TotalTechCare
TOTAL TECHNOLOGY SUPPORT

TECHMinutes

November 2016

Your Small Business Technology Information Source!

This Issue:

Hackers Scam CEOs for $3 Billion Over the Past 3 Years

4 Ways Outsourcing Your IT Will Revolutionize Operations

Take Commuting Out of the Picture and Watch Productivity Soar!

Shock: One-Third of Businesses Ignore Insider Threats

This Solution Lets You Kick that Bulky File Cabinet to the Curb!

Alert: New ATM Scam Can Steal 32,000 Card Numbers Per Machine

Take Commuting Out of the Picture and Watch Productivity Soar!

Commuting to and from the office is a regular occurrence all over the world. In the United States alone, according to the U.S. Census Bureau, the average commute for the everyday worker is around 25 minutes. Even if this commute is necessary, it could be holding...

Read the Rest Online!
http://bit.ly/2dMzIlP

About Total Tech Care

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
totaltechcare.com

Hackers Scam CEOs for $3 Billion Over the Past 3 Years

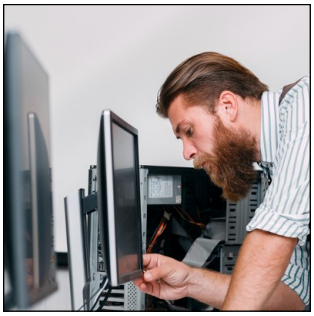
What would you do if a significant sum of money magically disappeared from your account due to a "miscommunication" between accounting and someone pretending to be you? Wire transfers have made it extraordinarily easy for scam artists to make large transactions, which are augmented by the ability to impersonate authority figures within the office; the c-suite staff, also known as management.

This type of CEO fraud is known as a "whaling" scheme. In a sense, it's like a phishing scheme, but on a much larger scale. When it comes to whaling, rather than faking the identity of your IT department or another employee, the hacker goes for the motherload: you, the business owner, or another member of your management staff. This plays to the employee's willingness to comply with your requests and makes it more likely that they'll perform unreasonable tasks, like sending "you" a large wire transfer.

Wire transfers in particular are proving to be a powerful tool for hackers to exploit. ITProPortal reports: "Individuals create bogus messages seemingly from a senior leader, for example, the CEO, which asks employees to wire funds across to them. The messages ultimately trick employees into transferring large amounts of cash electronically." The average value of a wire transfer is $67,000, and according to the FBI, CEO fraud has cost businesses over $3 billion over the past three years alone.

(Continued on page 3)

4 Ways Outsourcing Your IT Will Revolutionize Operations



The traditional break-fix IT model may have worked for businesses years ago, but today it holds them back from fully leveraging their IT to its fullest potential. Managed IT, the superior alternative, aims to take the difficulty out of managing IT so that you can focus on running your business. Here are just a few managed IT services that free up your business in this way.

Cloud Management

The cloud continues to grow more popular as time goes on, mostly due to the overwhelming convenience it offers for small businesses. Your workforce needs agility and constant access to important data and applications, especially if your organization wants to stay competitive in the ever-shifting business environment. This means that you need to provide your employees with the tools they need to stay productive anytime, anywhere. Still, managing a cloud server is far from a simple task, and not one to be taken lightly. When Total Tech Care manages your IT, you can outsource this responsibility to us and take the burden off of your shoulders.

Network Security

Network security requires an intensive knowledge of online threats and vulnerabilities, and as such, you want a seasoned professional handling the security of your systems. It's not enough to equip your business with consumer-grade antivirus and firewall solutions. Instead, you need someone with a thorough knowledge of your organization's potential vulnerabilities, including endpoints, network connections, and software solutions. This type

(Continued on page 2)

4 Ways Outsourcing Your IT Will Revolutionize Operations

(Continued from page 1)

of work is best handled by a third party working behind the scenes to keep your business secure.

Remote Management and Maintenance

Management and maintenance of critical IT systems are often a major pain point for small businesses, as they generally don't have a dedicated in-house IT department to handle this responsibility. More often than not, technology systems needing regular maintenance are left neglected, which can severely cut their lifespans. For example, in order for servers to stay healthy, they need regular maintenance and management. Otherwise, a crippling hardware failure resulting in data loss could happen at any moment. Remote monitoring and maintenance is designed to provide all of your maintenance needs remotely, without the need for expensive on-site visits.

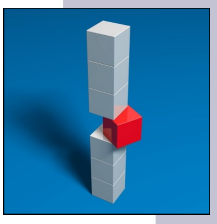
Help Desk Support

One of the most sought-after services is help desk support, especially for SMBs. An outsourced help desk solution provides your team with the support they need to get the most out of their technology. This helps to ensure that your team has the technology assistance they need when they need it. This is especially useful if you already have an internal IT department, allowing them to focus on implementing valuable and innovative solutions designed to improve operations.

