DTS DanTech Services
Computers under control!™
Technology Times October 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:

Stop losing money on email spam, get your email protected with Expanded Email Services & Capabilities

DanTech Services has partnered with **MailProtector** to provide our Customer's with an expanded set of email services. While **MailStop** has been effective, we've been looking for solutions that allow us to provide a better array of services that will provide your business with expanded options, which can be chosen a la carte or bundled.

MailProtector's CloudFilter will be our **MailStop** replacement. Our test drive of **CloudFilter** has found it to be very effective, with better reporting. It effectively stops spam, viruses, & malware in the cloud. Suspicious messages are held in quarantine for review, while good email is delivered to the end user. If you currently are filtered through **MailStop**, your service will be migrated to **CloudFilter**. To help eliminate confusion, digest & quarantine emails will still use the **DTS MailStop** branding.

SafeSend provides enhanced outbound scanning. It will stop bad email from leaving your organization while staying compliant. When your email users send out confidential files or messages caught as spam, it can severely damage the reputation of your business.

XtraMail provides email continuity with a web-based platform that stores a rolling 30 day backup of all your email, so when your systems are down, your users can simply login to XtraMail to continue sending & receiving email.

Email Archiving will be replaced with **SecureStore**. There are no storage or retention limits! An archived copy of all incoming, outgoing, and internal email. Users can access their archive anytime to search and send stored mail via the secure and fast web console. If your business is subject to certain compliance regulations, **SecureStore** provides a protection point that allows users to delete local emails yet giving management the knowledge that emails are protected in the archive.

Health care, legal, and other professionals that need to send, receive & track confidential email can use **ForcEncrypt. ForcEncrypt** makes email encryption easy and allows encrypted emails to be sent anytime, anywhere on any device.

For email hosting services, we can now introduce our two new platforms: **CloudMail**, a secure hosted email platform, and **Exchange+**, our secure hosted Microsoft Exchange platform.

CloudMail provides an affordable, robust email hosting platform which includes contacts & calendars, a large mailbox, & access from anywhere through the secure webmail console or an email client, such as Thunderbird or Outlook, using POP3 or IMAP.

- *Continued on page 4*

Business Briefings:

Savvy users are capitalizing on the LinkedIn–Microsoft merger. Here are three ways you too can profit: 1) Your profile photo now appears on both platforms. Run it by photofeeler.com to make sure it's up to snuff. 2) When it comes to updates, forget text – video rules. Check your newsfeed and you'll see how LinkedIn puts video on top and is burying articles. No wonder members have seen a 60% to 90% drop in readership. To get attention, go video. 3) Keep an eye on LinkedIn's social advertising. With access to user data from both platforms, your ads could now enjoy a wider audience of both LinkedIn and Microsoft users. This merger opens new doors for users. Now's the time to capitalize on it. Entrepreneur

A wafer-thin laptop so light you'll forget it's in your briefcase… Want an ultrasleek machine with enough battery life to keep you going long hours without plugging in? A new breed of ultraportables" offers that and more. The lightning-quick storage on these units lets you resume work in seconds, even after they've been idle or asleep for days. The "best in breed" will cost you a pretty penny. But if you're willing to spend a little, you can get premium features. Touch screens, full HDMI ports and eight hours or more of battery life are not uncommon. At the top end, you can expect a high-resolution 4K screen (3840 x 2160). Be extra-nice and Santa might even slip one in your stocking! PCmag.com.

Considering Facebook Live Video for your business? Using Facebook Live is very simple. If you haven't already, install the Facebook app on your smartphone. Open it up, tap the red "Go Live" icon and you're on. It tells you how many are watching, plus their names and comments. When you're done, it saves to your Timeline. And, unlike Snapchat or Periscope, it doesn't disappear after just 24 hours. You can share, embed, Tweet – or delete – to your heart's content. And you can filter who sees it. As for content? Interview key employees, big shots in your niche or your customers. Share how you're making a new product. Why do it? Your customers love getting that little peek "behind the scenes." PostPlanner.com

Dealing With The Dark Side of Social Media

By Mark Sanborn

Social media has become a true amplifier, permeating every nook and cranny of the web, giving a megaphone to those who might have previously found themselves voiceless.

While I generally believe that the proliferation of the social web is a good thing, it does have a dark side that is difficult, if not impossible, to ignore.

I was reminded of this recently when an unscrupulous competitor accused me and my friend Larry Winget of an ugly racial slur. While it was totally fabricated, this person willfully resorted to defamation of character to defend his indefensible behavior.

It's easy to get mad, get on your computer and allow emotions to run amok. And that can come back to bite you. Yet there are times you shouldn't acquiesce to digital bullies. You need to take a stand.

Here are a few tips on how to keep your social media actions in check, and how to react to others who just can't seem to control theirs:

How do I think through my social media actions in a heated moment?

If you wouldn't say it to your grandmother, don't write it on Twitter. It feels good to blast an opponent, but such outbursts can easily be used against you.

Remember that everything you say or do on the web is archived. Consider everything you write on the Internet to be permanent. Trolls may delete their comments, but they still leave a trail.

