DTS DanTech Services
Computers under control!™

Technology Times March 2021 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problem? - Click Here!

Fraud is on the Rise: How to Protect Your Small Business

After a year of tremendous challenges, small businesses are optimistic about their ability to bounce back and grow in 2021, according to a Capital One Small Business Confidence survey. While most of 2020 was focused on the global pandemic 2020 and the hope for economic relief, businesses need to ensure that they are protecting themselves from additional risks, namely fraud. In a recent survey conducted by the Association of Certified Fraud Examiners (ACFE), 90% of respondents say they expect fraud to increase over the next 12 months.

It could be a fake message claiming your small business trademarks are expiring, or "customers" start requesting bogus chargebacks from credit card companies. It might even be employees committing internal fraud. Whatever the case, small businesses are easy targets for criminals who believe smaller companies don't have the proper preventative policies in place to recognize fraud.

If you are the victim of a fraud scam, it's essential to immediately report the incident to the Federal Trade Commission (FTC). To make reporting easier for small business owners, the FTC just updated ReportFraud.ftc.gov, its consumer reporting website, to include small business reporting.

However, fighting fraud needs a proactive approach. Here are three common types of fraud and how to protect your small business from falling victim to them.

- Continued on page 3

Connecting the Pandemic Dots

One of the many affects that are the result of the pandemic, such as work from home, and shifts in business processes, are the effects on real estate, office space, and leases. I'd like to take this time to point out some considerations when it comes to moving your offices to a new location—either now or in the future.

Finding the right space can be challenging and rewarding. Maybe you've eyed a space that is "perfect" yet was unavailable until recently. The location is great, the rates are good, and it appears to make good business sense to make the change. What could go wrong? From a technology point of view, plenty.

Prior planning can prevent problems. Two months prior to any move, make sure that you've talked to the companies that deliver Internet services in your area. Can they deliver to your new space? What about your phone service? Is it time to consider an upgrade to a more modern phone service? What upgrades/downgrades or modifications are needed? Two months is the minimum amount of time to consider these items or to order service.

Does your new space have the network infrastructure your business needs? How many network drops are at each work area? Are you considering the use of old network cabling? Do you know what it's rated? Does it need to be replaced? If so, who's responsible to remove the old cabling and installation of the new? What standard will be used? As you can see, I've listed just a few questions that must be considered. Yet these are generalities that provide a starting point as my crystal ball isn't clear enough to see into your exact needs, some of which may require the moving of servers and other equipment that requires special handling!

Dan Foote

Why, Why Not, Why Don't We Try

by Robert Stevenson

Nobel Laureate and physicist Richard Feynman said that it was no coincidence that virtually all major discoveries in physics were made by those under the age of 25. When he was asked why he concluded, … "you don't know what you don't know." I guess another way you could put it is, when you are unaware of something that supposedly can't be done … you go at it with a blind determination to see if it CAN be done.

Any time I do a strategic planning session for a company, I always ask them to make sure they have some of their younger talents in the room. If you want fresh, new ideas, I think it is only appropriate to have fresh, new, young employees in the room sharing their ideas. You won't hear statements from them like, "that's the way we've always done it," because they've never done it. What you will hear are challenging statements like, "Why,"… or…"Why not,"…or…"Why don't we try".

I am not saying that the veterans in a company should be "put out to pasture" when it comes to coming up with ideas that will improve it. I think experience is an incredibly powerful resource. Intellectual capital is one of the most valuable assets of any company. What I am saying is don't discount an idea from a young associate by saying…"What could they know … they are too young to know anything … they haven't been here long enough to know how we do it at our company."

In the mid 1800's the head of the Patent Office in Washington recommended that the Patent Office be closed, because everything that could have been invented had already been invented. That same Patent Office rejected the patent applied for by the Wright Brothers for their flying machine, stating they believed machines that were heavier than air could not fly; someone forgot to tell the Wright Brothers. They just kept asking themselves…"Why"…"Why not,"…"Why don't we try", and aren't we glad they did.

