CLEVELAND
815 Superior Ave Suite 1711
Cleveland, Ohio 44113

THOUSAND OAKS
365 E. Avenida De Los Arboles Ste. B213
Thousand Oaks, CA 91360

VANCOUVER
365 E. 9504 NE 41st Ave
Vancouver, WA 98665

360.450.4759 · www.silverliningstechnology.com

Technology Times

Insider Tips to Make Your Business Run Faster, Easier, and More Profitably

We are looking for other business owners who have at least 50 employees and have multiple locations and who may be frustrated with their current IT company. Also, any business that is moving, expanding or growing fast. These are all situations where we can provide advice and services to help them be more efficient, profitable and help ease the frustration.

To show our appreciation for your help, we'll send you a delicious Pinot Noir from Oregon just to say thanks for the introduction. If they enroll in one of our services, we'll give YOU 50% off of your subscription service for new signed contracts. If you're a go-getter and you send us 5 potential client names, you'll not only get the Pinot but a $100 Visa gift card.

If you would like us to donate the referral money to a charity on your behalf, just let us know!

silverliningstechnology.com/about/referral-program

July 2018

The newsletter is provided by Steve Arndt, president of Silver Linings Technology.

Our Mission:
To build a community of success-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

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 them 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.

Continued on page 2...

... continued from cover

1 PHISHING EMAILS

An employee receives an e-mail directly from your company's billing company, urging them that they require your employee to fill out some information before they can finalize their paycheck. 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.

> **"Hackers can hook up automated strikes to lift data from thousands of small businesses at a time — the hit rate is that high."**

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."

As a manager, these statistics should bother you. 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.

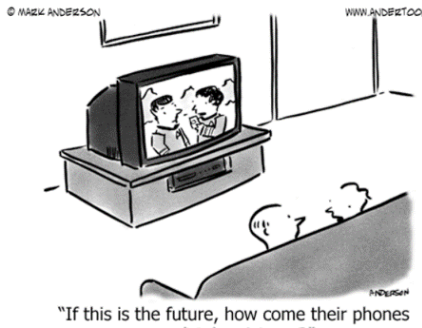
Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T Until You Read This ...

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Email Us For Your Free Copy Today:
info@silverliningstechnology.com

Cartoon Of The Month



"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 at the time of writing, a great deal for a security camera of any type, much less one that seems so useful.

Senior Risk

Silver Linings Technology is proud to work with outstanding companies that provide incredible services to the senior community. This month, we would like to feature Senior Risk, LLC. Founded in 2005 by Jay Stowers, Senior Risk is one of the top quality and clinical consulting firms in the U.S. With his extensive experience in the field, Mr. Stowers is known to many as the leading risk management consultant in senior living. Currently, Senior Risk is responsible for providing consulting services to over 1,400 senior housing communities and has conducted over 3,000 onsite QA reviews in 44 states! Their website hosts Senior Risk University, which provides comprehensive reference material and in-service training modules for caregivers working in various senior health care positions. With a qualified, competent staff and an extensive list of services available to seniors as well as caregivers in the field, it is no wonder Senior Risk is considered the premier consulting group in the industry.

Want to learn more? Check out their website at **www.srrisk.com/index.aspx**.

Leadership Is Lacking

Professor and leadership expert James O'Toole once said that "95 percent of American managers today say the right thing… 5 percent actually do it." I'm confident this is more true today than ever before. When I look around at the current business landscape, I see poor leadership destroying companies from the inside out. Disengaged employees, and especially those who abandon an organization altogether, cost companies billions of dollars each year, and as they say, people don't leave companies – they leave bosses. 46 percent of employees leave their job because they feel underappreciated, while 75 percent of employees cite their boss as the most stressful part of their job.

Luckily, the inverse of this is also true: Great leaders find that happy employees are 31 percent more productive, and 56 percent more effective at sales!

