GLOBALTECH
SOLUTIONS

TECHMinutes
October 2018

Providing IT Solutions Nationwide

This Issue:

Know Your Tech: A/B Testing

A key component to effectively attracting your audience is to better understand their preferences. Even the most seemingly insignificant change, like changing the color of the buttons on your website, can have a major impact on how effective your materials are. Fortunately, through a process called A/B testing, observing the impact of these changes is somewhat straightforward.

A/B Testing, Defined
Running an A/B test is the…

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

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

In October, we join IT professionals from all over the U.S. to celebrate National Cybersecurity Awareness Month.

In promoting the strategies and practices that individuals, businesses, and other organizations utilize to protect their interests from the ever-growing number of threats found on the Internet, we work to advance the pervasive protection of data and information systems.

What Exactly is Protecting Your Online Transactions?

So, like millions of others, you've taken to making purchases and paying your bills online. The speed of delivery, the ease, and the convenience are truly remarkable considering where we were just a couple short decades ago. But, have you ever considered what exactly makes up the technology that protects your personal information--and your money--from theft while operating on the Internet? We'll take a short look at the technology that is constantly working to protect your Internet transactions.

The main technology used by online retailers (or any other business that accepts payment through the web) is encryption. Encryption is the process of converting the manner in which data can be interpreted. All this means is that if you have the simple message "Hello", encryption will change it to something that makes it completely unreadable by any system that doesn't have the encryption key. This provides a data protection for any data sent through and encrypted channel.

There has to be more than that hasn't there? I mean, over a billion dollars a day is spent on the Internet on retail sales, and the only thing protecting all that data is one thing? The

(Continued on page 2)

Cybersecurity Industry Update

2018 will see many changes to the way that businesses manage security, but unlike 2017, when many companies suffered from large high-profile data breaches, the trends aren't as obvious as you might think. We'll go over some of the potential trends we could see as a result of 2018's security developments and why they matter to your business.

Ransomware Will Continue to Be an Issue

While ransomware isn't as high-profile of a threat as it has been in the past, it still continues to be a problem that could create dangerous situations for your business. Just the threat of it being out there is enough to make the average business question their security. Unfortunately, ransomware is one of the more difficult threats to protect your business from, as it can make its way into your office through a tricky medium--Internet of Things devices.

IoT devices are on the rise even today, and with so many devices being connected to the Internet, it's inevitable that one of them will become infected by some type of malware (perhaps even ransomware) and bring it to your office, where it can populate your network. To secure your network from IoT devices, you'll have to have a discussion with your team

(Continued on page 3)

Is Email Actually More Trouble than It's Worth?

If there is any solution that is a constant across businesses, it would have to be the use of email. This also means that the risk of threats coming in through an email solution is also present in businesses of every shape and size. How is this shaping our approach to security now, and how will this shift in the future?

A Prevalent Threat, Now and Tomorrow

While messaging applications and other forms of communication are largely phasing email out where personal use is concerned, it is alive and well in the business world. Yet, while it makes for a very useful tool, it can also make organizations vulnerable. Email has been repeatedly identified as the initial touchpoint for 90 percent of security breaches (96 percent according to the 2018 Verizon Data Breaches Investigation Report), yet a survey conducted by email security firm GreatHorn showed that this isn't being communicated between IT security professionals and users.

The results of this study effectively demonstrated that a full 66 percent of those interviewed for the study saw spam and junk messages, as the biggest threat facing them, but if the responses from the security professionals were isolated, that number drops to lower than 16 percent. This means that approximately 85 percent of security professionals see other factors as larger threats to an email user, while most users assume spam is the worst thing that their inbox will see.

This discrepancy only becomes more disconcerting when the variety of attacks that leverage email in some way is considered. Sure, there's spam to contend with, but there's also the propensity that email has to deliver malware, along with the human vulnerability to social engineering and phishing. Some attackers prefer to "join" their targeted company, using business email compromise and spoofing to benefit financially at the company's expense.

Another concerning statistic to consider: the average professional's work email open rate is 100 percent. This means that all of those users will not only be blind to threats that don't look like spam, they are effectively guaranteed to open these messages as well. From there, it isn't too much of a stretch to think that they might click on a link they shouldn't, or open a potentially malicious attachment.

