GLOBALTECH SOLUTIONS

TECHMinutes

January 2019

Providing IT Solutions Nationwide

This Issue:

The Good, Bad, And Ugly Of The Internet

Network Security Is All About Handling Threats

Clearing Up A Few Common MSP Misunderstandings

Protecting Your Business By Understanding IoT Security

Use VoIP To Build Better Business Communications

As 2018 Ends, Mobile Cyberthreats Won't

Clearing Up A Few Common MSP Misunderstandings

Let's be real: the title "managed service provider" doesn't cast much insight into what we do on a daily basis. Even when people understand what we do, there are a lot of parts that confuse them and lead them to false conclusions. As a result, we wanted to take a few minutes and go over what it is that we do for our clients.

Breaking Down Managed Service Providers (Also Known As MSPs)

First, our title throws a lot of people. What are managed services, and why do you need a provider...

Read the Rest Online!
http://bit.ly/2UANf0x

About Global Tech Solutions

We provide IT Support such as technical helpdesk support, computer support, and consulting to businesses nationwide. It's always been our goal to provide enterprise-level IT practices and solutions, with small business prices.

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

It has been our honor to have been your trusted provider in 2018. Our New Year's resolution is to make 2019 even better - and this one will last longer than resolutions usually do!

The Good, Bad, And Ugly Of The Internet

Anyone that has spent any time online recently is sure to have come across something they've perceived as deplorable. For all the good that it does, some of the most divisive of human interaction happens on the web. Since it really depends on your perspective just how much negativity you take from the Internet, we'll go through the good, the bad, and the ugly of the Internet to put into perspective just how it affects our lives.

The Good

Let's start with the resoundingly positive attributes of the Internet. Firstly, it makes life extraordinarily easier. Banking, shopping, and direct communication with other individuals and businesses are all simpler and faster. People can get more done in a shorter amount of time. It makes people smarter by providing them access to a knowledge base unprecedented in human history. It provides the opportunity to connect with like-minded people from anywhere in the world at minimal cost, giving people the ability to do wonderful things for others whom they may have never met. It provides businesses and individuals, alike, the access to better opportunities, more knowledge, and interactions with people that matter to them.

Speaking of business, it has changed things for entrepreneurs precipitously. Data storage and retrieval is faster. Cloud platforms of all types offer software, hardware, security, and

(Continued on page 2)

Network Security Is All About Handling Threats

Countless threats stand between your business and productivity, even if modern security solutions have prevented the majority of them from ever becoming a problem. The fact remains that, unless you're being proactive about security, your organization could face a considerable challenge in keeping its network secure from intruders. We'll delve into what some of these threats are, why they are such an issue, and what you can do about them.

The Basics: Viruses and Malware

Your computer depends on software to run, whether it's the operating system or the software solutions on the device itself. Viruses are created to make changes to this code, and the results can vary in scope and scale. They can go from being minor annoyances to major time wasters. Malware is a bit more dangerous in scope. It stands for "malicious software," and its intentions are right in the name. Hackers develop malware for various purposes, but for the most part, it's with the intention of stealing, altering, or destroying data, depending

(Continued on page 3)

Protecting Your Business By Understanding IoT Security

Ah, the holidays; they are a time for good food and good cheer, but also tend to be a time of gift-giving of all kinds. You might have all kinds of new gadgets running around your office that aren't being accounted for. Some of these devices might be a security issue for your business precisely because they aren't normally meant to connect to the Internet. These Internet of Things devices just aren't as secure as they should be, especially in a business environment.

Of course, it's not entirely the fault of the user, even if they do represent part of the blame for this. Internet of Things devices are well-known security threats, but it's largely because of the way they are designed and developed. Even if the user was aware of the security issues presented by these devices, the truth is that there isn't anything they can do about it barring just not using them outright.

This is due to the fact that the security issues found in Internet of Things devices are built into them, particularly because the developers of the devices don't build them with security in mind. If you think about it in terms of what they are used to building--devices that don't have any kind of connectivity--it all begins to make sense. A manufacturer who produces a smart blender isn't a software engineer or a security professional. Up until that point, they just made blenders, so they had no need for software development or security. Unfortunately, this creates a device that is made with functionality in mind over security, much to the detriment of businesses.

