



This Issue:

Some Hackers Are Out to Give IT Departments a Bad Reputation

Unfamiliar with BYOD? Here's Where to Begin

A Step-By-Step Guide to Broadcasting WiFi From Your Android Device

It's Easy to Forget about Quality IT Service, and That's Okay

Using Big Data Gives You a Big Competitive Advantage

Block People from Your Network that Have No Business Being There

A Step-By-Step Guide to Broadcasting WiFi From Your Android Device



We all know how touchy WiFi can be, especially when you need it most. A

shoddy wireless signal can be especially troublesome if you have tasks that need to be completed, and you need a WiFi connection to complete them.



Read the Rest Online!
<http://bit.ly/1dL7u1E>

About Celera Networks

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.celeranetworks.com

Some Hackers Are Out to Give IT Departments a Bad Reputation



We all know that hacking is one of the biggest risks we must deal with in today's technology-based society. Most hackers out there try to take advantage of the latest vulnerabilities in software, but there are some that use a more sophisticated method. These hackers try to take advantage of the weaknesses found in the human psyche, rather than the technological flaws that consistently get patched.

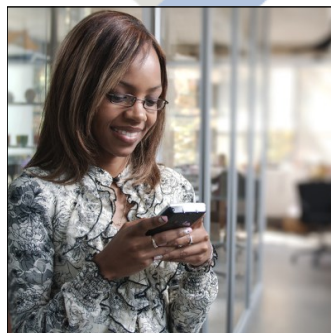
Attacks like these are generally classified as phishing scams, in which the hacker will attempt to steal sensitive information by taking advantage of employees who might not know any better. They will often pose as important individuals from recognized institutions, like banks or business partners, and attempt to coerce credentials from your team. These can come through phone calls, emails, or other mediums.

Some of the most offensive crimes against the general populace and this technological society in general are how hackers will often impersonate IT staff to further their own goals. As IT technicians ourselves, this makes us sick. We can't think of a more grievous way to infiltrate a system. Not only do these hackers access systems without permission, but they also ruin the good name of hard-working IT professionals whose goal it is to put a stop to attacks like these in the first place.

In fact, the security experts at FireEye have reported that these impersonation crimes rank as some of the most commonly used tactics by hackers. The primary reason these tactics work is due to a lack of two-factor authentication. As ZDNet reports:

(Continued on page 3)

Unfamiliar with BYOD? Here's Where to Begin



A trend that's taking the office by storm is BYOD, or Bring Your Own Device. These policies entail workers bringing their own devices to the office and using them for work-related purposes. While this opens up many avenues for enhanced productivity and efficiency, being too laissez faire with your BYOD policy could instigate some problems later on, primarily in the security field.

Why BYOD?

Before diving head-first into BYOD, you should take a moment to consider why you want a BYOD policy in the first place. If you're concerned about your team using their personal devices for work because you think they'll waste time playing games, perhaps a BYOD policy might not be the best solution for you and your business. If you're allowing your team to bring their devices to work, you need to be prepared to take certain steps to guarantee productivity and security. Additionally, the Internet of Things complicates the nature of BYOD. More devices are connected to the Internet than ever before. In light of these complications, you might feel that BYOD is a security discrepancy, at best.

(Continued on page 2)

It's Easy to Forget about Quality IT Service, and That's Okay



When it comes to service jobs, there are two kinds: Those where the work is highly visible, and those where work gets ac-

complished behind the scenes. Each service is valued and needed, yet, one may receive more attention and recognition than the other. Managed IT service falls under the latter category, and we're totally okay with that.

How do you know if we're doing our job correctly? If you don't physically see us at your office managing and maintaining your company's IT infrastructure, does

that mean that we're not doing anything? Absolutely not. With Celera Networks managed IT service, we're monitoring your systems around the clock and constantly taking care of a variety of IT issues so that your systems run as smooth as can be. Due to the nature of this kind of preventative service, it's easy for you to forget about us, and that's kind of the point.

For those of us at Celera Networks, it's not like we're antisocial or that we don't value the company of your business. Instead, it's our prerogative to stay behind the scenes. This approach keeps us out of your way while we do what it takes to get the job done. As odd as this sounds, when it comes to preventive IT

care, lack of interaction with those we serve is how we gauge success.

This idea is communicated in a mantra that we've been going by for years, "Making Technology Work for You." The entire point of technology is that it's meant to enhance your goals and improve the efficiency of your business. If you have to spend time resolving technology issues, or even managing IT technicians that are on your premise, then that's time taken away from running your business, which negatively affects your bottom line.