How Companies are Securing Themselves

Naturally, firewalls and yes, spam filters, will always be useful in stripping your company's inboxes of some threats. However, other threats need a different approach to be taken. This has resulted in a few different circumstances.

First, security companies have needed to add extra value to their services in order to stand out from their competition, because if everyone is offering the same antivirus and spam protections...

Read the Rest Online!
http://bit.ly/2Nt5J2e

What Exactly is Protecting Your Online Transactions?

(Continued from page 1)

answer to that is a resounding no. Encryption is a must-have tool, but overall, the strategies that keep you going online--the ones that will protect your assets--come from you. Here are four things you can do to ensure that e-commerce and e-payment don't become e-mergencies.

Change Your Passwords

This one is simple, but effective. Every account you have has some type of password. Most accounts today have two-factor authentication with some sort of biometric or authorization option that provides an additional level of security. The first level of security, however, is always the password. If you change your password frequently, there will be a major reduction in the chances that your account will be compromised. The National Institute of Standards and Technology (NIST) has changed their recommendations about how to effectively utilize passwords. At one time, it was en vogue to utilize a string of random numbers, uppercase and lowercase letters, and symbols, but too often the unique string of characters were too difficult for the user to remember, repeatedly locking people out of their accounts. Today, they suggest using phrases of random words that you can remember, or to use a password manager.

Shop On Secure Sites

When shopping online, it is important that you are shopping behind technology designed to secure your financial information. This can be easily ascertained just by looking at the protocol bar in the browser. If the URL of the site you are shopping on doesn't have the protocol "https", the website you are on does not have a security certificate, and you are risking your information being exposed by entering personal or financial information into fields on that page.

Utilize Safe Payment Methods

If a company has an e-commerce store on their website, there is a pretty decent chance that they accept several secure methods of payment. One extremely popular option is to use PayPal. PayPal is a third-party payment site that securely holds people's financial information for instances where they want to purchase something online. PayPal...

Read the Rest Online!
http://bit.ly/2NkiSL1

Cybersecurity Industry Update

(Continued from page 1)

members about data access best practices, as well as mobile device practices that minimize their likelihood of exposing themselves to potential threats. You can also round out your network security by implementing a Bring Your Own Device (BYOD) policy for your business in which employees who want to use their personal devices for work purposes must subscribe to specific practices, including device monitoring, remote wiping, and more.

Artificial Intelligence Will Plague Businesses

Artificial intelligence has been used by security professionals to make considerable leaps and bounds in network security, but it's thought that in the near future, hackers will be able to leverage it to their own nefarious ends. With security software constantly learning and adapting to specific scenarios, it makes sense that in order to combat these types of protective solutions, hackers would want threats that can do the same.

A.I. can be used to collect information on specific businesses from all parts of the Internet, be it support websites, directories, and so much more. Artificial intelligence threats can then use this information to methodically create a targeted attempt at breaking down your organization's defenses. If you're not concerned about the future of A.I. in regard to cyber threats, you should be, as it represents a dangerous trend toward intelligent threats undermining the best efforts by security professionals at keeping up with the industry.

GDPR Will Shake Things Up

As of this past May, the European Union's General Data Protection Regulation, or GDPR, is in full effect. While this does aim to help protect users' data privacy, it presents some complications for businesses. Since these organizations aren't allowed to store information (like cookies) without the user's consent, it's expected that at least a couple of businesses will fail to adhere to these new regulations.

According to Forrester, it's expected that 80% of businesses will fail to comply with these new regulations. The reasoning, however, is a bit odd. 50% of these organizations will actually choose not to comply, citing the reason as the fact that actually complying with these new guidelines will cost more than the fines associated with failure. Whatever the case, it's likely that this will have an impact on user security and data privacy in the future.

Don't let your business fall behind the times in terms of network security. To learn more about how you can protect your business, reach out to us at (800) 484-0195.

Share this Article!
http://bit.ly/2Nmi0Wb

You'd Be Surprised How Many Disasters Aren't Caused By Disasters

Disasters happen. This is a fact of life, and no amount of hoping can help your business dodge one. You might be able to predict weather anomalies that can cause damage to your organization, like a flood or a fire, but some of the most dangerous disasters out there are impossible to see coming--namely, threats to your organizational security, both internal and external.

We'll discuss how your organization can secure itself from cyberattacks and user error, both major issues for security and business continuity.

