TECHMinutes

December 2011

Your Small Business Technology Information Source!

This Issue:

Welcome Saysha Goodrow to the team!

Saysha is our newest edition to the team, she is responsible for coordinating of all of the IT support, web design and development groups. She will be answering the phones and dispatching tickets with the proper SLA.

Her #1 job is to make sure your company is getting serviced as quickly and efficiently as possible. Improving customer service and satisfaction.

She has been in training for almost three months with Charlotte and has recently taken over the Service Dispatch Role!

About Directive

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:
newsletter.directive.com

Making Your Business BYOD Compliant

We talk a lot about smartphones and tablets as business tools, but these days more and more people are using high-end devices personally. It's likely that they are bringing these devices in to work, and often using them to become more productive at their job. We call this Bring-Your-Own-Device, or BYOD, and it isn't a bad thing. The catch is managing security risks when users are using their own personal gadgets.

Some companies outlaw the use of personal devices, or lock employees into company-owned devices such as mobile phones simply to escape the responsibility of trying to manage personally owned devices. The goal is to not stifle productivity or make your employees feel like they can't use their smart phone as a work tool, but protect sensitive company information and promote security. The lines are fine - policies that hinder employees from doing their jobs correctly can affect employee longevity and morale, and savvy users will find ways around them whenever possible.

Making sure your users are aware of risks and educating proper use is important, and it's more than half the battle. Simple concepts like not clicking links from unknown senders and using secure passwords should always be passed down to staff. Some industries may need to enforce additional rules to protect sensitive data, so what works for a real estate agency isn't the same solution an accounting firm should use.

Setting up policies such as the ability to deactivate or purge the device in the event it is lost or stolen is a great idea, and not only protects the business but the personal information the owner might have on the device. Most devices let you kick off domain and email policies such as data encryption as well, so if the device is stolen the data can't be accessed without a password.

(Continued on page 2)

"If I had eight hours to chop down a tree, I'd spend six hours sharpening my ax"

-Abraham Lincoln

Making Your Business BYOD Compliant

(Continued from page 1)

The real focus however, shouldn't be on the device, but on the data itself. Look at where your data is being stored, how it is being accessed, and ask yourself if there are ways to improve that security. Contact Directive if you'd like to evaluate your current security, it may be much more cost effective and secure to lock things down internally instead of trying to do so for each device that needs to access the data.

Finally, if a user brings their own laptop or tablet in to increase their productivity, consider controlling its access to the internet. One solution is to provide a completely separate way to access the internet that doesn't go through the company's internal network; such as a wireless access point. The device can then dial into the network and authenticate just as it would if it were outside of the organization. At that point, you wouldn't need to manage the device so much as the same security policies that you have in place for remote access.

Do your employees bring mobile smartphones, tablets, or other devices into work to help them perform their job better? Give us a call at 607.433.2200 to secure your sensitive data without getting in the way of productivity.

Share this Article!
http://bit.ly/tvXJuR

Social Media Scammers Play Dirty

Ever since the public has been logging on to the Internet, certain people have been using the Internet to take advantage of others. Whether it be through scams, viruses, malware, phishing, or a whole slew of other dangerous activity, cyber criminals have been very good at making Internet security an industry on its own. With the colossal popularity of social networks like Twitter and Facebook, miscreants are capable of targeting even more users than ever before. On top of that, their methods seem to be hitting people where it hurts. Learn how you can prevent falling into one of their traps.

Cyber criminals are adaptive - they target weak points and vulnerabilities not just in technology, but the vulnerabilities in society as well. Think about the infected attachments that used to get passed around in chain emails, or the Nigerian Advance Fee scams where a complete stranger would offer you 'the sum of $40 million U.S. dollars' if you send them a few grand to unfreeze their bank accounts. I hope that very concept sounds like hogwash to everyone, but believe it or not, folks fall for it.