These devices are most vulnerable to threats that could be patched, if only the Internet of Things devices were easily patched by the developer and the user. This isn't currently the case. It's practically impossible to distribute patches to all Internet of Things devices manually, so if the developer hasn't enabled automatic updates, you can forget about the user actually doing it, unless it gets in the way of the core functionality of the device. While this responsibility would fall on the developer, some have also suggested the implementation of unique default passwords, as users often see no need to change the default password on their new device before putting it to work.

To counteract these threats, businesses have to implement measures to keep their networks safe from the wave of additional devices entering the office. Whether you're aware of it or not, it's likely that employees are bringing new devices to work every day, whether it's a tablet or a smart watch. A Bring Your Own Device policy with clear-cut rules on what's allowed and what's not will go a long way toward keeping unwanted devices in the workplace, and it can help to provide a general outline for...

Read the Rest Online!
http://bit.ly/2Ba5L6ty

The Good, Bad, And Ugly Of The Internet

(Continued from page 1)

development platforms that reduces the enormous capital costs many organizations were spending on their IT. It gives organizations access to a glut of resources, no more important than a growing mobile workforce that is available around the clock, promoting better productivity. It provides the opportunity to streamline all types of work, whether it be reducing face-to-face interactions with your vendors, or utilizing tracking software that helps administrators build more efficient business practices.

The Internet has provided a social outlet to people who didn't have one. The use of social media has revolutionized the way people share and communicate. Each person has the freedom to do whatever they choose online, and often this results in positive action. Many important groups that have been marginalized for one reason or another are now able to promote their platforms thoroughly.

The Bad

There are some things about the Internet that many people can give or take. In fact, for every benefit listed above, there is a drawback. The easier access to information opens the door for more misinformation. For all the ease of banking, shopping, and communication there are threat actors looking to steal resources and personal information for profit. For every like-minded person that you meet, you meet all manners of Internet trolls and other unattractive people.

Social media has had an amazing amount of influence, but for all the good that it does, it also promotes individual freedom from convention, sure, but also creates what is known as a "toxic mirror" effect. This is the concept of making people feel bad about themselves by constantly being exposed to information that would make them create negative opinions about themselves. The toxic mirror makes anything that isn't physical, emotional, and mental perfection, ugly and bad.

Beyond the toxic mirror, many people use social media in ways that hurt the people around them. The manifestation of a social persona can often present the opportunity for a user to put out very public misinformation. This break from reality, further muddies people's ability to properly identify risk, putting them in harmful situations. The Internet is filled with trolls, stalkers, and bullies. These groups are allowed to run...

Read the Rest Online!
http://bit.ly/2BeGatC

Network Security Is All About Handling Threats

(Continued from page 1)

on what nefarious plot the hacker is using it for.

The More Dangerous: Ransomware and Spyware

There are other more specialized types of malware that are designed for specific purposes. Ransomware, for instance, is designed to extort money from unsuspecting victims. It encrypts files located on the infected device, only decrypting them when a ransom has been paid to the hacker responsible. These kinds of threats are quite popular with hackers as they can be used to target a considerable number of victims in a short amount of time. Spyware is also a popular threat that allows hackers to steal information in a covert manner through various means, including backdoor infiltrations, keyloggers, and so much more. This is particularly dangerous to your business' intellectual property.

The Vehicle: Spam and Phishing Attacks

Cybersecurity threats are the most dangerous when they can be concealed. After all, you never hear in the news about how a brute-force attack exposed millions of health records or passwords to the world. No, the most devastating data breaches are typically those that occur over an extended period of time, shielded from the eyes of security professionals and network administrators. Spam and phishing attacks that deceive users into clicking on links or downloading suspicious files play a key role in allowing threats into a network. It's more important than ever before to be cautious while online, as there is no telling who might try to trick you into exposing your network to threats.

Protect Your Business with Proactive Tools and Best Practices

Thankfully, while it's easier for threats to make their way through your defenses, the defenses put into place by businesses are much more substantial than in previous years. A Unified Threat Management (UTM) solution is easily the most comprehensive security tool on the market today, combining well-known methods of cybersecurity into an easy and accessible package. This includes a firewall, antivirus, spam blocker, and content filter to minimize the chances of threats manifesting on your network in the first place, as well as solutions to mitigate threats that do make it through your defenses. This can be further augmented through industry best practices that dictate how and when to share data.

To learn more about how your organization can take advantage of security solutions, reach out to us at (800) 484-0195.

