CELERANETWORKS
Making Technology Work For You

TECHMinutes
July 2015
Making Technology Work for You

This Issue:

What a Firewall Does (and Doesn't) Keep Out of Your Network

One of the most vital parts of your network security is a firewall. This is generally your first line of defense against the myriad of threats that can be found while online, and are instrumental to comprehensive network security.

Read the Rest Online!
http://bit.ly/1dG4A1c

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

Why Using a VPN is the Most Secure Way of Accessing Corporate Data

As a business owner, you're constantly moving around. At the same time, you're expected to keep in touch with your base of operations, respond to employee and client inquiries, and many more mission-critical tasks that require the use of remote technology solutions. Unfortunately, public WiFi hotspots are known to be cesspools of online filth, where a secure connection is nothing but a dream. One way to correct this issue is with a Virtual Private Network (VPN).

What is a VPN?

To put it simply, a VPN is a network that only authorized personnel can access. This helps keep the transfer of data private, meaning that VPNs are especially useful for connecting to confidential enterprise data. This is generally done through encryption hardware or software, which entails encoding and decoding information as it's sent or received.

How Does It Work?

VPNs basically keep your data safe while it's being sent and received from your corporate infrastructure, but how does this work? Gizmodo describes the process which a VPN tends to use in more detail:

"Because VPNs use a combination of dedicated connections and encryption protocols to generate virtual P2P connections, even if snoopers did manage to siphon off some of the transmitted data, they'd be unable to access it on account of the encryption. What's more, VPNs allow individuals to spoof their physical location—the user's actual IP address is re-

(Continued on page 3)

Passwords May Be "Ineffective," But They're Still Necessary

It seems like we can't go on the Internet without reading about some sort of data breach. Sometimes they're caused by poor security measures, like lack of data encryption or two-factor authentication; other times, it's because of lackluster password security. Despite the antiquity of the username and password, they're staples in the modern office. Thus, it's important that they're as secure as possible at all times.

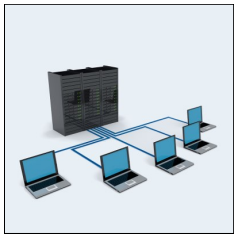
Passwords might have their flaws, but they're necessary if you want to maximize your business's security from online threats. It's not just your organization's future at stake; it's also yours as an individual, not to mention your employees and anyone associated with your company. Here are three ways you can improve the security of your passwords in the workplace.

Educate Your Staff About Best Practices

According to Processor magazine, "In establishing a pragmatic password policy, the first step is balancing risk, compliance, and usability needs, followed by education and enforcement."

(Continued on page 2)

Improve Business Operations with Virtual Desktops



Anything that makes your business more mobile is a good thing, right? This is one of the main goals of virtualization services. These separate the software from the hardware it's installed on, allowing it to be isolated and installed on a virtual machine where it can be accessed as an individual instance. Many businesses are finding success in their workplace by taking advantage of desktop virtualization services.

According to Processor magazine, "virtualized desktop infrastructure (VDI) technologies give IT administrators more control over their infrastructure and in turn help IT teams deliver operating systems and applications to end users in new ways." This means that virtualization has the ability to help your business simplify its infrastructure and make it more efficient. In other words, a virtualized desktop system can help your business push above and beyond its current expectations.

> ***"Virtualized desktop infrastructure (VDI) technologies give IT administrators more control over their infrastructure and in turn help IT teams deliver operating systems and applications to end users in new ways."***

There are several benefits that your business can reap from a virtualized desktop infrastructure:

- **Consolidate your infrastructure:** Limiting the amount of physical hardware your business needs to run can be one of the best benefits that virtualization offers. Rather than running many different workstations, you have the ability to switch to thin clients. These devices are much more energy-efficient and don't require the heavy-duty hardware that an ordinary workstation would. The IT administrator has the ability to allocate resources equivelant to the needs of an individual machine, allowing for more versatility and control than an ordinary PC.
- **Virtual desktops can be used remotely:** Another great capability of virtual desktops is that they can be used remotely, as well as within the office, provided their devices have been approved. This lets them gain access to the same desktop and applications they would have if they were in the office. This is especially helpful if you have workers across the country, or on business trips.
- **Simple integration and upgrade procedures:** While the configura-

(Continued on page 4)

Passwords May Be "Ineffective," But They're Still Necessary

(Continued from page 1)

This means that it's the responsibility of you, the business owner, to make sure that everyone is exercising precaution and following strict security standards for their passwords. The usernames aren't so important, so long as they aren't "admin," or other similar common denotations.