At Celera Networks, we understand the dynamics of how valuable your time is,

(Continued on page 4)

Unfamiliar with BYOD? Here's Where to Begin

(Continued from page 1)

However, contrary to some opinions out there, BYOD has incredible potential to be beneficial for your business's operations. With BYOD, your team can feel encouraged to work more hours, especially from the comfort of their own home. Additionally, some employees find themselves more productive using their own familiar devices rather than the foreign company-provided machines. Finally, being able to use their own devices can be a significant morale booster for your team, and you know what they say; when you feel good, you work even better.

Integrate Solid Guidelines

Integrating a BYOD policy into your business strategy is one that requires precision and careful thought. More often than not, it requires a dedicated project manager that knows their way around the industry. If this is your first foray into the unknown wilds of BYOD management, it'd be best to contact Celera Networks and let our trusted technicians help you find your way forward.

As for a general pointer, one of the best things you can do is to set up specific guidelines that your team should abide

by when using their devices for work. Without set-in-stone rules that can be applied company-wide, you risk the chance of someone being out of the loop, and therefore, not abiding by the rules you've put in place for your organization.

Mobile Device Management

It can be time-consuming and difficult to integrate your own BYOD policy, especially if you aren't sure how to approach doing so. A mobile device solution from Celera Networks can make these difficult decisions for you. In order to maximize security, the mobile device management solution can perform these functions:

- **Limits network access to secured wireless devices.** With a BYOD policy, you'll have a lot of new devices attempting to access your network. It's important that only devices which have been approved have this access. Otherwise, you might be opening up your network to a whole new host of threats.
- **Whitelists and blacklists applications.** Certain applications request data from the mobile device which accesses them. Many users will

download a new application and immediately install it, ignoring the window which reveals what personal information the app pulls from your device. We can limit the information which is shared with applications by whitelisting and blacklisting them.

- **Remotely wipes misplaced devices.** Devices that hold sensitive corporate data could accidentally fall into the wrong hands, be it a competitor, a hacker, or just a jerk. It's your job as the business owner to make sure you're ready to deal with this regrettable situation. Setting up remote device wiping is a good way to ensure that your private data stays private, even when it's misplaced.

If you're ready to get started with BYOD, but you aren't sure what the best approach is, give Celera Networks a call at (617) 375-9100. We'll be sure to help you understand and implement the best BYOD strategy for your business.



Share this Article!

<http://bit.ly/1E5H841>

Some Hackers Are Out to Give IT Departments a Bad Reputation

(Continued from page 1)

“Social engineering, phishing campaigns and the impersonation of legitimate IT personnel are also on the rise. The security firm says that through 2014, FireEye observed hackers impersonating IT staff in 78 percent of phishing schemes directed at companies, in comparison to just 44 percent in the previous year.”

As IT professionals and human beings, we cannot stand idly by while innocent people are targeted. The small or medium-sized business may not have the in-house IT department to constantly keep watch over your company’s network. This is why Celera Networks offers security solutions that are designed for inte-

gration into any network. Our Unified Threat Management (UTM) device is a comprehensive network security measure that includes a firewall, antivirus, spam-blocking, and content-filtering solution, all designed to help your organization cope with the constantly-evolving threat landscape that comes with the business environment.

Additionally, Celera Networks offers two-factor authentication services which can make phishing attacks less dangerous. With two-factor authentication, your team will need to enter in a secondary credential in addition to their username and password. These are often sent to a secondary device which prevents a hack-

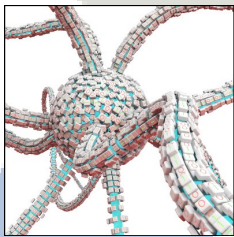
er from accessing it. This secondary credential is often sent to a phone in a text message, but you can also rig it to send automated voice calls, and much more. Whatever you choose to do, these messages provide an extra hurdle for hackers, making it vastly more difficult to access your important data.

Don’t let hackers get the better of your company’s network. Give the real IT pros at Celera Networks a call at (617) 375-9100 to show cybercriminals you mean business.



Share this Article!
<http://bit.ly/1E5GaFc>

Using Big Data Gives You a Big Competitive Advantage



Today’s technology has accomplished a ton of fascinating things, but none are more important for the average business

than big data analytics. When considering the incredibly competitive nature of the business environment, anything that gives your company an edge is a welcome addition to your strategy, and it’s more important than ever before to heed this call to action.

What is Big Data?

Big data is the act of analyzing chunks of raw data for trends and other important information. This helps businesses make informed decisions concerning new policies, their target audience, and much, much more. With the knowledge of these trends, your team can apply them to your business model and potentially surpass your competitors.

