Total Networks
Business IT Done Right

NetworkNews
July 2015

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. Despite this common knowledge, some folks might not understand specifically…

Read the Rest Online!
http://bit.ly/1fd0vCI

About Total Networks

Building on the tradition of providing industry best solutions, the Kinseys continue to invest in tools, training, recruiting, and procedures, continuing to extend our reputation as the premier IT service provider in Arizona.

Visit us **online** at:
totalnetworks.com

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.

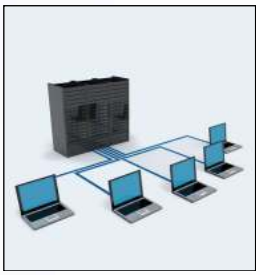
Educate Your Staff About Best Practices

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." 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

(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.

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

(Continued on page 3)

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

(Continued from page 1)

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. Total 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 (602)412-5025.

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

Uncovering the Hidden Dangers Lurking in your Inbox

Email is one of the easiest and most reliable ways to connect with your clients, and with the added bonus of allowing you to track your communication, you will never have to guess what your client said when.

But for all of the time management and organizational gains that email provides, it has one major vulnerability. Email is the road into your computer and once someone gets in, they can follow the digital arrows to infiltrate firm's entire IT system.

Clicking on a spam email allow hackers and spammers to easily bypass your firm's security system and get their hands on confidential information – like social security and financial account numbers that can be sold on the street. Or they can hold your data ransom until you pay, usually in the form of bitcoins, to have it released. And if this hack does happen, chances are your IT partner will have to restore your lost or corrupted files, and that can only happen if they've been properly backed up.

So how do you prevent utter email destruction? Below are several common tactics that spammers and hackers employ. If any of your staff fall for their tricks and open that suspicious email, it will not only cause a major headache with huge downtime, but breach your firm's security as well.

No Phishing allowed! One incorrectly identified phishing email is all it takes to infiltrate a business. McAfee conducted a quiz of 30,000 business users in 49 countries. Only 6% of the respondents correctly classified all of the emails as legitimate or phishing. 80% of all employees fell for at least one phishing email. If you suspect your message is phishing, hit Alt-F4 or upper-right "X" instead of "Cancel" or "Close" to close the email.

Email FakeOut: If you see an email from someone you know with a message that just doesn't seem right, it doesn't necessarily mean they've been hacked. But in reality, spoofing email addresses is a very simple hacking trick. Learn how to read message headers and trace IP addresses. In Outlook, you can double-click to select the spam message and open it in a new window to avoid clicking on the email. Click File > Properties to display the "Internet Headers."

Solicitors Not Invited: A legitimate company would never send out an unsolicited email asking users for personal information. Likewise, a real company would never send out an unsolicited email asking you to download an attachment. Even if the message looks real, understand that if it's unsolicited and is asking something of you (or even threatening you), then it's a scam. If you think there's a chance the message is from a trusted organization, then you can double check by calling the company about the email with the phone number from your records, not the one provided in the email. But never under no circumstance should you click or download on any attachment found in the email.

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

Improve Business Operations with Virtual Desktops

(Continued from page 1)

- **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 configuration 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 Total Networks, we can make sure that your virtual machines are kept up to date and functioning properly. Just give us a call at (602)412-5025 to learn more.

Share this Article!
http://bit.ly/1fcWK05

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. Therefore, you need to properly assess just how much you have available to allocate toward proper server cooling units.

You might also consider revamping your backup policy to one which constantly takes snapshots of your data. This way, despite your best efforts, if the server does overheat, you have a backup plan that can handle these unexpected problems. Our Backup and Disaster Recovery (BDR) solution is perfect for a time like this. It can take the place of your server in a pinch if it were to somehow become inoperable, and allows for a quick and efficient restore once you arrange for a replacement.

As a managed service provider, Total Networks knows how to provide quality technology management services to small and medium-sized business owners like yourself. One of our services is server hosting and management. This lifts the burden of maintaining your server hardware from your shoulders, and places it on ours. As capable technology experts, you'll have little to worry about in terms of proper...

Read the rest Online!
http://bit.ly/1fcYmaa

Fans of Facebook Now Have a Facebook Business App

Facebook has come a long way. Originally designed as a networking tool to be exclusively used by college students, Facebook now has 1.44 billion active users, making it the world's largest social network. Today, businesses take Facebook seriously and utilize it for their marketing initiatives. However, it's still viewed as a time-waster by many office managers who restrict or ban employees from accessing it.

Facebook is looking to change this perception, as well as capitalize on its popularity, with its new business application, Facebook at Work. Essentially, Facebook at Work provides companies with an inter-office communication tool that functions like regular Facebook. This can be advantageous for workers who are active on Facebook, making it easier to use than traditional communication tools that would be completely new to them. Plus, the familiarity of the Facebook interface may even get workers to be more willing to use it–something you want in an office communication tool.

Rest assured; unlike regular Facebook, which makes its posts available for the entire world to see, as well as has a reputation for monitoring personal messages, and even conducting social experiments on its users, Facebook at Work keeps the content private so that it's only visible to users within your organization, whom you give permission to.

According to Larry Dignan of ZDNet, there are a number of reasons why this expansion makes sense, including:

- Engagement during the workday is important for Facebook's business.
- Without work engagement, Facebook might lose users as they grow older and move into the professional world.
- A professional version of Facebook might convince enterprises to unblock the social network.

Will Facebook at Work… Work?

It's difficult to tell for sure. Even though it's a solid business communications tool, Facebook has a lot of PR work to do in order to change what business owners think about it, both in terms of productivity and trust. ZDNet's Charlie Osborne feels like the success of Facebook at Work is unlikely, citing the extremely protective stance towards data that today's companies are taking, as well as Facebook's previously-mentioned reputation for its handling of consumer data.

Additionally, one has to wonder just how successful Facebook will be at transitioning a product, known all over the world as a fun social tool, to a legitimate business tool. Granted, the components are all there for Facebook at Work to improve office communications, but Facebook's reputation precedes its latest business offering.

Another concern that business owners should consider is how tools like Facebook at Work will affect network security. Many companies block Facebook for security reasons, and an employee that gets comfortable sharing sensitive corporate information over Facebook at Work may grow too comfortable sharing the same information over their regular Facebook account.

When it comes to tools like this, it's important to keep in mind that every company is...

Read the Rest Online!
http://bit.ly/1fd07nR

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email skinsey@totalnetworks.com

Dave and Stephanie Kinsey
Owners

Bill Fox
VP, Customer Service

Total Networks

4201 North 24th Street
Suite 230
Phoenix, AZ 85016
Voice: 602-412-5025

Visit us **online** at:
totalnetworks.com

info@totalnetworks.com
facebook.totalnetworks.com
linkedin.totalnetworks.com
twitter.totalnetworks.com