Passwords should include many different types of characters, including symbols, numbers, lower-case, and upper-case letters. You should avoid using whole words whenever possible, and strive to make them as difficult to replicate as you can; and whatever you do, do NOT use your Social Security number or birthday. Taking these preventative measures will decrease the chances of hackers accessing accounts without permission.

Integrate Two-Factor Authentication

Two-factor authentication is growing in popularity, and it's easy to see why. These measures add an extra layer of security to your online accounts, which require an external credential in order to crack. This could be your mobile device, or it could be a set of credentials emailed to you or sent via SMS. Regardless, this adds another step to a hacker's process which often requires them to have physical access to your mobile device, which could discourage them. Celera Networks can help your business set up a two-factor authentication system that can help your business achieve optimal security.

On the Server-Side, Use Strong Network Security Practices

We all remember how technology supergiant Sony got hacked a few months back. Sony foolishly labeled the folder which held their passwords, "passwords." This meant that, once hackers got into their infrastructure, they knew exactly where to look to steal passwords from the lax company. This isn't something you want to experience first-hand, as the fallout from the Sony hack so painfully showed us.

Instead, you should prioritize making sure that hackers can't get into your network in the first place. A Unified Threat Management (UTM) solution is capable of such a feat. Armed with a firewall, antivirus, spam blocking, and content filtering solution, you'll have little to fear from both internal and external threats. Still, it never hurts to be prepared for the worst.

Always take precaution when dealing with passwords, especially if they protect sensitive information. For more security advice and to establish two-factor authentication, our UTM, or more, contact us at (617) 375-9100.

Share this Article!
http://bit.ly/1dG3in3

Why Using a VPN is the Most Secure Way of Accessing Corporate Data

(Continued from page 1)
placed by the VPN provider—allowing them to bypass content filters."

In essence, the most secure way to access any information online is through a VPN. Not only is your data hidden from view, but even your physical location is obfuscated from any prying eyes.

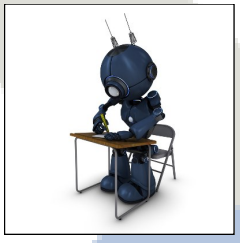
Why Should You Use a VPN?

The reasoning is clear. When you're out and about, or working remotely from an airport, train station - anywhere, really - you can't afford to use sketchy WiFi signals that may be teeming with hackers, waiting to jump your data while it's in transit. Putting your data at risk is the same as putting the future of your business at risk.

You don't have time to worry about corrupt WiFi networks when work needs to get done. Additionally, integrating a corporate VPN solution can be challenging if you're unfamiliar with the territory. The skilled, professional IT technicians at Celera Networks have the knowledge required to equip your organization with powerful, flexible VPN solutions designed to help you keep a secure connection to your company's data infrastructure while you're on the go. Give us a call at (617) 375-9100 to learn more.

Share this Article!
http://bit.ly/1dG3e6G

Can You Spot an Article Written By a Robot?



When your website has content or makes changes to its existing content, it can be of great benefit to your business's marketing endeavors. In fact, it's so important that innovators and programmers have built software that's designed to perform the act of content writing. In other words, there are robots that compose web content. How does the writing of a robot hold up to that which is written by a human?

According to Slate, many organizations, like The Associated Press, Edmunds, and Yahoo, have turned to automation processes for producing content. This means that it's grown common enough to invade the reading habits of the average consumer. Thankfully, for the time being, humans still have the upper hand in the art of content writing due to a number of reasons, including the ability to think critically and behave like a human being.

So, how can you tell if a robot has written an article? It's usually pretty simple; if the text doesn't appear to have a grasp of the underlying concerns of a piece of writing, or it has a shocking lack of emotional investment, it's safe to say that a robot probably wrote it (or someone with no personality wrote it, which is also a possibility). Humans are able to instill some sense of emotion into their writing, which is a clear one-up on computers, despite their impressive plethora of other advanced capabilities.

