COMPUTER DEPOT INC.
BUSINESS SOLUTIONS

Tech Bits and Bytes to Help You with Your Business

Computer Depot Inc. Business Solutions Newsletter March 2019

Thomas Hill, President & Founder

"Prompt response means faster resolution and less down time, now let's GO!"

3 Ways Your Employees Will Invite Hackers Into Your Network

... And What You Must Do To Prevent It TODAY

No matter how professional they are, members of your team – yourself included – are going to make mistakes. It's true of every organization on earth. They'll spill scalding coffee into the company copier. They'll work overtime until the office is empty, then head home without thinking to arm the security system. They'll neglect key accounts, muck up workflows and waste hours developing convoluted solutions to simple problems. And, worst of all, they may unknowingly bumble into the cyber-attack that forces your business to go belly-up for good.

In the majority of cases, that will be by design. There's a saying in the cyber security industry, coined by renowned cryptographer Bruce Schneier: "Only amateurs attack machines; professionals target people." When it comes to repeating the same process safely and autonomously, machines are less fallible than the average person sitting at a desk. Savvy hackers looking to boost funds from unsuspecting small businesses know this. So instead of developing a complex program that dances around the security measures baked into sophisticated modern technology, they target the hapless folks on the other side of the screen.

The strategy works disturbingly well. According to IBM's 2018 X-Force Threat Intelligence Index, more than two-thirds of company records compromised in 2017 were due to what they call "inadvertent insiders" – employees who left the front door wide-open for the bad guys without even realizing it. Negligence, lack of awareness and sheer bad luck put the best -laid plans to shame on both sides.

But how does it happen? There are three

Continued on page 2

Daylight-Savings Time

begins March 10

TRIVIA

CONGRATULATIONS

Jeannie Allen
Operations & Business Manager,
Log Cabin Pancake House, Inc.

Although **1900** is divisible by four, **it was not a leap year**. In years ending with 00, the first two digits standing alone have to be divisible by four. Thus 1600 and 2000 were leap years, 1700, 1800 and 1900 were not. Now don't you feel smart?!

TURN TO PAGE 2 FOR THIS MONTHS TRIVIA

Continued from page 1

primary causes of employee-related breaches, each of them contributing to a sizable portion of hacks across the country.

1. Social Engineering

Phishing remains one of the most prominent strategies deployed by hackers to lift data from small and midsize businesses. The majority of these attacks stem from an employee clicking on a suspicious link that is embedded in a dubious or absolutely convincing e-mail. To lure your team into the trap, cybercriminals often use data gathered from cursory investigations of your organization from the Internet or social media. Maybe they pose as a security expert contracting with your company or a member of a customer support team behind one of your employees' personal devices. Whatever mask they wear, it doesn't take much to convince an uninformed individual to click on anything, resulting in a high success rate for phishing attacks.

2.Circumvented Or Incorrectly Implemented Security Measures

Even if you do everything you can to protect your business from digital attack, your team may dodge those measures anyway. According to a report by cyber security firm Dtex Systems, around 95% of companies have employees who will attempt to override the security processes. And that's if the security measures are configured, patched and installed properly in the first place. The IBM X-Force report lists "misconfigured cloud servers and networked backup incidents" among the chief concerns of last year.

3. Insiders With Malicious Intent

Hell hath no fury like an employee scorned. A strikingly large number of breaches come not from error at all, but from insidious tactics by disgruntled employees or undercover criminals looking to make a quick buck. It's not quite a "you can't trust anyone" scenario, but there are definitely folks out there who would sell your business right out from under your nose.

With each of these in mind, it's vital that you incorporate employee training and vetting protocols to maximize their cyber security know-how. In addition, you need to implement safe practices that reduce the room for human error, alert employees when something is amiss and protect them.

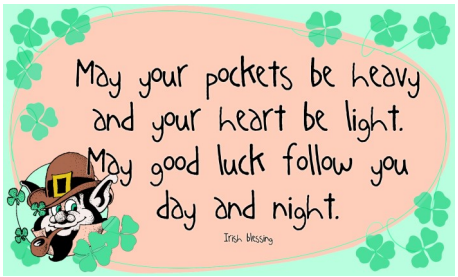
We can help. It's difficult to overhaul your cyber security, especially on the people side, without a round-the-clock team dedicated to pinpointing the weaknesses in your organization and working to patch them up. Partner with an organization that has expertise in training employees on security basics and bolstering your defenses, and head into Q2 knowing your assets aren't up to the whims of an unlucky employee.