One example of big data would be a consumer-based company monitoring their social media pages for trends in their followers. They look for patterns in the interests of their followers, including

age, gender, liked pages, and more. These trends allow the company to tailor their marketing campaigns to meet the interests of their primary consumer base.

As explained by Bill Detwiler of ZDNet:

“According to a 2014 study by Accenture and General Electric, 84% of the companies surveyed believe that big data analytics could “shift the competitive landscape” for their industry within the next year and 89% believe companies that fail to adopt a big data analytics strategy could lose both market share and momentum.”

If what this survey says is correct, businesses who have taken the initiative that big data has to offer will have an incredible advantage over those that don’t. Additionally, big data analytic tools are growing more popular and more affordable, making them more readily available to the average small or medium-sized business.

How to Get Started

Unless you have a solid plan for gathering all of the data required for these kinds of analytics, you’ll probably run

into some trouble at first. Instead of jumping the gun and getting ahead of yourself, consider what kind of data needs to be acquired. According to Max Shron, a data scientist at Polynumeral, it’s important to find out what kind of data you need before collecting it. Otherwise, you might collect data that isn’t of any use, and you’ll have wasted time.

Instead, ask yourself what kind of data your business already possesses. From there, consider what kind of data you need. Once you understand your target, you can go about collecting this data in an organized manner. It’s important to put aside any predispositions you might have concerning your data or product. After all, numbers don’t lie, and it’s much easier to put together a solid plan based on facts rather than remain biased toward your services.

Celera Networks can help equip your company with the big data analytic tools your business needs to get ahead in the industry. For more information about what we can do for your business, give us a call at (617) 375-9100.



Share this Article!
<http://bit.ly/1dL6DBs>

It's Easy to Forget about Quality IT Service, and That's Okay

(Continued from page 2)

which is why we do everything within our power to resolve an issue before bringing it to your attention. Granted, from time-to-time there may be hardware issues that can't be taken care of over the phone, and if you're looking to stay on top of the latest technologies, then you will want to see us before signing off on a new IT solution; but our point here is that, with managed IT services, this face time is minimized.

How's this work? The point of managed IT is that technology issues are quietly taken care of by remote maintenance while they are still small enough to not cause alarm. Ultimately, this proactive approach leads to far fewer technology problems that are major enough to

require your attention, especially compared to the break-fix model where the lack of proper maintenance causes more severe problems to happen much more frequently.

Of course, it's not like we're purposely trying to avoid you or anything like that. On the contrary, we at Celera Networks are available to see to any and all of your technology needs, including the ones that require a lot of face-to-face interaction, like sitting down together to create a technology roadmap that covers your company's present and future technology needs. In fact, we think that your business can greatly benefit by regularly meeting with us to discuss your organization's goals. We're happy to meet regularly with you to dis-

cuss these goals through our IT consultation service, which we feel is the absolute best way to maximize how technology can be leveraged to help you reach your unique goals.

At Celera Networks, we work hard to get out of the way and stay behind the scenes so that you're not distracted by technology issues, and we're always available to fully engage you with expert advice on how you should handle your technology. Call Celera Networks at (617) 375-9100 to check in with us. We're here to help you succeed.



Share This Article!
<http://bit.ly/1E5HWWP>

We partner with businesses in many different vertical markets throughout the New England area. The Celera team is focused on customer service and we strive to eliminate IT issues before they cause expensive downtime. Our goal is for our clients to continue to focus on what's most important - their business. Our dedicated staff is known for going the extra mile and doing what it takes for our clients to be successful with their technology investments. Your firm's success is our success.

Block People from Your Network that Have No Business Being There



When a company is lax about their network security, this can

lead to countless threats swarming the network and invading your systems. Yet, sometimes the most dangerous threats come from within. A common issue comes from employees accessing undis-

closed files unintentionally and deleting them, which can cause more damage than you think.

Take, for instance, the food industry. There are several integral employees that a fast food restaurant employs. There are cashiers, managers, and food prep team members. The cashiers require access to the cash registers. The managers require access so they can

count the drawers and record the day's profits. The average food prep employee, though, doesn't need to access the cash drawers. Therefore, they have no reason to do so.

This is how the principle of least privilege operates.



Read the Rest Online!
<http://bit.ly/1dL7a6x>

Tech Fun Fact
In 1975 the retail price of an Intel 8080 microprocessor chip was \$150!

Celera Networks

11 Elkins Street
Suite 330
Boston, Massachusetts 02127
Voice: (617) 375-9100



-  facebook.celeranetworks.com
-  linkedin.celeranetworks.com
-  twitter.celeranetworks.com
-  blog.celeranetworks.com
-  newsletter@celeranetworks.com

Visit us **online** at:

newsletter.celeranetworks.com