In contrast, a computer performs a vastly different role when it comes to producing content. With the power to process data and generate it quickly, they are, if nothing else, efficient. Despite this advantage, it's unlikely that content produced by computers can have the same characteristics as that which is produced by humans.

Robotic Writing: The Benefits

Despite the significant sacrifice that robots make concerning human emotional attachment, there are some benefits that a computer holds over human writers. Computers, due to the speed at which they operate, are capable of pushing out text much faster than any human writer. This can be helpful for reporting on boring, cut-and-dry topics that human writers might find difficult (or at the very least, monotonous) to write about.

Additionally, once the software has been built and installed, it's relatively simple to keep running. Basically, it is a machine equipped with software, so as long as these are maintained, the operating costs of using a robotic writer is more efficient than accounting for breaks, sick days, and the all-important salary. Basically, robotic writers are good for writing articles that humans don't want to write, and the kind of articles that readers… well, don't want to read.

Humanity's Counteroffensive

In response to the computer threat, humanity has the enduring hope of ideals, feelings, opinions, and the human mindset in general. The machine isn't able to understand the text on a fundamental level. It might be able to interpret it, but it can't be emotionally invested in it the way that humans can. They have no prior experience to recollect and reflect upon; hence, their inability to create interesting and relevant articles.

What it comes down to for humanity is our ability to call upon past knowledge and use it to add something of value to the text. Computers lack the ability to use shared experience to connect to the audience, which puts the relatability of the text on the line.

While computers and humanity might differ in their approaches to the writing of content, they can work together to produce both dull, boring content, and text which can connect to the audience and engage them. Be sure to let us...

Read the Rest Online!
http://bit.ly/1dG4ird

Improve Business Operations with Virtual Desktops

(Continued from page 2)

tion of a virtual desktop solution can be tricky to implement in the beginning, these complications are nothing compared to the ease of upgrading later on. Instead of applying patches and updates to multiple different machines, the network administrator can dispatch updates to multiple virtual machines at once.

Setting up a virtualized desktop infrastructure doesn't have to be painful. Contacting a managed IT service provider is your best shot at making sure that virtualization happens smoothly. By outsourcing this responsibility to Celera Networks, we can make sure that your virtual machines are kept up to date and functioning properly. Just give us a call at (617) 375-9100 to learn more.

Share This Article!
http://bit.ly/1dG3CCd

When it's Hot Outside, Your Servers Are Burning Up Inside

If you host your own servers in-house, or in an off-site data center, you know all about the frustrations of keeping your hardware up to date and healthy. This also includes keeping your servers from overheating. These mission-critical pieces of hardware are known to produce incredulous amounts of heat, and keeping them cool only gets more challenging during hot, sticky summer months.

When a server overheats, it can have unexpected (or, well, obvious) results. Too much heat can fry your server's hardware, effectively disabling it and possibly ruining it for good. This is obviously not a good thing, and it can happen when you least expect it. Therefore, it's important that you always have a way in which to keep it cool and under control.

Here are three cooling factors you should consider when hosting your own server in-house:

- **Keep your servers in a temperature-controlled climate.** Basically, you should store your servers somewhere where you can easily control the temperature. There are cooling racks specifically designed for such a task, but many SMBs simply resort to closets with air-conditioning. However, if your server room consists of a closet with fans blowing directly on your hardware, you might want to consider a cooler solution.
- **Take care of your cooling equipment.** If your cooling machines fail, it's the same as allowing your servers to overheat. Therefore, the upkeep of your cooling system is of the utmost importance. Is the overall atmosphere damp? Is dust accumulating on your fan blades? Set up routine maintenance procedures and stick to them to avoid surprises, like a failing cooling system.

Be sure to allocate enough assets from your budget. Air-conditioning can be a costly expense. Even having fans running constantly can add a hefty addition to your electric bill.

Read the Rest Online!
http://bit.ly/1dG4nv5

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.

Tech Fun Fact
The S-100 is a data bus commonly used in early microcomputers.

Celera Networks

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

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

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