" Thomas and the folks at Computer Depot are there when we need them and I know they are in the background ..."watching our back."

Melissa Quarve, Agate Group

AGATE

Welcome Spring! March 20



This Month's

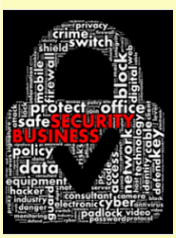
TRIVIA

Here is your next chance to WIN!

Who said it? "The way I see it, if you want the rainbow, you gotta put up with the rain."

Email your answer to RHill@ComputerDepotOnline.com

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, we will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security. Afterwards, we'll prepare a customized Report Of Findings and provide a Prioritized Action Plan. This report and action plan is likely to be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment, call 865-909-7606.

HIPAA FACTS

Protect Your Practice from HIPAA Violations

Top 3 Causes of Data Breach

Employee Action

Third-Party Error

Lost or Stolen Devises

The average cost

per lost record:

$401

HIPAA Fines Can Range From

$100-$50,000

67%

of healthcare organizations plan to spend money on HIPAA audit services.

Want to avoid a data breach and validate your compliance?

Call us today: 909-7606

"You want to throw off the hackers, so put something with 'CAT' in the title."

Client Spotlight

Remote Area Medical or RAM, held their 1000th free medical clinic last month in Knoxville and we were honored to be able to see up close the work that they do.

This expedition took an army of volunteers and it was an amazing event. Held in the Jacobs building in Chilhowie park, the 3 day clinic ran astonishingly smooth. The hours were long but the volunteers remained cheerful. We got to meet many of them at the snack station we set up and we have to say, these volunteers, they are the salt of the earth. They have hearts of gold and it was a privilege to watch them work.

Remote Area Medical

Medical care can be very expensive, so for decades RAM, an East Tennessee non– profit organization, has made it their mission to prevent pain and alleviate suffering by providing free quality healthcare to those in need. To learn more about RAM and the important work they do in communities big and small all over the United States and abroad, visit their website www.ramusa.org

3 Steps To Protect Your Business After The Marriott Data Breach

Last November, Marriott announced some bad news: the data of up to 500 million customers may have been compromised in an attack. If you travel regularly for business and are a customer of the Marriott chain –including Westin, Sheraton, the Luxury Collection, Four Points, W Hotels, St. Regis, Aloft, Element, Tribute Portfolio and Design Hotels – there are some things you need to do.

First, change your passcodes. This should include your potentially compromised account and any accounts that, for some reason, still use the same login or passcode in 2019. Also, keep a close eye on your credit card and bank accounts. Finally, be very careful about opening e-mails. We cannot say this enough! Cybercriminals love piggybacking on actual customer contacts from big corporations to send out phishing e-mails. SmallBusinessTrends.com, 12/13/2018

Computer Depot
Business Solutions
5416 S Middlebrook Pike,
Knoxville, TN 37921

PLACE STAMP HERE

March 2019

Look What's Inside...

- **3 Ways Your Employees Will Invite Hackers Into Your Network**
- Client Spotlight: Remote Area Medical, RAM
- Hurry-You could WIN this month's Trivia and this → LOWE'S
- 3 Steps To Protect Your Business After The Marriott Data Breach
- Windows End of Life Warning

COMPUTER DEPOT BUSINESS SOLUTIONS - WE ARE BIG TECHNOLOGY FOR YOUR GLICH-FREE SMALL BUSINESS

An URGENT Security Warning for Businesses Running Windows 7 or Windows Server 2008

If your organization is currently running Windows 7 on one or more computers in your office and/or if you are running Windows Server 2008, you need to know about a very real security threat to your organization that must be addressed in the next 11 months. Microsoft has officially announced that it will retire support on both the Windows 7 and Windows Server 2008. That means that any computer or server with these operating systems will be completely exposed to serious hacker attacks. This is such a serious threat that **all companies housing financial and medical information are being required by law to upgrade**. As a local Microsoft Certified Partner, Computer Depot Business Solutions is offering a Microsoft Risk Assessment and Migration Plan for free. Call today with your questions or to schedule this free consultation. 865-909-7606

Contact Us

Computer Depot
Business Solutions

For over two decades

Serving Knox and Sevier Counties

5416 S Middlebrook Pike
Knoxville, TN 37921
Phone: (865) 909-7606

or

10721 Chapman Hwy
Seymour, TN 37865
Phone: (865) 577-4775

Email: thill@ComputerDepotOnline.com
Visit us on the web at
www.ComputerDepotBusiness.com