Share this Article!
http://bit.ly/2BdRFBz

Use VoIP To Build Better Business Communications

There aren't many technological assets as important for the modern business than its communications solutions. The telephone, while being one of the oldest currently-utilized communications systems available, is still the most utilized. Today, we will look at business telephone systems and why choosing Voice over Internet Protocol simply makes sense for your business.

VoIP, either hosted locally or in the cloud, can bring any business a solid ROI because you use a resource that your company already has in place, your Internet connection to send and receive calls.

Out With the Old

If you're still relying on the traditional telephone system of yesteryear, you could be making your job more difficult than it needs to be. Businesses that still use traditional telephone systems have limited ability to grow and expand. Adding new users can mean adding new telephone lines and extensions--a process that's not necessarily easy.

The most logical course of action is to figure out how your business can get away from traditional telephone providers. After all, these are the same organizations that are known to provide bundles filled with services you don't need. Plus, running telephone wires and adding new users or phone numbers can be quite the hassle, and one that you don't have to worry about with a more dynamic solution.

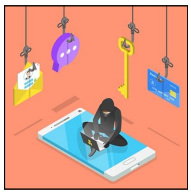
In With the New

With great new features that put traditional telephony to shame, VoIP is a sustainable and investment-worthy technology for any business, small or large. VoIP uses your Internet connection rather than a traditional telephone line to function, giving any device with a VoIP application and an Internet connection the ability to work like a phone. Since VoIP only needs your Internet connection, you're essentially eliminating an expense from your budget.

To learn more about how your organization can benefit from VoIP, reach out to us at (800) 484-0195.

Share This Article!
http://bit.ly/2UFwsJr

As 2018 Ends, Mobile Cyberthreats Won't



Mobile devices have made conducting business much more convenient, as the right application can allow transactions to be made from anywhere you may be reading this blog. However, this increased accessibility has come with a price - threats to mobile security - which requires any business to be aware of the state of cybersecurity, especially concerning mobile devices, now and in the foreseeable future.

The Now:

It's the holiday season, which means that many will find that themselves traveling, either to visit family and friends or to seek out more agreeable climates. However, business being what it is, many will also still be trying to get work done during their travels.

Thanks to the incredible capabilities of the mobile devices we have today, this is made much easier. A business that leverages cloud solutions offers mobile users an exceptional amount of maneuverability, and the popularity of Bring Your Own Device policies have made it so that the resources needed to accomplish work goals are never too far away. Yet, this access is a catch-22, as it also means that data can be easily lost, far from the business' location and the protections it should have in place.

Resultantly, there are a multitude of ways that a cybercriminal can come into possession of your data, either personal or professional. Fortunately, there are some ways to help prevent this from happening as well.

- **Public Wi-Fi is Too Public:** When out in public, you'll want to avoid connecting to public Wi-Fi networks when shopping or accessing sensitive information. We all know that hunting for the best deals is made much easier when you can look up prices online, but you'll want to use your data instead. Public signals make hackers' jobs that much easier with their typically insufficient security standards.
- **Charity Good, Charity Scams Bad:** These phishing variants can come in via all avenues, but very commonly take the form of calls and text messages. A scammer pretends to be working for some charity, but in actuality, just wants your money and data for themselves. If you receive what you believe to be a charity scam attempt, you'd be wise to do some research into who is asking for it before handing over your data, payment information or otherwise.
- **Charge Carefully:** Whether you're at the airport during a layover and trying to eke a few more minutes out of your device, or you're deal-hunting online as you're wandering the mall, you need to make sure you're being smart about how you're keeping your device charged. Many attackers will hide attacks in charging stations, waiting to strike whomever connects.

The Then:

Of course, these hacks and threats aren't going to end after the holiday season is over. Moving into 2019, the above threats are still going to be just as large of a problem, along with many other threats. Much of this will be in part due to our reliance on mobile devices.

Hackers will still be able to intercept data exchanged on an unsecure network, more devices will become outdated and insecure (you may want to peek at some of those holiday deals for an upgrade), and yes, more people will enable these threats through uninformed decisions...

Read the Rest Online!
http://bit.ly/2BiHewm

We partner with many types of businesses nationwide, 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.

Abraham Brown
CEO

Tech Trivia
Time Magazine named the computer the "Man of the Year" in 1982.

Global Tech Solutions

2964 Nostrand Avenue
Brooklyn, New York 11229
Voice: (718) 360-2000

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

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