COMPUTER DEPOT INC.
BUSINESS SOLUTIONS

Tech Bits and Bytes to Help You with Your Business

Computer Depot Inc. Business Solutions Newsletter April 2020

Thomas Hill, President & Founder

"The road is paved with dead squirrels that couldn't make a decision!"

What You Need To Know In Order To Protect Your Network While Employees Are Working From Home!

If you have found yourself massively disruptive and scrambling to figure out a way to keep things going during this pandemic, you are not alone. Whether your business is considered essential or non-essential, you are undoubtedly trying to figure out a way to protect yourselves, your family, and your employees, all while trying to keep your business up and running. If that isn't stressful enough, the fact that you are still a target for hackers, scammers, and cyber criminals is almost unbearable. Here's the kicker these criminals are loving all the chaos and are counting on hitting it big when you are most vulnerable. The reality is, they don't need malicious code or advanced hacking skills to get what they want. Many of them are simply going to go through your own employees who are also distracted and vulnerable and put your network at risk.

It's a sad truth, but every day, now more than ever, employees of small businesses let hackers right in because they don't know better. They see an email with COVID-19 in the subject line. It seems official and urgent and they open it and click the link inside. By the time they realize they've made a mistake, they're too embarrassed to say anything. From there, the problem gets worse. Actions like this can end in DISASTER for your business. The problem is that most employees don't have the training to identify and report IT security issues. They aren't familiar with today's threats or they don't know to not click that e-mail link. There are many things employees are doing – or not doing – that cause serious problems for small-business owners. Here are some things people do that allow hackers to waltz in through your front door.

1. They don't know better. The COVID-19 news and barrage of

Continued on page 2

Happy Easter

TRIVIA

CONGRATULATIONS

The Ladies
At Deal's Distributing
DEAL'S SMALL ENGINE

Who knew that there are an estimated 1500 black bears in the Great Smoky Mountain National Park.

TURN TO PAGE 3 FOR THIS MONTHS TRIVIA

Continued from page 1

information (and misinformation) is non-stop. They have never been trained in cyber security best practices. While some of us may know how to protect our network, safely browse the web and access e-mail, many people *don't*. Believe it or not, people do click on ads on the Internet or links in their e-mail without verifying the source. This can be fixed with regular cyber security training. Call in an experienced IT security firm and set up training for everyone in your organization, including yourself. Learn about best practices, current threats and how to safely navigate today's networked world.

2. They use bad passwords. Many people still use bad passwords like "12345" and "qwerty." Simple passwords are golden tickets for hackers. Once they have a username (which is often just a person's actual name), if they can guess the password, they can let themselves into your network.

> **"The problem is that most employees don't have the training to identify and report IT security issues."**

Many security experts suggest having a policy that requires employees to use strong passwords. Passwords should be a mix of letters (uppercase and lowercase), numbers and symbols. The more characters, the better. On top of that, passwords need to be changed every three months, and employees should use a different password for every account. Employees may groan, but your network security is on the line.

3. They don't practice good security at home. These days, many businesses are relying on "bring your own device" (BYOD) policies. Employees use the same devices at home and at work, and if they have poor security at home, they could be opening up your business to major outside threats.

How do you fix this? Define a security policy that covers personal devices used in the workplace, including laptops, smartphones and more. Have a list of approved devices and approved anti-malware software. This is where working with an IT security firm can be hugely beneficial. They can help you put together a solid BYOD security policy.

4. They don't communicate problems. If an employee opens a strange file in an e-mail, they might not say anything. They might be embarrassed or worry that they'll get in trouble. But by not saying anything, they put your business at huge risk. If the file was malware, it could infect your entire network.

Employees must be trained to communicate potential security threats immediately. If they see something odd in their inbox, they should tell their direct supervisor, manager or you. The lines of communication should be open and safe. When your team is willing to ask questions and verify, they protect your business.

5. They fall for phishing scams. One of the most common scams today is the phishing scam. Cybercriminals can spoof e-mail addresses to trick people into thinking the message is legitimate. As the world struggles to contain the COVID-19 pandemic, people are scrambling to find trustworthy information about the spread of the disease, how they can protect themselves, how they can get tested, and more. Unfortunately, the spammers and scammers of the world are using the situation to take advantage of people during these uncertain times. The COVID-19 scams are everywhere right now and most involve attempts by companies and individuals to sell products they claim to prevent or cure the novel coronavirus. Scammers are peddling fake remedies ranging from colloidal silver to cow manure. They are also claiming to have test and of course they will need all your personal information. Criminals will do anything to trick people into opening fraudulent e-mails.

