DTS DanTech Services
Computers under control!™

Technology Times December 2016 Issue

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

What's Inside:

$1.5M Cyber-Heist Typifies Growing Threat

Efficient Escrow of California was forced to close its doors and lay off its entire staff when cybercriminals nabbed $1.5 million from its bank account. The thieves gained access to the escrow company's bank data using a form of "Trojan horse" malware.

Once the hackers broke in, they wired $432,215 from the firm's bank to an account in Moscow. That was followed by two more transfers totaling $1.1 million, this time to banks in Heilongjiang Province in China, near the Russian border.

The company recovered the first transfer, but not the next two. They were shocked to discover that, unlike with consumer accounts, banks are under no obligation to recoup losses in a cybertheft against a commercial account. That meant a loss of $1.1 million, in a year when they expected to clear less than half that. Unable to replace the funds, they were shut down by state regulators just three days after reporting the loss.

Net result? The two brothers who owned the firm lost their nine-person staff and faced mounting attorneys' fees nearing the total amount of the funds recovered, with no immediate way to return their customers' money.

Avoid Getting Blindsided

While hacks against the big boys like Target, Home Depot and Sony get more than their share of public attention, cyber-attacks on small and medium-sized companies often go unreported, and rarely make national headlines.

Don't let this lull you into a false sense of security. The number of crippling attacks against everyday businesses is growing. Cybersecurity company Symantec reports, for example, that 52.4% of "phishing" attacks last December were against SMEs – with a massive spike in November. Here are just a few examples out of thousands that you'll probably never hear about:

- Green Ford Sales, a car dealership in Kansas, lost $23,000 when hackers broke into their network and swiped bank account info. They added nine fake employees to the company payroll in less than 24 hours and paid them a total of $63,000 before the company caught on. Only some of the transfers could be canceled in time.

- Wright Hotels, a real estate development firm, had $1 million drained from their bank account after thieves gained access to a company e-mail account. Information gleaned from e-mails allowed the thieves to impersonate the owner and convince the bookkeeper to wire money to an account in China.

- Continued on page 4

Business Briefings:

"Smart Cities" are adding a whole new layer of complexity to data protection. Driverless cars, cloud-based services and networks of sensors are driving rapid change… Yet along with great benefits, the smart city revolution adds new threats. For instance, since it relies heavily on interconnectivity, weak links make the whole system vulnerable to cyber-attack. Yet a study by Kaspersky Labs estimates that 57% of smaller companies underinvest in security. With deeper connectivity to these "weak links," encryption of your own data becomes more critical than ever. Using secured websites (the "https" vs. "http" protocol), for example, not only secures data, it also creates trust among your customers and vendors. Clearly, the smart thing to do is to be ready for smart city challenges. *HarvardKennedySchoolReview.com*

Stop wasting your time and costing your company money. No company is 100% productive 100% of the time. But talk of last night's game, social media check-ins and long lunch breaks aren't the only time thieves. Without realizing it, you may be asking your team to do things that frankly hurt the bottom line. For instance, do you hold meetings that take longer than necessary – or don't need to be held at all? Consider holding meetings only when critical. And when they are, use an agenda to keep everyone on track. Another big time killer is trying to fix a problem via multiple e-mails or chat. Often a simple phone call could resolve the issue with a lot less back and forth. *Entrepreneur.com*

Want better collaboration at work? Play these tunes. Research has already shown that teams who listen to music together at work feel more bonded and collaborate better. Yet that begs the question – what type of music do you listen to? It's a topic likely to end up in wrangling and conflict. However, a recent study at Cornell University offers a scientific answer. And, while metal fans may not be thrilled with it, the results weren't exactly shocking. The study found that people who listen to happy music were more likely to cooperate, regardless of age, gender or academic major, than those who listen to unhappy music. Interestingly, they found it was not the vibe, but the bouncing beat, that gets teams in sync. Inc.com

At the Office: Be the Adult in the Room

By Andy Bailey

There's a reason people refer to the office as a "sandbox," because some folks refuse to act like adults. And, if the level of childish behavior rises to tantrum pitch and the culture becomes toxic, there's no chance for communication or growth. But the office is not a playground, and we're not children. So it's important that we enter into an "adult agreement" when we walk through the doors at work and begin our day.

When I work with companies looking to improve their business, one of the things we start with is our adult agreement. It informs the work we do for the entire day, and hopefully beyond.

Here are three agreements to make sure you're acting your age in the workplace:

Don't shoot each other down.
When a colleague brings an idea to the table – even if you disagree with it – don't shut them down just to be "right." If we want to be collaborative, we've got to consider that those around us have something valuable to offer. If you make it a habit to cut people off or discount what they're saying out of hand, you'll not only guarantee that they won't share their ideas with you again, but you'll likely miss out on insights that could help you and your company.

