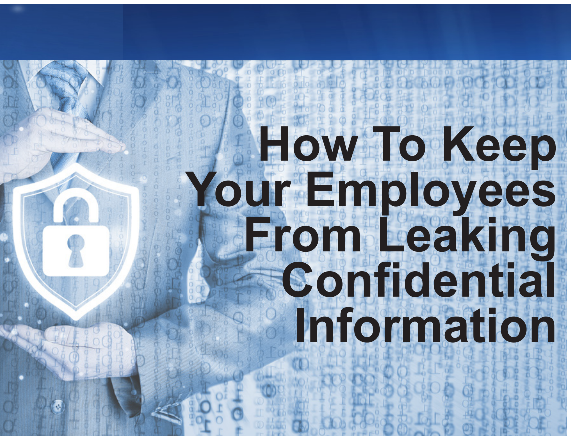
Business System Solutions

June 2017

The BSS Advisor



# How To Keep Your Employees From Leaking Confidential Information

Back in 2014, Code Spaces was murdered. The company offered tools for source code management, but they didn't have solid control over sensitive information — including their backups. One cyberattack later, and Code Spaces was out of business. Their killer had used some standard techniques, but the most effective was getting an unwitting Code Space employee to help — likely via a phishing attack.

When it comes to cybercrime that targets businesses, employees are the largest risks. Sure, your IT guys and gals are trained to recognize phishing attempts, funky websites, and other things that just don't seem right. But can you say the same thing about the people in reception, or the folks over in sales?

Sure, those employees might know that clicking on links or opening attachments in strange emails can cause issues. But things have become pretty sophisticated; cybercriminals can make it look like someone in your office is sending the email, even if the content looks funny. It only takes a click to compromise the system. It also only takes a click to Google a funny-looking link or ask IT about a weird download you don't recognize.

Just as you can't trust people to be email-savvy, you also can't trust them to come up with good passwords as people still use birthdays, pet names, or even "password" as their passcodes — or they meet the bare-minimum standards for required passcode complexity. Randomly generated passcodes are always better, and requiring multiple levels of authentication for secure data access is a must-do.

**When it comes to cybercrime that targets businesses, employees are the largest risks.**

Remember, that's just for the office. Once employees start working outside of your network, even more issues crop up. It's not always possible to keep them from working from home, or from a coffee shop on the road. But it is possible to invest in security tools, like email encryption, that keep data more secure if they have to work outside your network. And if people are working remotely, remind them that walking away from the computer is a no-no. Anybody could lean over and see what they're working on, download malware or spyware, or even swipe the entire device and walk out — all of which are cybersecurity disasters.

Last but not least, you need to consider the possibility of a deliberate security compromise. Whether they're setting themselves up for a future job or setting you up for a vengeful fall, this common occurrence is hard to prevent. It's possible that Code Space's demise was the result of malice, so let it be a warning to you as well! Whenever an employee leaves the company for any reason, remove their accounts and access to your data. And make it clear to employees that this behavior is considered stealing, or worse, and will be treated as such in criminal and civil court.

You really have your work cut out for you, huh? Fortunately, it's still possible to run a secure-enough company in today's world. Keep an eye on your data and on your employees. And foster an open communication that allows you to spot potential — or developing — compromises as soon as possible.

Lafayette Office:
1211 Cumberland Ave.
West Lafayette, IN 47906
(765) 742-3440

Kokomo Office:
3138 S Lafountain St.
Kokomo, IN 46902
(765) 507-9583

www.bssconsulting.com

**BSS** is your IT Partner providing **Total Care** support for all your technology needs with exceptional **Customer Service** and the best IT Solutions to make ***your business*** more productive and profitable!

A publication of Business System Solutions, Inc. | Managing Technology For Small Businesses Since 1995

## IT Security Tip #17: Don't Just Close Your Browser!

When online accessing a banking site or any other application containing sensitive data, make sure you log out of the site and THEN close your browser. If you simply close your browser, some of the session information that a hacker can use to gain entry is still running in the background.

## Font Not Found Message In Firefox Could Carry Nasty Malware

Several months ago, a nasty malware attack caused quite a stir among Google Chrome users.

