BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • July 2018

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

Top 4 Ways Hackers Will Attack Your Network

And They Are Targeting You RIGHT NOW

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy – why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork out thousands of dollars to malicious hackers and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network … While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge.

Start here with the four most common ways hackers infiltrate hapless small businesses.

1) PHISHING E-MAILS

An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to complete the process. But when they click the link, they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

It's one of the oldest tricks in the hacker toolbox, but today it's easier than ever for an attacker to gather key information and make a phishing e-mail look exactly like every other run-of-the-mill e-mail you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

2) BAD PASSWORDS

According to Inc.com contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

Continue on Page 3...

Grow Your Business by Creating a Business Plan or Watch It Fail

by Irv Michaels

Most of my clients come to me because their business has reached a plateau and has stalled. They have stopped growing, and they don't know how to breakthrough to the next level. Not having a business plan for growth increases the risk that can lead to a fadeout and ultimate failure.

"The biggest missing element entrepreneurs and business owners have when pursuing their goals is holding themselves accountable. Without a structure in place, there is nothing holding our feet to the fire." *Justin Sachs, Forbes*

A business plan starts with accountability and soul-searching assessment of the business today and the vision of tomorrow. It is not easy, and, often, an objective party is needed to move them through the process. Evaluating their current products and services, sales, operations, human resources, technology, etc. can lead to new structures, accountability, and realistic risk assessment.

The key components of the business plan for strategic growth

1. **Strategy**
2. **Execution**
3. **Milestones and metrics**
4. **Essential business numbers**
5. **From then on keep it fresh**

Tim Berry, founder and
CEO Palo Alto Software and Bplans.com

Using the **SWOT** analysis is a strategic planning technique used to help an organization identify the **S**trengths, **W**eaknesses, **O**pportunities, and **T**hreats.

A new client had a business plan created in 2013. The last time he looked at it was 2013! Often when a plan is completed, they are filed away and disregarded.

The business plan should be an active document to measure goals and results.

"Change before you have to." —Jack Welch

Today, customers demand more and better products/services, customer service, prices and faster response. To compete, your technology and systems need to timely provide accurate financial information and reporting including key performance indicators (KPIs). In this way, the company can quickly assess and make decisions.

"Irv has been instrumental in mapping-out how our studio will grow in the next five years. His strategies for business planning, financial planning and human resource management have allowed us to create a clear plan informed by a holistic view of the company's position and potential."
Glen Cummings, owner,
MTWTF, a graphic design studio

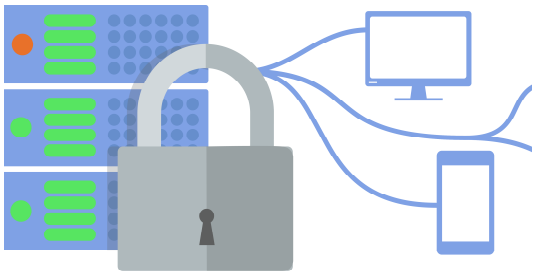
The old adage "Grow or Die" applies to every business. It is essential for any organization to be accountable for its goals and being flexible to adapt to unexpected situations that inevitably occur. The business plan is a tool to a guide to get your company to the next plateau.

Irv Michaels, CPA, is the Founder of Michaels Consulting, Ltd., a business advisory firm helping entrepreneurial businesses thrive by providing business plans and financial, business development, human resources and technology advice.

...*Continued from Page 1*

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. Instead, it's a good idea to make a password out of four random common words, splicing in a few special characters for good measure. To check the strength of your password, type it into HowSecureIsMyPassword.net before you make it official.

3. MALWARE



As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typosquatting"), a USB drive loaded with viruses or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats. These tools are not typically very expensive to put in place, especially considering the security holes they plug in your network.

4. SOCIAL ENGINEERING

As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but honestly, the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, but if you've done everything you can to prepare, your business will be safe.

The Lighter Side….

There was a man who worked all of his life and saved all of his money. He was a real miser when it came to his money. He loved money more than just about anything, and just before he died, he said to his wife, "Now listen, when I die I want you to take all of my money and place it in the casket with me. Because I want to take all my money to the after life."

So he got his wife to promise him with all her heart that when he died she would put all the money in the casket with him. Well one day he died.

He was stretch out in the casket, the wife sitting there in black next to their best friend. When they finished the ceremony, just before the undertakers got ready to close the casket, the wife said "Wait a Minute!"

She had a shoebox with her, she came over with the box and placed it in the casket. Then the undertakers locked the casket and rolled it away.

Her friend said, "I hope you weren't crazy enough to put all that money in there with that stingy old man."

She said, "Yes, I promised. And I don't lie. I promised him that I was going to put that money in the casket with him."

"You mean to tell me you put every cent of his money in the casket with him?" asked her friend.

"I sure did," said the wife. "I got it all together, put it into my account and I wrote him a check."

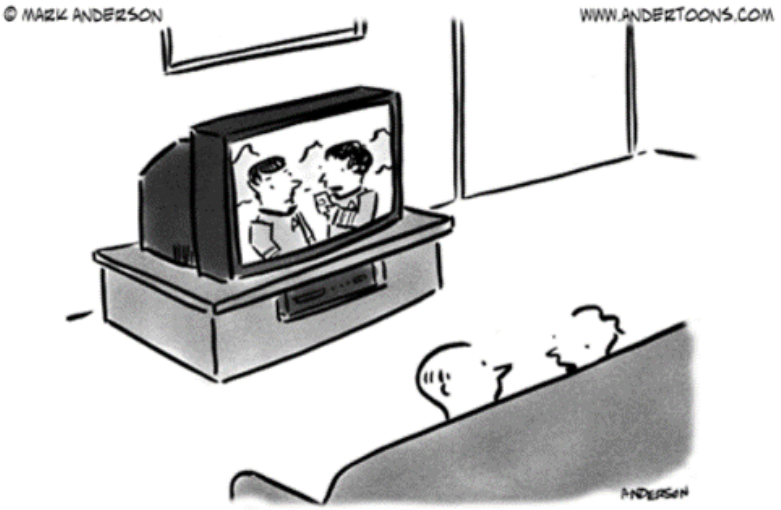
July 2018

35 Aztec Court
South Barrington,
IL 60010

(312) 752-4679

www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"



"If this is the future, how come their phones can't take pictures?"

Shiny New Gadget of the Month

Introducing The Snap SmartCam

Today, the security of your home is more important than ever before. Lawbreakers are constantly getting bolder, and as our technology advances, they switch up their tactics. With that in mind, all of us should be on the lookout for a security camera that's difficult to spot, is intelligent about the footage it collects, and grabs high-quality footage to identify burglars.

Enter the Snap SmartCam, a tiny little camera that looks — and operates — just like a phone charger. The innocuous-looking device uses motion-detecting technology to pick up when shady activity is going on in your house, and takes high-quality footage to catch a person in the act. If you're interested, the camera will cost you $57.00 at the time of writing, a great deal for a security camera of any type, much less one that seems so useful.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc