Technology Times

ProComputer Solutions

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

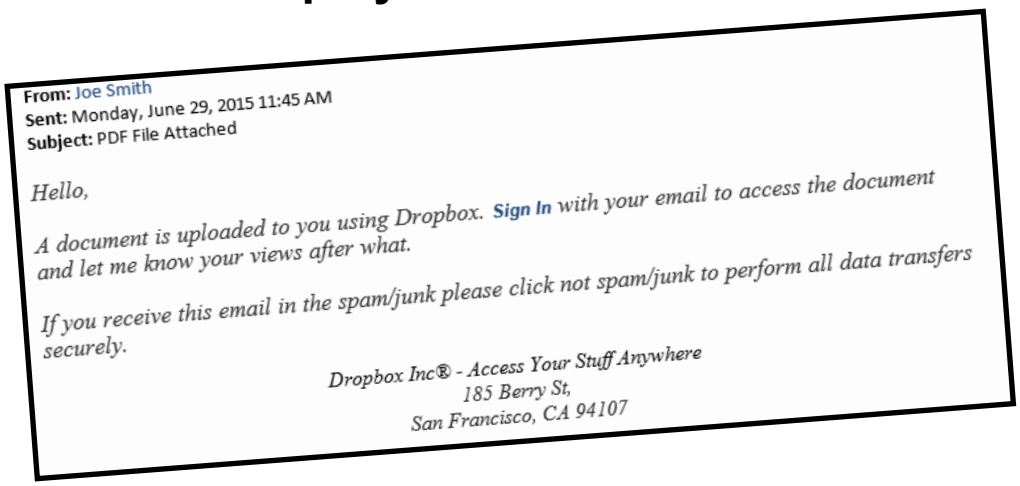
July 2015

"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!"

David Downs, Owner
Pro Computer Solutions

Inside This Issue...

SECURITY ALERT!! This Email Virus will do BIG DAMAGE if you or your employees click on it!



From: Joe Smith
Sent: Monday, June 29, 2015 11:45 AM
Subject: PDF File Attached

Hello,

A document is uploaded to you using Dropbox. **Sign In** *with your email to access the document and let me know your views after what.*

If you receive this email in the spam/junk please click not spam/junk to perform all data transfers securely.

Dropbox Inc® - Access Your Stuff Anywhere
185 Berry St,
San Francisco, CA 94107

Please take a careful look at this email. Not one but **two** of our clients received this last month. Looks pretty legitimate, right? **It's not!** If the recipient of this email clicks that embedded "Sign In" link, an old but particularly nasty computer virus will INSTANTLY lock every data file that the recipient has access to, whether that is on her computer or in your company's computer network. You will be instantly stopped dead in your tracks, unable to work until the files can be restored. This is a tedious process, and some files may be permanently lost.

Once locked by this nasty virus, you must find a professional consultant to help you eliminate it from your company's computer network and (hopefully) recover your back-up files *(Note: this is another GREAT example for why it is so incredibly important for every business owner to develop a back-up and disaster recovery plan for your company's computer network!)*

Keep in mind, the sender of this email was a business associate to the receiver. In fact, unbeknownst to the sender, copies of this email went to every single contact in his mailbox. It just as easily could have been received by you or one of your employees. Would you have clicked the "Sign In" link in this email from your close business associate? Would your employees at every level in your company know not to click that link?

One tell-tale sign that the receiver could have looked at to help determine if this is a legitimate email is to hover over the link without clicking it. The link destination name will pop up to show you what web address the link points to. In the case of our clients, the destination link pointed to an unfamiliar web address. The word "dropbox" did appear in the url, however it was not www.dropbox.com (which would have been the only acceptable destination in this case.)

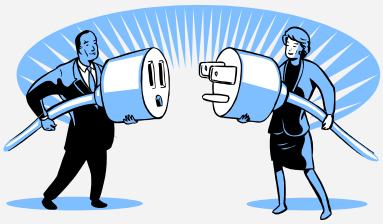
There is a lot that we can do to help protect you and your company's computer network from the inevitable damage that is inflicted when you receive an attack like this. My staff and I are always happy to talk with you about what we can do to ensure you have the appropriate level of protection you need for your company's computer network.

Cheers!

David Downs

Get More Free Tips, Tools, and Services: **www.procomputersolutions.com.**

Refer Us And Receive Up To $75!



Connect Us With A Friend In Need And Reap Rewards For Yourself!

- Send in your referral information by either calling our office at **816-229-2290**, emailing us at **referral@pcsiweb.com**, or visiting our page, **www.pcsiweb.com/referral**.
- We will pay you $25 for anyone that you refer to us with whom we get an appointment.
- If your referral becomes a client, we will pay you an additional $50 AND we will give your referral $100 off their purchase.
- So, if you have a friend or an associate in need, please contact us and we will reach out to them. Doesn't everyone deserve worry-free IT?

The 5 Most Dangerous Pieces Of Information To Give In An E-mail

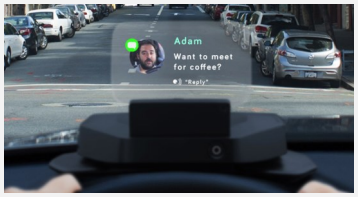
In the book *Spam Nation*, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. **Your social security number.** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.
2. **Banking information.** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.
3. **Your credit and/or debit card information.** NEVER update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do NOT click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating VERY legit-looking e-mails designed to fool you into logging in to their spoof site, which LOOKS very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply CALL the vendor direct.
4. **Login credentials and passwords.** You should never share your passwords or answers to security questions with anyone for any site, period.
5. **Financial documents.** An ATTACHMENT that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!

Shiny New Gadget Of The Month



Navdy

Many of us realize how dangerous it is to check e-mail or text messages while we're driving, but we don't feel like we can afford to ignore our phone. Brand-new product Navdy to the rescue!

Navdy is a transparent Head-Up Display (HUD) that projects information as if it's floating six feet in front of you. It's very similar to what commercial airline pilots use. Navdy works with any car, and with all iPhones and Androids.

Using the apps you already have on your phone, and with no service plans required, Navdy allows you to focus on the road and not on your phone.

As a phone call comes in, Navdy's built-in camera allows you to simply swipe in midair to answer calls (or dismiss them), so you no longer have to fumble with buttons or touch screens. Plus, Navdy's voice recognition uses the voice commands you're already familiar with, whether you use Google Now or Siri.

Any notification on your phone (such as text messages or social media) can be played, read aloud or disabled, based on your preferences. Navdy even allows you to keep your teenagers safe by giving you parental controls.

"It Never Hurts To Ask"

"It never hurts to ask."

We often hear that said. But is it true? Recently someone asked me for a favor. The request came in an impersonal form e-mail. I had some business dealings with this person many years ago. Since then, I had heard from them only once when they asked another favor.

I was being asked to promote something on my social media network. The request did not offer an excerpt, a preview, a sample or any compelling reason why I should offer my assistance and ping the people on my e-mail list.

I thought, "Why should I help?" The implied assumption that I owed this individual something, or that I should help for no reason other than that they asked, seemed a bit off-putting. Have I helped an unfamiliar person before? Yes, there have been circumstances where I was glad to do so. But "Do this for me because our paths crossed" is not a good reason. Sometimes it *does* hurt to ask. Sometimes it comes across as inappropriate or entitled. Asking someone for a favor when you have no relationship with them *is* a bad idea. Naturally, most people like to help — but very few people like to waste their time or energy. And *nobody* likes to feel someone has taken advantage of them.

There's nothing wrong with asking for a favor or assistance. Just make sure you ask the right person for the right reason in the right way. Otherwise, you might damage your reputation and your relationships.

Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller *The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary,* which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

The Lighter Side:

Great Starting Salary

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

"I need someone with an accounting degree," the man said. "But mainly, I'm looking for someone to do my worrying for me."

"How's that?" the would-be accountant asked.

"I worry about a lot of things," the man said. "But I don't want to have to worry about money. Your job will be to take all the money worries off my back."

"I see," the accountant said. "And how much will my position pay?"

"I'll start you at 85,000," responded the owner decisively.

"Eighty-five thousand dollars!" the accountant exclaimed. "How can such a small business afford a sum like that?"

"That," the owner said, "is your first worry. Now get to work."

Vacation Alert!

The ONE Thing You And Your Employees Should NEVER Do When On Vacation

'Tis the season when you and your team will be taking a little time off to head to the beach or your favorite vacation spot, and while we know we *should* completely disconnect from work, most of us will still check e-mail and do a little work while away — and that could end up causing some issues if you're not careful while working remote.

So before you head off to have a little fun with your laptop tucked under your arm, keep this in mind: never automatically connect to "any available network." Not all Internet connections are secure, so if you're going to log in to the company's network, e-mail or other critical cloud apps that are hosting sensitive information, ONLY do so on a trusted, secured WiFi and NEVER a public one. We recommend investing in a personal MiFi device that acts as a mobile WiFi hotspot IF you're going to be traveling a lot and accessing company info.

Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

Finally, disable all printer and file-sharing options on your mobile devices. This is another way hackers can gain access to your network. In an ideal world, you and your employees would take a true break from work, but if they aren't able to completely detach themselves, then at least require them to stay safe using the above tips.

Who Wants To Win A $10 Gift Card?

Just for fun... First person to call us with the correct answer will win a $10 Amazon.com Gift Card!!

Which kind of animal did Florence Nightingale often carry around in her pocket?

a) Kitten **b) Puppy** **c) Owl** **d) Snake**

Call us right now with your answer to win!

816-229-2290

*"Like" our **Pro Computer Solutions** page on Facebook for tech news and company announcements throughout the month!*