Overcoming these threats falls on proper training and education. Phishing e-mails are easy to spot if you take the time to do it. Look at the details. For example, a CEO's e-mail might be CEO@yourcompany.com, but the scam e-mail is CEO@yourcompany1.com. It's a small but significant difference. Again, it's all about asking questions and verifying. If someone isn't sure if an e-mail is legit, they should always ask.

"THANK YOU for taking such good care of me and my business. Your team worked diligently to get me up and running for tax season. My tax software is working and printing fine now too. You guys are awesome and I truly appreciate you and your computer knowledge."

Teresa Lipham
Tick Tock Tax Service

HIPAA FACTS

Protect Your Practice from HIPAA Violations

Top 3 Causes of Data Breach

Employee Action

Third-Party Error

Lost or Stolen Devises

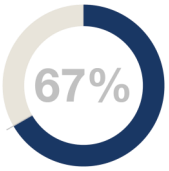
The average cost

per lost record:

$401

HIPAA Fines Can Range From

$100-$50,000



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

"I'm afraid there are some things we can't fix in Photoshop."

Things Mentally Strong People Don't Waste Time Doing

Overthinking – They look at their situation and take decisive actions. Some look at all the available information and go. Others rely more on their gut. Either way, they keep things moving forward. One of our favorite sayings around the office here at Computer Depot Business Solutions is "The road is paved with dead squirrels that couldn't make a decision!"

Regretting – It's natural to want a different outcome than the one you got or to think, "I should have done X instead of Y." But these thoughts can hold you back and lead to second-guessing yourself later.

Complaining – It can be healthy to complain. It gets your thoughts into the open where they can be discussed. But you have to discuss and arrive at solutions. Complaining for the sake of complaining – or complaining to people who can't help – is unproductive.

This Month's

TRIVIA

Here is your next chance to WIN!

How long is the federal tax code?

Email your answer to RHill@ComputerDepotOnline.com

4 Cyber Security Myths Business Owners Need To Know

Myth: Cyberattacks only come from external sources.

Reality: Upward of 90% of successful data breaches can be traced back to employee error. They may leave sensitive data on unsecured hardware rather than behind digital walls. They may open malicious files that copy and send data to an external location. Employee IT security training goes a long way to fix this.

Myth: Simple antivirus software or firewalls are enough to protect your business.

Reality: Cybercriminals use sophisticated tools to get what they want. The fewer security solutions you have in place, the easier it is. Antivirus software can't do anything to stop a motivated hacker, and firewalls should never be considered a primary line of defense. Web scanning and malware detection software can give you more protection on top of these.

Myth: Your business is too small or niche to be a target.

Reality: Cybercriminals don't care about the size or type of your business. They target everyone because they know they'll eventually break through somewhere. Small businesses are more appealing because they often lack serious cyber security solutions.

Myth: You don't collect payment or financial data, so you aren't worth targeting.

Reality: They aren't just looking for credit card details. They want usernames, passwords, e-mail addresses and other personal identifying information they may be able to use elsewhere because people have a bad habit of reusing passwords for other accounts, including online banking. *Inc., Dec. 16, 2019*

Computer Depot
Business Solutions
10721 Chapman Hwy #30
Seymour, TN 37865

PLACE STAMP HERE

April 2020

Look What's Inside…

- **What You Need To Know In Order To Protect Your Network While Employees Are Working From Home!**
- Things Mentally Strong People Don't Waste Time Doing
- Hurry-You could WIN this month's Trivia and this

- Our Favorite Spring Hikes
- **WARNING:** 4 Cyber Security Myths Business Owners Need To Know

COMPUTER DEPOT BUSINESS SOLUTIONS - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

Some Favorite Spring Hikes: For good mental health while practicing social distancing

1. **Cades Cove** Go during the week to avoid the massive crowds that grow each year. Remind yourself that there is a reason it is so popular. The cove is lovely anytime of the year, but really early you can see daffodils that mark homesteads of the past. Hike any of the trails, or get out and sit for a bit, but whatever you do, get out of your car and take in the beauty of the cove.
2. **Chestnut Top Trail.** This trail starts near the Townsend Entrance across from the Y. Wildflowers, Wildflowers, and more Wildflowers. I have never gotten more than about a mile before it was time to turn around and come back because I love taking pictures of wildflowers. My family does not understand, THEY ARE ALL DIFFERENT!
3. **Andrews Bald,** down and back is 3.6 miles. The trail features stunning displays of flame azaleas and rhododendron during the late spring. Pack a picnic and have lunch with a view.

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