After a flurry of activity, it went dormant. Now, it seems to have returned, and this time, it's targeting Firefox users. The basic form of the attack is unchanged, however. From the user's perspective, it looks like this:

You surf to a webpage that is unreadable. You get a popup message that says "The HoeflerText" font was not found. The message box helpfully provides an update button that supposedly allows you to install the font on your computer.

When you click the button, though, rather than getting the font, you get a banking trojan called Zeus Panda. It will then log your password, and it can initiate rogue transactions in your name.

Unfortunately for the hackers, they didn't bother to change the name of the font. "HoeflerText" was the exact bogus font name they used a few months ago when they targeted Chrome users, and by now, is quite well known.

Even if it weren't, this is a fairly crude, heavy-handed attack that only fools a small percentage of users.

The simplest way to avoid having the malware installed is to simply close the browser window any time you see a page load that contains garbage characters and asks you to install a new font, regardless of the font name. It's almost certainly a trap.

If you do inadvertently click to install the font, contact a member of your IT staff immediately, and don't do anything else with or on the PC until the malware is removed.

Remember, once this malware is armed with your credentials, it can initiate transactions on its own. From the bank's perspective, every transaction this malware initiates appears to be perfectly legitimate, which can cause you no end of trouble, and be extremely difficult to reverse.

FACT FILE

## DID YOU KNOW?

- Pope Francis was at one time a nightclub bouncer.
- There is a town in Arizona called "Nothing" and has a population of 0. Nothing once contained a gas station and a small convenience store.
- You are more likely to become a famous movie star than win the lottery.
- For a chicken to be considered "free range," it only has to have access to the outdoors for a minimum of five minutes per day.
- McDonald's feeds 68 million people per day, that's about 1% of the world's population.
- In the U.S. it costs an average of $234,000 to raise a child from birth through age 17.
- The U.S. dropped 26,171 bombs in 2016. That's about 3 bombs every hour 24 hours a day.
- To your brain, one sleepless night is the cognitive equivalent of being legally drunk.
- A single Boeing 777 engine delivers twice the horsepower of all the Titanic's steam engines combined
- There are 43 giant sculptures of the heads of former U.S. Presidents rotting away in a Virginian field due to a failed tourist attraction named "President's Park".

"You know what I've been trying lately? Taking pictures of other people!"

© MARK ANDERSON

WWW.ANDERTOONS.COM

## Client Bill of Rights

**You have the right** to understand every aspect of our business policies and support procedures.

We pledge to make it easy for you to communicate with our staff via our website, email, or by phone and to receive answers to any questions you may have about how or why a decision, recommendation or resolution plan is reached.

## Telephone Scammers Get Tricky By Recording "Yes," Using It Against You

What's old is new again.

In the days before the internet, scammers frequently weaponized the telephone, but now, that's considered old school. While telephone scams still exist, they're not nearly as common as they once were.

Recently, however, a new scam has been making the rounds that has even gotten the attention of the FCC. Perhaps the most shocking aspect of this latest scam is its sheer audacity and simplicity. It is stunningly effective. Here's how it works.

You get a call from an unknown number. When you answer, the first thing you hear is a voice asking, "Can you hear me?"

Of course, most people simply say yes. It's practically a programmed response, and that's what the scammers are counting on. That's literally all they need you to say. They record your response so they can use it later, using your recorded "yes" to authorize rogue credit card transactions in your name.

This is an incredibly difficult scam for victims to defend against. Even if you report the transaction as bogus, they have a digital recording of you confirming the transaction, and of course, your voice print is a perfect match. It is, after all, you.

Given that there's no viable defense, the FCC has issued instructions that if you see an incoming call from a number you don't recognize, you should simply let it go to voicemail. The best defense is simply not to place yourself in a position where you might say the wrong thing, and have it be recorded.

A similar recent telephone-based scam sees the scammers offering fake tech support to fix nonexistent problems for a fee.

From the perspective of the scammers, there's almost no way they can lose. These attacks are easy to set up and inexpensive to initiate on a large scale. The bottom line is, don't trust your phone, and don't take calls from numbers you don't recognize.