Our young ones have grown up in a world of speed, multi-tasking, constantly changing technology where virtually anything is accessible through the Internet. I don't care what they don't know … I want to hear what they want to change, don't like, think is stupid or is a waste of time. If you want to be successful … then stay curious and keep asking WHY, WHY NOT, WHY DON'T WE TRY.

NEED REMOTE IT SUPPORT AT YOUR HOME? Call us about our residential service offering. **907-885-0500**

Shiny New Gadget Of The Month:

The Sony SRS-RA5000 Wireless Speaker Offers Immersive Audio

The Sony SRS-RA5000 wireless speaker is a powerful audio solution for users who are in need of a way to enjoy their favorite music or content at their leisure. The speaker will deliver ambient room-filling sound thanks to the brand's proprietary 360 Reality Audio and Immersive Audio Enhancement that will diffuse sound waves both horizontally as well as vertically.

The unit will also calibrate according to the environment that it's in thanks to an internal microphone, while the auto volume functionality will adjust the audio of each song to balance them out.

With a total of seven driver units, you'll hear the difference. A trio of up-firing speakers spreads music vertically while three side speakers spread sound horizontally. These are complemented by a woofer, which floods the room with rich, deep bass. The Sony SRS-RA5000 wireless speaker also provides access to the Google Assistant and Amazon Alexa voice assistants, and is also compatible for use with Bravia TVs.

"Fraud is on the Rise"
- Continued from Page 1

1. Cyberfraud

For any business with online activity, a cybersecurity plan is crucial to establish and follow. According to the Federal Communications Commission (FCC), digital information theft has become the most commonly reported fraud, exceeding physical theft. When you create your cybersecurity strategy, the FCC recommends you follow these tips:

- Train your employees. Establish basic security procedures for employees, including using strong passwords, protecting customer data and other vital information.
- Update all devices to the latest security software, web browsers, and operating systems. Use antivirus software and firewalls.
- With so many employees now working remotely, create a mobile device action plan to encrypt data. Also, make sure each employee has a separate user account, so you or your accountant can trace any activity if there's a problem.
- Back up critical business data and store the information in the cloud.
- Secure Wi-Fi networks with Service Set Identifier (SSID) and password protection.
- Work with banks or credit card processors to safeguard payment information.

2. Payment and Banking Fraud

Payment fraud is characterized in several ways, such as bounced checks, unauthorized transactions, lost or stolen stock, and fake requests for refunds/returns. Most hackers target credit card users and credit card merchant accounts using stolen card numbers. To prevent payment fraud, make sure you are aware of the newest fraud trends, encrypt payment transactions, and partner with a secure payment processor, such as Bill.com.

They will never ask you to provide credit card or ACH information in an email or over the phone and won't ever send ZIP or EXE attachments (many of these attachments contain viruses).

Plus, your online bank account is at risk for accounting fraud, so limit how and with who you share confidential banking information. A payment solution like Bill.com protects your banking information by allowing payment without ever accessing the online banking account. Bill.com builds in user-based permissions, which means you can control what employees can see.

3. Employee Embezzlement

Unfortunately, employee fraud is a very real and costly risk for small businesses—especially in a struggling economy. To prevent employee fraud, check out these tips from Bill.com:

- **Go paperless.** Paper invoices and checks are a security risk. Going digital reduces the chance of thieving hands having access to the information, and you, your accounting department, or your accountant can easily track every transaction.
- **Enforce payment controls.** You can enable fraud preventive accounting controls and authorization limitations by using digital solutions.
- **Automate work processes.** By computerizing reminders and creating an audit trail, you ensure that nothing falls through the cracks.
- **Eliminate checks (incoming and outgoing).** Paper checks contain confidential information that cybercrooks can use to access your business's financial information or accounts. When you receive and make payments electronically, you shield these numbers from unauthorized people.
- **Increase the number of regular internal audits you conduct.** Automated digital systems create an easy-to-trace audit trail.