Social Media scams work the same way; they target both a vulnerability in the technology and spread it by focusing on a human weakness. One recent example is the death of Steve Jobs - cyber-crooks took advantage of this unfortunate headliner and fabricated a fake Steve Jobs Charitable Foundation asking for donations to help young programmers. Other scams include offering free iPads, but the end results really just tricks you into clicking on a link and submitting your personal information. Other scams are designed to peak your interest with topics like discovering who is viewing your Facebook profile, or claiming that there are pictures of you or your friends here that 'you won't believe.'

Often, clicking on these links will spam your friends with the same message, which contributes in the spreading of the scam. The links can even take you to a site that can infect your machine with malware, or trick you into sharing private information with the scammer. On top of that, it can install an app on your Facebook account that will continue to hijack your account and spam your friends. The problem is when you see something posted by a friend, even if it is suspicious, your guard is down. This means scams like this spread faster than wild fire.

What to Look For

If you've clicked on a link posted by a friend and it just doesn't seem to be what you expected, raise a flag. Be wary of offers to find out who's been looking at your Facebook profile, free iPads (and other popular consumer electronics), or sensationalized content involving you (like messages referring to pictures of you or your friends from last weekend). These are typically going to be scams. If you aren't sure, try strumming up some dialog with your friend before clicking. If they don't know what you are talking about, chances are they are spreading spam posts without even knowing it. If someone sends you a link, ask them about it before just clicking it.

If you get friend requests from users you don't know, check their location. If they are local, chances are they are legit. You might even be able to go one step ahead and Google their name to see if there is any information about them being a scammer. Granted, it's terrible that we need to resort to these levels in a social environment, but it is better to be proactive.

Above all else, don't ever share your personal information (social security number, credit cards, and passwords) when things seem suspicious. If it suddenly appears you need to log back into

Online Shopping Safety for the Holidays

Still haven't found all the right gifts for this holiday season? You are on your own there - but we CAN help ensure a safe online shopping experience. Internet shopping has become widely popular over the years, and this year retailers have seen a big increase in mobile transactions as well. Consumers can skip the lines and the crowds and save a lot of cash in the process. Online shopping is generally safe, although there are a few tips you'll want to be aware of before going virtual shopping this holiday season.

Be Sure It Is a Trusted Site

When dealing with big names like www.amazon.com and the online sites of big retail outlets you are typically in good hands, but be a little wary when shopping somewhere you don't recognize. One of the simplest and non-technical ways to check if a site is legit is by doing some very quick research. Reseller Ratings.com and Bizrate.com let users review and rate online shopping experiences.

Lookout for Prechecked Offers

Just like brick and mortar retailers trying to get you to opt in for expensive warranty or buy-back services, online retailers might try to opt you into special offers. Don't hurry through the forms - you might sign up for something you didn't want and end up paying for it in the long run.

Document Your Purchase

Although most sites email you a statement of what you purchased, it doesn't hurt to document it yourself. Copying and Pasting everything (especially the transaction summary) into a Word document could be handy. Don't forget you can take screenshots and past them into your Word document by either using the PrtScn key on your keyboard, Microsoft OneNote's screen capture tool (Windows key + S if you have OneNote), or the Windows 7 Snipping Tool (Start Menu > All Programs > Accessories > Snipping Tool). Be sure to document the date you made the purchase and the expected delivery, and what should be included. On top of that, be sure to take down the web address, vendor name, address and telephone number.

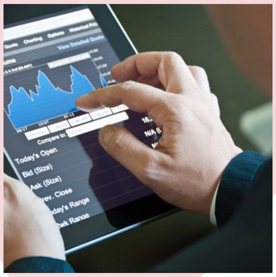
Watch your Credit Cards

Keep track of your credit card statement for any mystery charges. Although in the grand scheme of things it is rare, sometimes vendors get hijacked and customer credit card information gets stolen. Keep an eye on it and be prepared to challenge any unauthorized fees or other charges.

On top of that, be sure to read the site's privacy, return, and refund policies, and above all else, trust your instincts! If the site gives you a bad feeling in your gut, leave it. If prices seem too good to be true on popular consumer electronics ($85 iPad 2s, anyone?) then it probably is.