*Used with permission from Article Aggregator*

## TECH TALK

**Awesome tech you can't buy yet: Airport Jacket – Cargo jacket for Travel.** If you always find yourself forking out for excess baggage every time you take a flight, then an Aussie-based startup has come up with an ingenious solution that'll have you confidently packing the kitchen sink for your next trip. The "Airport Jacket" is, for all intents and purposes, a wearable suitcase. With a whopping 14 pockets and two detachable pocket panels capable of taking up to 15 kgs. (about 33 lbs.) of stuff, your only concern will be ensuring your legs don't give way as you stagger toward the check-in desk. The jacket — with all the stuff inside — can be quickly transformed into a small bag so you only need to put it on when you arrive at the airport. Once you're through check-in and on the plane, you can fold it back up again before throwing it into one of the overhead bins.

*Digital Trends*

**Big Red is still the big dog…but T-Mobile is nipping at its heels.** In the battle to claim best mobile network, the winner is arguable. RootMetrics says it's Verizon. OpenSignal says T-Mobile. Digging into their reports, you'll find that geographical factors determine the winner. OpenSignal's crowdsourced data comes mostly from city dwellers. So their finding that T-Mobile wins most likely applies to urban areas. But that data doesn't apply if you're out in the sticks. RootMetrics reports more on overall coverage, and they find Verizon at the top. So who's got the best network for you? At this point, it boils down to where you live and work. But stay tuned…this race is getting close. *AndroidCentral*

## Contest Corner
### Who Wants To Win A Gift Card?

This month we are giving away a $10 Panera gift card. The winner will be chosen at random from all correct entries received by the 16th.

What late night host was born in Indianapolis?

A) Jay Leno B) David Letterman
C) Johnny Carson D) Conan O'Brien

E-mail **Jeff@bssconsulting.com** with your answers!

Last month's question was: **Jim Davis, the creator of Garfield, was from which Indiana County? The answer was D) Marion.**
***Last month's question contained an error- Jim Davis is from the CITY of Marion which is in Grant County.**

Debby Parisi and Ann Hopkins were drawn as the winners. Congratulations!

Business System Solutions

# Managing Technology For Your Business

BUSINESS SYSTEM SOLUTIONS
1211 Cumberland Avenue
West Lafayette, IN 47906

Phone: (765) 742-3440
Email: bill@bssconsulting.com

**Inside This Issue:**

*For you make me glad by your deeds, Lord ; I sing for joy at what your hands have done. How great are your works, Lord , how profound your thoughts! Psalm 92:4-5*

## From Bill’s Desk

Recently a new strain of ransomware called WannaCry was ripping through the Internet and infecting computers in high-profile organizations. This new ransomware is particularly alarming, as it not only infected the single PC but also EVERY vulnerable PC on the network that PC is connected to!

The WannaCry ransomware exploits a vulnerability in Windows that Microsoft discovered and issued a software patch to correct back in March. However, many organizations apparently still use Windows XP that is vulnerable, and they have not applied it to all their other computers, leaving them vulnerable to being compromised.

BSS has not had any ransomware or viruses in the past 18 months on our managed clients systems. Why? We take proactive steps to ensure their systems are up to date; that old and outdated software is upgraded or replaced; and that best practice security recommendations are implemented.

If you are not currently on one of our managed service plans and would like a **FREE, no obligation Security Audit** to see if your systems are protected, call us NOW at (765) 742-3440 or email me at bill@bssconsulting.com. At no cost or obligation, we’ll send one of our security consultants to your office to conduct a free Security And Backup Audit of your company’s overall network health to review and validate as many as 27 different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We’ll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs.

## Business System Solutions Is Your Total IT Partner

www.bssconsulting.com

***“The Client Relationship Is Priority One”***

## What Our Clients Are Saying

“Not only has BSS met our target objectives, but we have been very pleased with the level and responsiveness of service and attention. Our primary BSS contact Zach has always been very accessible when Nanshan needs arise...day, night, weekends whether it be solving system issues that challenges our production process or providing a quote for new hardware. What resounds with us and has gained our respect is BSS willingness to communicate to us when a request is outside their area of expertise and directing us to alternative resources that are more experienced in the providing the needed solution. BSS demonstrates on a daily basis that the client relationship is priority one.”

NANSHAN

**-Duane Hanni,
ERP Administrator
Nanshan America**