Own up to mistakes and bring them to the table.
Nobody is perfect – not you, not me, not Bill Gates or Mark Cuban or anyone you might admire in business. We all make mistakes, and the worst thing we can do is deny that they exist. Instead, own up to your mistakes and let everybody know what they are. We only grow and learn when we're vulnerable with each other. Admitting error is often considered a risk, but it's really an opportunity. Our mistakes let others understand who we are, what risks we're willing to take and what lessons we've had to learn. Share freely to engender trust and understanding among your teammates.

Don't hide problems.
Maybe you want to stay focused on the positive and don't want to highlight "problems." Wrong. You're not a negative person just because you bring problems to light or point out conflicts where they might exist. More likely, you're finally saying what everyone else is thinking and is afraid to say. Or you're bringing something up that's important for everyone to understand in order to improve and move forward. Put problems up for discussion and brainstorm solutions. Hiding problems only makes them grow.

As you seek to master these three steps, remember one more thing: adults don't crush each other just for acting like adults. We've got to support each other in our efforts to be truthful and vulnerable. A team is only as strong as its weakest link, so it's critical that we lift each other up.

When we act like adults – especially in the sandbox – we all win.

Mobile Users Running Old IOS Versions Vulnerable To Fake Apps.

Back in the good ol' days before the rise of the iPhone, Apple devices were largely considered to be more secure than their Wintel counterparts. There was a time when Apple used this as a major plank in their marketing efforts. These days, it is increasingly clear that that's no longer the case.

A recent TrendMicro survey of Apple Apps offered by third party marketplaces has discovered that the ecosystem is infested with a variety of malware.

The most common method of infection is spoofing Bundle IDs. Hackers can make fake copies of popular apps, inject whatever malicious code they want, give them a Bundle ID that will pass iOS inspection, and ride the wave of app popularity to get downloads and installs.

Fortunately, anyone running iOS 10 is safe from this type of attack. The problem, of course, is that not everyone is running the latest version of the OS.

This presents enormous challenges for small to medium sized business owners, especially if your company has a BYOD policy. It's all too easy to envision a scenario in which a poisoned app on one of your employees' devices proves to be the back door that allows a hacker access to your company's data.

With proper security protocols in place, the risk of such an occurrence can be minimized, but it can never be completely eliminated.

What's the current state of your digital security and your policy on employee devices? If you're worried that either (or both) might need to be shored up, but aren't sure how to proceed, give us a call at 907-885-0500. One of our talented team members will be happy to work with you to assess your current situation. We can work with you to design a more robust and security digital security system that minimizes your risks.

The **DanTech Services Team** wishes you & your team all our best for this **Christmas and New Year !**

Let us quote one person who knew a couple of things about life:

"Learn from yesterday, live for today, hope for tomorrow" - Albert Einstein

Have a great celebration!

AND

KEEP YOUR COMPUTERS UNDER CONTROL!™

Shiny New Gadget Of The Month:

Your Desk Is Killing You: Do This Instead

The evidence is piling up that sitting all day is bad for your health. Though not perfect, Varidesk offers a compelling solution.

On the plus side, The Varidesk sets up right out of the box – no assembly required. With its weight-balancing system, you don't need any hardware to fasten it to your desk. And it features an attractive, sturdy design. You can lean on it and your monitor won't go crashing to the floor. Springs and levers make it easy to raise or lower it to one of 11 preset levels.

The main flaw is that when you raise it, it also moves forward – a problem if you're in a tight space. All in all, though, it's worth looking at, especially if you have a wireless keyboard and mouse – and enough space in your office or cubicle to back up a bit.

DanTech Services provides knowledgeable management, support & sales of SonicWALL UTM's.
Whether you're upgrading or replacing your current firewall, DanTech Services has the experience to size, deliver and install the best perimeter protection available.

"$1.5M Cyber-Heist Typifies Growing Threat"
- Continued from page 1

- Maine-based PATCO Construction lost $588,000 in a Trojan horse cyber-heist. They managed to reclaim some of it, but that was offset by interest on thousands of dollars in overdraft loans from their bank.

Why You're A Target – And How To Fight Back!
Increasingly, cyberthieves view SMEs like yours and mine as easy "soft targets." That's because all too often we have:

1. Bank accounts with thousands of dollars.
2. A false sense of security about not being targeted.
3. Our customers' credit card information, social security numbers and other vital data that hackers can easily sell on the black market.

If you don't want your company to become yet another statistic in today's cyberwar against smaller companies, and your business doesn't currently have a "bullet-proof" security shield, **you MUST take action without delay – or put everything you've worked for at risk. The choice is yours.**

Here are three things you can do right away:

1. Remove software that you don't need from any systems linked to your bank account.
2. Make sure everyone with a device in your network NEVER opens an attachment in an unexpected e-mail.
3. Require two people to sign off on every transaction.

Let Us Help
When it comes to defending your data, whether it's bank account information, customer and employee records or proprietary intellectual property or processes, Do NOT take chances.

We are offering our ***Cyber Security Assessment*** **at no cost** through the end of December to 10 companies in the Anchorage area. **Call us at 907-885-0500 or e-mail at info@dantechservices.com TODAY** because we can only offer this valuable service to the first 5 companies that apply.