> ***"We'll discuss how your organization can secure itself from cyberattacks and user error, both major issues…"***

Security Threats and Data Breaches

At first glance, you might forget that cyberattacks and data breaches are also a type of disaster--not necessarily the natural kind, but a man-made one that can be just as devastating as a flood or fire ever could be. Think about it like this. If your office is hit by a natural disaster that destroys the infrastructure, you're left with time when your business isn't working as intended. Your employees can't do their jobs. Your clients can't contact you. You have a big mess to clean up. The same can be said for a hacking attack. Nobody can be allowed on the network until it's been secured again, and in the meantime, the total costs of downtime rise.

The most common cause for cyberattacks include poor network security practices and poor employee practices in general. The former can be addressed with a firewall, antivirus, spam blocking, and content filtering solution, but the latter is a bit more difficult to address.

End Users Complicate Things

If your employees aren't properly trained in how to prevent disasters, they could become a problem for your business' long-term sustainability. Let's imagine that you have an employee…

Read the Rest Online!
http://bit.ly/2x1Mm5X

Hackers Target Major Sporting Events

There are literally billions of sports fans in the world, and the popularity of these events brings in big money; and big money typically attracts hackers. Using all types of methods, there has been a history of hacking in almost every sport. Today, we take a look at some of the most famous hacks that have shaken up the sports world.

The World Cup

The FIFA World Cup is one of the, if not the, most popular sporting events in the world. Held once every four years, it attracts the attention of billions of people. Since the event is held every four years, it gives the host city a lot of time to get ready for possible hacker attacks. In fact, each new venue spends years and tens of millions of dollars ramping up on their cyber security.

The 2018 event held in Russia proved to be one of the most successful insofar as there wasn't a major hack of the tournament in any way. It's not a coincidence that typically state-sponsored Russian hackers are well known to be at the forefront of a lot of the major international sporting hacks. Fans that visited Russia from abroad during the World Cup were warned (mostly by their own governments) that they needed to be diligent not to fall into any tourist traps that would leave their cyber welfare in the hands of the thriving ecosystem of hackers that call Russia home.

Previously, in the 2014 World Cup in Brazil, the World Cup website was taken down by a distributed denial of service (DDoS) attack and thousands of visitors had their data breached through sophisticated phishing attacks. Each World Cup, especially the next one that will be held in the Middle East (Qatar) for the first time, is a goldmine for hackers.

The Olympic Games

International competitions like the Winter and Summer Olympic Games grab the eye of world for a couple of weeks. Unfortunately for athletes, coaches, and fans from all over the world, they also catch the eyes of hackers. Again, since these events are held every four years there is a long time for administrators to get ready, but that doesn't stop those inside the host cities (or often outside of them) from trying to get over on the hundreds of thousands of people that show up to watch the events.

At the past Winter Olympics, held in Pyongyang, South Korea, the opening ceremonies were hacked by what turned out to be a Russian hacking collective. The hack caused delays in the festivities and infiltrated the games' website, so administrators, fearing significant data loss, took down the website. Initially they had masked the attack as coming from North Korea, but it didn't take long for professionals to ascertain that the hacks were retribution for Russia's prohibition from the games as a result of a decade-long antidoping policy that found state-sponsored use of performance enhancing drugs; a revelation that many had suspected for decades.

While local hackers spoofed Wi-Fi and targeted athletes and guests during the 2016 Summer Olympics held in Rio De Janeiro, Brazil, Russian hackers from "Tsar Team" and "Fancy Bear" were busy hacking into the Olympic databases to gain access to athletes' personal information. They subsequently have released some of that information, including information about gold medal gymnast Simone Biles, and tennis legend Venus Williams.

NFL

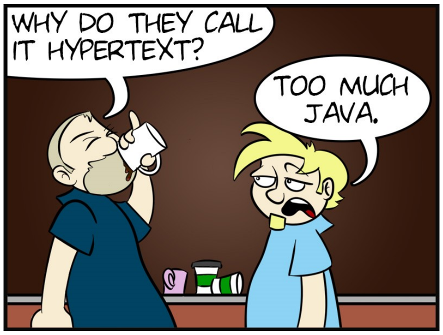
In the United States, it doesn't get much bigger...

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

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
The Most Expensive Mobile Number Sold For $2.7 Million!



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