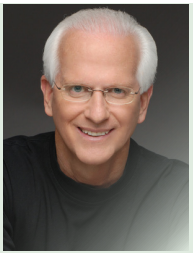
But what makes a great leader? A truly excellent leader makes people believe in themselves, feel good about working for the company, and, most importantly, feel special about being chosen to work there. Ralph Hart, a former CEO for Heublin, a company with thousands of employees, made it a policy to personally greet every new hire. He'd sit down with them during the first month of their employment to have a short chat and let them know just how he and the company felt about them joining on. He would tell them that "The company you are working for is first-class. I want you to know we have first-class products, first-class marketing, first-class advertising and first-class customer service." However, he'd always stress that, "To be able to list everything we do as first-class, we have found that we must hire only first-class

people!" He made sure they knew that he was delighted to have them on the team.

In less than two minutes, this CEO made an enormous impact on his new employee. They couldn't believe that the CEO of this huge company even knew their name, much less believed that they were a first-class talent. There's nothing better than making someone feel special – nothing better than telling someone you believe in their abilities.

Ralph Hart knew better than anyone that how you treat your employees is how they will treat your customers and associates. If you want first-class employees, then treat them as such. They'll respond in turn by going out of their way to do more, deliver more, help more, innovate more and stick around for the long term.

When you think about your employees' needs ahead of your own, the success of your business will take care of itself. If you show them that you are concerned about them advancing in their career, then they will help your company prosper. When you help them to succeed, they will help *you* succeed. Your relationship will grow and the need to micromanage will never be a concern.



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.*

SILVERLININGS TECHNOLOGY
9504 NE 41st Ave
Vancouver, WA 98665

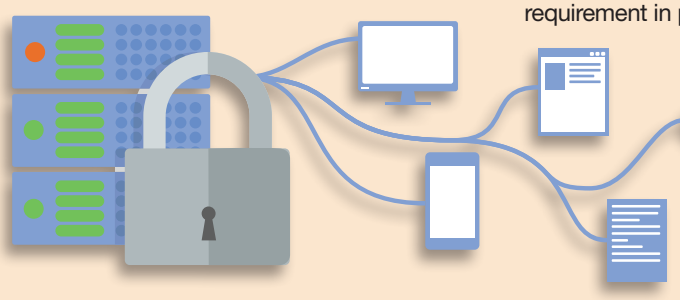
PRST STD
US POSTAGE
PAID
BOISE, ID
PERMIT 411

Inside This Issue

What To Do BEFORE You Go To Starbucks

You're in the car on the way home from Starbucks, basking in the glowing of your triple-shot, low-foam, extra hot pumpkin spice latte when you suddenly realize your laptop has gone missing. You drive back to the store like a caffeinated lunatic, only to discover no one has turned it in. What do you do?

Well, first you should notify your IT department (us!) immediately to tell them your device has gone missing. That way, we can change passwords and lock access to applications and data. We can also remotely wipe your device to make sure no one will be able to gain access – a key reason it's critical to back up your data on a daily basis.



Next, change ALL the passwords to every website you regularly log into, starting with any sites that contain financial data or company data. If your laptop contained others' medical records, financial information, or other sensitive data (social security numbers, birthdays, etc.), you should contact a qualified attorney to understand what you may be required to do by law to notify the affected individuals.

An ounce of prevention is worth a pound of cure, so make sure you're engaging us to encrypt/back up your data, and put remote monitoring software on all your mobile devices. Put a pin-code lock or password requirement in place to access your devices after 10 minutes of inactivity, and get in the habit of logging out of websites when you're done using them.

6 Surefire Ways To Protect Yourself From Data Leaks, Hacks, And Scandals

1. Reconsider what you put online. This goes beyond social media posts. Even sharing your telephone number with a store associate can come back to bite you later.
2. Use password managers. This way, you can use different, randomized passwords for all your sites without losing track of them.
3. Use two-factor authentication. It's a no-brainer.
4. Encrypt the information on your drive. It's easier than it sounds!
5. Read privacy policies, otherwise you may be signing away more than you think.
6. Monitor your credit. That way, if someone tries to use your info to make a big purchase, you can stop it in its tracks.

Inc.com, 4/26/18