Share this Article!
http://bit.ly/sOqSqL

Holiday Shopping - Let's Talk Tablets



Tablets are definitely becoming a staple in the consumer electronics world. For the longest time, the tablet PC was an expensive, clunky device that just didn't wow consumers. Some businesses had adopted tablets back in the day, but they were difficult to use, hard to support, and they simply didn't perform for the price tag. However, like many consumer electronics, Apple reinvigorated the tablet market with the original iPad, and now it would seem tablets are here to stay. The question is, are they right for businesses?

Tablet devices are very similar to modern day smart phones. In fact, in most cases, the apps you run on the phone usually translate to the apps ran on the tablet. You get the basics; email, web surfing, streaming video, calendar, note taking, and more, but the difference is you get all that on a larger device. Ask yourself if you would like that basic functionality that your smart phone gets with a larger playing field, and you'll have a pretty good inclination of you want to jump on the tablet bandwagon. However, the future of tablets is looking even more robust; Microsoft's Windows 8 operating system is being built for both desktops and laptops and also tablets. This means you'll get the same OS you would run on a desktop PC on your handheld tablet. Although the hardware in a tablet isn't quite as beefy as what you'd find in a desktop, dual and quad-core CPUs and integrated graphics and generous amounts of memory are ...

Read the rest Online!
http://bit.ly/rpuemu

Social Media Scammers Play Dirty

(Continued from page 2)

Facebook, you are probably being phished - a scam that makes you think you are providing sensitive information to log into a site, but really that data is being sent to a crook.

What to do When You are the Victim

If you think you've been scammed, go into your Facebook privacy settings and edit the settings next to Apps and Websites. Click the X next to any apps that you want to delete. You'll want to go onto your profile and remove any posts that app has made and alert your friends to what happened, and share these instructions with them in the event they fell victim as well. Finally, change your Facebook account password. It wouldn't hurt to check your antivirus and make sure it is running the latest definitions, just to be safe.

Social Network Safety Rules to Live By

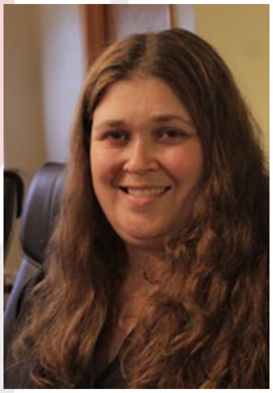
- Verify Facebook apps before you approve them. During the approval process (before you grant the app access to your account), the app will display the author's name. Clicking on it should take you to the app's homepage. Check for anything that seems strange, out of place, or unprofessional. You can also check user experience and even do a Google search to find out if it is a scam or not.
- Don't give out personal information (including your login and password). Always check the URL in your address bar to make sure you are on the official (Facebook, Twitter, LinkedIn, etc.) website when logging in.
- Be skeptical: It's likely your friend doesn't have embarrassing photos of you from last weekend, or has a solution for finding out who's stalking their account on Facebook. When in doubt, a quick Google search should be able to confirm a scam.
- With social media, a big part of the way scams and attacks get passed around is amongst trustworthy friends and acquaintances. Not everybody is mindful of security.
- And the big golden rule that will provide you the best protection is to be mindful of what you click on.

Do you think you've been scammed? Contact us at 607.433.2200 for assistance in recovery and future prevention.

Share this Article!
http://bit.ly/rU5iaP

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.

Chris Chase
Solutions Integrator



Charlotte Chase
Solutions Integrator

Closed for the Holidays!

In observance of the Holidays Directive will be closed on Friday, December 23rd, Monday, December 26th and on Monday, January 2nd, 2012.

As always Emergency Support is available by calling (607) 433-2200

Happy Holidays and a Happy New Year!

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

facebook.directive.com

linkedin.directive.com

twitter.directive.com

blog.directive.com

newsletter@directive.com