How to Stop Sending Angry Emails

"You've got to be kidding me." I'd just received an email. A client was looking for a strategy document that I hadn't even started yet. (We had never finalized a deadline and we obviously had different ideas of how high a priority this was.) It had been a busy month...and I was feeling a little overwhelmed. Now, I was getting a request from a client...on the weekend.

I started drafting a response: Hey Jason, we never set a deadline on this and I've been swamped. I haven't even started on this document yet. You see… I decided to stop before sending the reply. Sending this will be a huge mistake, I thought. What if you were the one receiving this message. What would you think? Probably that you contracted the wrong person. The thing was, I really loved this client, and this project. I had gotten through the rough period, and now I was ready to focus. So, I rewrote the draft: Hey Jason, thanks for your message. I'm on this. Should have a draft to you within 48 hours. Look forward to discussing.

The result? - Jason responded with a thumbs up, and the project moved forward without worry. Everybody's happy. So, how can you make sure to get your emotions under control and avoid sending angry emails? **Follow the 3-step process.**

The three-step process is rooted in emotional intelligence, the ability to understand and manage emotions. When you get an email that inspires anger, frustration, anxiety, or similar feelings, do the following:

1. Don't respond right away. Depending on the subject, a few minutes pause may be enough...But if you're really riled up, it may be good to wait 24 hours.

2. Write a draft. Your first draft will be emotional...But writing something down right away can help you clarify your own thoughts and feelings. Giving yourself the chance to vent--to yourself--can also help relieve stress.

3. After waiting, review and revise. Again, 24 hours is ideal...but if that's not possible, just give it as much time as you can. Then, thinking of your audience, ask yourself:

Is there anything that could be misinterpreted, or that sounds angry, desperate, or emotional? Is the message confusing? Will it raise more questions than it will answer?
Is there anything unnecessary I can remove from this message? Would it be better to communicate this by phone (or in person)? Revise as necessary. This may seem like a lot at first, but do it enough and it becomes second nature.

5 of the Biggest Computer Hacks in History

1. Operation Shady RAT

A computer programmer based in the People's Republic of China is assumed to be responsible for these continuing cyber attacks that first began in 2006. Named for its utilization of remote access tools that allows computers to be remotely controlled from anywhere in the world, this hacker has succeeded in stealing the intellectual property from at least 70 public and private organizations across 14 countries. Those victimized include the United Nations, multiple defense contractors, worldwide businesses, the World Anti-Doping Agency and the International Olympic Committee.

2. Department Of Defense Hack

Those who yearn for a security position at the Department of Defense will definitely have their work cut out for them. Wanna-be hackers attempt to attack its security system on a regular basis, and a teenager from Florida managed to compromise the military's computer system way back in 1999. By installing backdoor software into the computer system of the Defense Threat Reduction Agency, Jonathan James was able to intercept highly classified emails. These included information about the life support code for the International Space Station and many other important matters.

3. Melissa Virus

Perhaps the first major computer virus that made the world's population realize that their computers weren't always safe, Melissa was created in 1999 by a New Jersey programmer with too much idle time on his hands. David L. Smith disguised his virus as a simple Microsoft Word program, and he sent it to countless unsuspecting recipients. It then resent itself to the first 50 people from each infected computer's address book. Before long, Melissa had compromised a full 20 percent of the world's computers, and big companies like Intel and Microsoft were forced to shut down all outgoing mail programs until the problem could be solved.

4. Comodo Hack

Everyone who uses a computer is familiar with those reassuring security certificates that let you know that you've arrived at a secure site, but they aren't always what they seem. Comodo, a company that provides those certificates, was hacked in 2011 by an Iranian programmer who was then able to create fake security certificates that led people to believe that they were actually logging into Yahoo or Google. This allowed the hacker to eavesdrop on any e-mail that was sent from these services and gain personal information.

5. Play Station Network Hack

This particular hack clearly demonstrates that more than just computers are at risk of being compromised. In 2011, a hacker accessed the Play Station Network system, which resulted in the loss of data and personal information for some 77 million users. The company had to shut down for 20 days and lost an estimated $171 million.