courtesy of Kurt Williams, Chief Information Officer at [C3 Technology Services](http://www.c3technology.com)

Contact US:

1536 E. Warner, Santa Ana, CA 92705
Phone: 657-383-4552
Email: marketing@c3os.com

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.

Continued on pg.2

Continued from page 1

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

“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.”

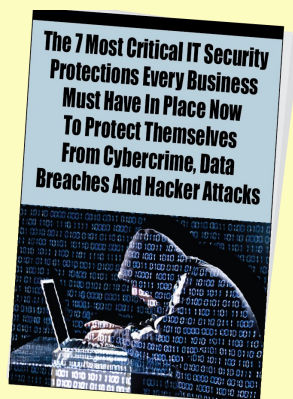


Even if you've somehow managed to make it through the past few years without a data breach, statistically, you can be confident that hackers *will* come for your business one day. With that in mind, it's important to be prepared. Just because you haven't had a life-threatening illness in the past two 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.

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

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 we're providing.

Claim Your FREE Copy Today at bit.ly/c3techtip

**Get More Free Tips, Tools and Services At Our Website: <http://www.c3technology.services/>
Or call: 657-383-4552**

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.



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 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.

Continued on pg. 4

What Makes You Stand Out

By Robert Stevenson

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 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. I think it would be advisable for all companies to spend some time thinking about and carefully answering the following questions:

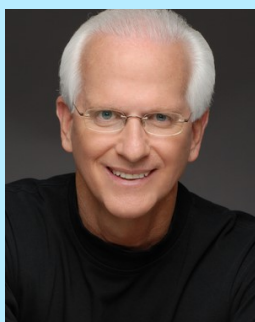
1. What's your competitive advantage?
2. What are several ways your customer service stands out?
3. Are there ways you can sell value instead of selling price?
4. What makes you special?
5. What will make your clients tell their friends about you?
6. How can you deliver more than you promised to your 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.

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.



1536 E. Warner, Santa Ana, CA 92705

We are your IT partner. One low flat monthly rate for unlimited support and IT services. We also provide Document Management Software, Printers, Copiers, Scanners, Digital Signage and Collaboration Whiteboards.

Continued from Page 3

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