Still debating saying it? Sleep on it. If you really feel the need to say something that might be taken the wrong way, consider sitting on it overnight. Waiting until the next day will rarely hurt your point, and it may save huge amounts of embarrassment.

If you do say it…make sure you feel you could defend it in a court of law. Falsely accusing someone of something is a big deal, and the repercussions could amplify beyond your original intentions.

How do I react when I am targeted on social media?

Grab screenshots. If someone truly is going after you, the first move is to gather evidence. Make sure you have copies. Odds are that they will quickly realize what they have done and will try to erase their trail, so the best thing you can do is make sure you have a copy on hand.

Report them. Twitter, LinkedIn, Facebook and most other platforms have guards against those who harass others. Don't hesitate to put in a report – that's why those guards are there!

Remember that the truth is your best defense. As someone who has been egregiously accused of something I did not do, I took solace in the fact that I was innocent, and as such the accusation cruelly asserted could never be proven.

We live in a world where unscrupulous people have migrated to online communities and live among the rest of us. I hope you never have to use the above actions, but when you do, I hope they serve you well.

iOS Users: Apple Says Update Immediately

There is a large and growing body of evidence that hackers and their attacks are increasing in sophistication. Hardly a month goes by that there isn't a headline somewhere in the world about a new attack vector. The level of innovation and cunning is staggering.

Apple used to be largely immune to such attacks, a fact brought about by virtue of a greater emphasis on security, and because Apple's share of the desktop and laptop market was quite small, and generally seen as not worth going after on a large scale. There were bigger, easier targets.

That changed with the release of the iPhone, and suddenly Apple found itself increasingly targeted by hackers from around the world.

Recently, an exotic, highly complex chained attack was uncovered that relies on a trio of "zero day exploits," which are as bad as they come. Note that these attacks were found being used in the wild, so this is not some theoretical musing about what could happen. It's an attack that has already occurred.

The attack is not something that a casual hacker could pull off, which means that there isn't a huge number of people who could do it, but the fact that it happened at all sent Apple scrambling to release an emergency patch that addressed all three zero day vulnerabilities found.

The attack works like this:

A link (URL) is sent to the user via SMS. This link opens a web page which loads JavaScript, and executes a binary inside the Safari web browser.

This leads to the second event in the zero day chain, where another exploit allows it to bypass KASLR protections that would normally prevent malware from identifying where the core of the OS is found in memory.

Armed with this information, the third exploit in the chain kicks off, which corrupts the memory in the kernel. This incapacitates iOS, leaving it incapable of blocking software from running that hasn't been signed by Apple. From here, the hacker has unfettered access to the phone.

All that is to say if you're running a version of iOS older than 9.3.5, patch it immediately, or risk losing control of your device.

Could One Tiny Leak Wipe Out Your Company?

Things were going great at Michael Daugherty's up-and-coming $4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network. A hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

Have you developed a false sense of security? Please, please, please do NOT think you are immune to a cyber-attack simply because you are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers.

- *Continued on page 4*

Shiny New Gadget Of The Month:

HoloLens: Your New Reality?

A game designer sees a moving 3-D image of a living, breathing, mace-wielding ogre – on her desk. She flicks a finger and he turns from side to side, giving her a full view of his outfit and weapons belt.

An architect looks up at the ceiling in a building he's just designed. He waves his hand and reshapes it, allowing more light through. All virtually.

A space scientist designing a Mars rover strolls through the landscape, noting from all sides the position, shape and size of rocks his vehicle must navigate.

Now it's your turn. Put on the new HoloLens by Microsoft, and what do you see? How could you use this cool new augmented reality (AR) tool in your business?

At $3,000 for the developer's version, it may not be an impulse buy. But new AR tools like this will soon be part of your computing world.

"Could One Tiny Leak Wipe Out Your Company?"
- Continued from page 3

A simple client profile with name, address and phone number sells for as little as $1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – $300 per record is not uncommon. Being small doesn't mean you are immune.

Are you skimping on security to save money? Sure, of course you have a tight budget… So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your network. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

Could lack of an off-boarding process put your company at risk? It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet? The greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Don't let a tiny leak sink your ship – here's what to do next… Let us run our complete Network Security Audit for you. We'll send our top data security specialist to your location and give you a complete top-to-bottom security analysis with action plan. This is normally a $297 service. **It's yours FREE when you call now through the end of October. Don't wait until disaster strikes. Call 907-885-0500 or e-mail us at info@dantechservices.com to schedule your FREE Network Security Audit TODAY.**

- "Expanded Email Services & Capabilities"
continued from page 1

Exchange+ uses Microsoft Exchange 2016 to deliver the ultimate hosted email solution. Combined with layers of security & compliance services, plus the collaboration tools that Microsoft Exchange offers, **Exchange+** provides users with form, function and the business standard for email delivery.

What this means to you: Looking forward, as I noted above, if you currently use either DanTech Services MailStop or our hosted email service, we will be migrating you to our new platform. At a minimum, all MailStop filtering will be done by **CloudFilter** and hosted email will be migrated to **CloudMail**.

If you're interested in learning more about these offerings, please let us know. An email to info@dantechservices.com is the best way to get the conversation started. Hosted solutions are cost effective, especially when it comes to replacing a server that requires upgrading AND runs MS Exchange.