So, what are you waiting for? To get started with any of the above-mentioned IT services, reach out to Total Tech Care at 866-348-2602.

Share this Article!
http://bit.ly/2e1VQDQ

Shock: One-Third of Businesses Ignore Insider Threats



Regardless of your security protocol, there will always be threats. One of the most often forgotten outlets for attacks comes from insider threats. Sometimes these threats may be from angry employees wanting to sink your business, but more often than not, those behind insider threats don't have malicious intentions. Still, it's best to cover your bases and ensure that your organization isn't at risk from careless or negligent employees.

Insider threats are categorized as internal threats that are either malicious or negligent in nature, like irate employees, or those who just don't care about security best practices. Regardless of why the insider threat is a threat, you should be aware of these enlightening statistics concerning security and insider threats.

Internal and External Threats: Reality vs Expectations

A study by Accenture and HfS Research claims that 69 percent of organizations have experienced the theft or destruction of data due to internal threats. This is compared to only 57 percent experiencing the same from external threats. These numbers are much different from their expectations, however; only 55 percent expect to become a victim of an internal threat, while 80 percent expect external threats to make trouble. The lesson: be prepared for anything, or you'll be prepared for nothing.

Exposure of Sensitive Data to the End User

The Ponemon Institute issued a study claiming that 62 percent of users felt that they had access to data that they probably didn't need access to. To resolve this problem, employers can implement a user-access control system that restricts access to certain information on a per-user basis. For example, your average employee has no business accessing financial records, salary information, and personally identifiable information (Social Security numbers, birth dates, addresses, etc.).

Reaction Time to Insider Threats

According to Ponemon, the reaction time to insider threats varied. Some organizations responded quickly, while others went months, or even years before finding out:

- Within 24 hours: 24 percent
- Within a week: 19 percent
- Within a month: 14 percent
- Within 6 months: 20 percent
- Within a year: 9 percent
- More than a year: 14 percent

It's a bit surprising that organizations have taken this long to find out about insider threats, but regardless, it's proof that something needs to be done, sooner rather than later. Organizations need to have ways to keep track of who accesses what data, and how their data is handled.

The Ability to Respond to Insider Threats

SANS Institute reports that 31.9 percent of businesses have no way of fighting against insider threats, while 68.1 percent have tools to take the fight to them. It's surprising that the numbers are so low, but perhaps it's because administrators simply aren't aware of the activity themselves.

How Effective Preventative Measures Are

According to SANS Institute, only 9 percent of organizations have techniques proven to prevent insider threats from becoming an issue. 42 percent have the tools, but they aren't used. 36.4 percent are currently implementing processes to mitigate insider threats, while 2.3 percent simply aren't concerned by them...

Read the Rest Online!
http://bit.ly/2dT1qO0

Hackers Scam CEOs for $3 Billion Over the Past 3 Years

(Continued from page 1)

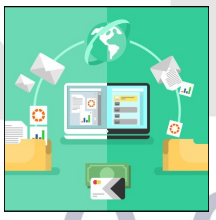
One of the biggest problems with wire transfers is that they are difficult, and often impossible, to challenge. Therefore, your best chance of recovering from a whaling scheme is to avoid getting scammed in the first place, unfortunately. Due to the fact that wire transfers are too fast and finite, you'll want to ensure that your business has practices in place to handle this influx of CEO fraud. A good place to start would be to address how your business handles unsolicited requests for payments or credentials via email, telephone, or otherwise. Here are a few tips and tricks to consider for your business.

- Implement hands-on phishing scam training: If you want someone to learn something, it's best to have them go through the process themselves. This type of hands-on education works well against phishing scams. Engineer a system that roots out those who have subpar reactions to phishing scams, and help them learn how to improve their ability to react to threats.
- Always check in person before sending credentials, or anything else: Emails that request suspicious or sensitive information need to be cross-referenced, either in-person or by checking the email addresses that you have on record. Although, even this might not work at all times, as hackers can potentially spoof email addresses to make their messages appear legitimate. Basically, it's better to just ask whoever supposedly sent the message before responding rashly to a request.
- Educate employees on best practices: We return to the hands-on phishing scam training to emphasize the importance of best practices. Make sure that your team understands how to respond to threats, and regularly quiz them to ensure that they're not going to inadvertently sink your business or cause data loss.

Reach out to us at 866-348-2602!

Share this Article!
http://bit.ly/2e1RCMy

This Solution Lets You Kick that Bulky File Cabinet to the Curb!



Since the late 19th century, office environments have used the filing cabinet to keep records stored in an efficient order. However, today's workplace environment contains more technology than ever before, allowing for more efficient document management solutions. This begs the question, what's better; the traditional file cabinet, or the digital document management solution?

Accessibility and Permissions

A filing cabinet system is a relatively simple invention, and since it's located in the office, the only way to access the files stored within is to physically be in the office. We should also note that nothing is stopping an employee from snooping around and browsing files that they may not be privy to. With traditional file cabinets, the only way to keep employees from browsing files is to lock the drawers or to use a separate cabinet altogether. A security move like this unnecessarily complicates accessing files.

In comparison, a document management solution can be accessed anywhere through the cloud via a secured Internet connection--as long as the user has proper login credentials. This improves worker mobility and eliminates the risk that your employees might lose physical copies of your files. Plus, a document management solution allows you to delegate access on a per-user basis so that your employees can access everything they need to do their jobs, and nothing more. If an employee needs to access something in particular that they don't have permission for, then a quick message to an administrator can resolve this.

Versions of Documents and Searching for Them

A file cabinet can hold a big stack of documents, many of which are probably different versions of the same thing. As years go by, information may change and these documents may require edits, and you can't really throw everything out because information from your older documents may still prove valuable. As you have likely experienced, digging through filing cabinets just to find a specific version of a document is both time-consuming and inefficient, and it only gets worse the longer your business is around.

That is unless you equip your organization with a digital document storage system. A user can easily view the previous versions of a document, so long as the functionality has been built into their solution. Plus, if you misplace a file, all you have to do is use a built-in search feature to locate it.

Disaster Preparedness

This is perhaps the only real advantage that the traditional file storage cabinet might have over document management systems. Say what you will about them, but they are more likely to survive a disaster than an on-site server unit. Of course, nothing can stop the brute force of nature; not even a bulky filing...

Read the Rest Online!
http://bit.ly/2e1Vf56

Alert: New ATM Scam Can Steal 32,000 Card Numbers Per Machine

Banks and companies that manage automated teller machines, better known as ATMs, have been warned against another method thieves have been utilizing to commit identity theft--by no less than the Secret Service.

Machines in Connecticut and Pennsylvania have been found to have periscope skimmer devices attached inside, especially in those machines with openable lids that provide relatively easy access to the inner workings. The device is placed in such a way as to allow the probe of the device to read the magnetic strip on the card as the machine's user makes the mistake of utilizing that particular ATM.

Estimates place the device's battery life at 14 days per charge, with enough storage to collect 32,000 card numbers. Fortunately, the device doesn't seem to collect PIN numbers, but that is also unfortunate, as it indicates that these devices were possibly part of a practice run in preparation for a real robbery.

Despite the apparent lack of a PIN collection device on this version of the periscope skimmers, it is a good habit to cover the entry pad with your free hand as you input your number on most ATM devices, just in case the thieves have placed a hidden camera on the device, or accessed the native camera, which can capture your credentials as you type.

"The best advice to protect yourself from these scams, therefore, is to think a bit like a criminal trying to place a device."

The new use of chip-based cards won't help you much, either, as many ATMs still require the magnetic strip in order to accept the card as legitimate.

Unfortunately, as these skimmers are placed internally, there isn't much of a method of identifying these devices by sight. The best advice to protect yourself from these scams, therefore, is to think a bit like a criminal trying to place a device. Is the ATM in a busy place with lots of potential eyes on it, or is it set aside, secluded and solitary? Is the top accessible, allowing for a cybercriminal to access the machine's inner workings through the lid? Be on the lookout for all of these suspicious traits.

As a precaution, do your best to utilize ATMs in high-traffic areas, with plenty of eyes around as to serve as witnesses for as many hours of the day as possible. Also, avoid ATMs where the body of the machine may be accessed easily, and use those that are embedded in a wall as often as possible. Those well-lit ATMs that are embedded in the walls of banking institutions are the ideal ones to use, as the high surveillance banks utilize will protect the machine (already well-defended on three sides by the building's construction) from tampering, as well as you from a cash-machine mugging attempt. Plus, most ATMs also have a built-in camera.

Of course, if dealing with finances pertaining to your business, it may be most advisable to utilize the tellers that aren't automated, or to handle your banking online behind the online protections that Total Tech Care can put in place for your business...

Read the Rest Online!
http://bit.ly/2dMzL0V

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Robert St. Germain
CEO

Tech Fun Fact
Two-thirds of American Internet users shop online.

Total Tech Care

600 W Prospect RD
STE 2G
Oakland Park, Florida 33309
Voice: 866-348-2602

facebook.totaltechcare.com
twitter.com/totaltechcare
newsletter@totaltechcare.com

Visit us **online** at:
totaltechcare.com