Simplicit Tech News

What's New

Is your company still using **Windows 7 and/or Server 2008**? See the list of potential threats that your company is facing right now. See **page 3** for details.

We are running a **FREE iPad** promotion! For more details, see bottom of **page 2** of this newsletter.

Read some information on **high-profile security breaches in 2019** on **page 3.**

Beware of **phishing emails** related to Kobe Bryant tragedy. See **page 4** for helpful tips to avoid being a victim.

February 2020

This monthly publication provided courtesy of **Eyal Bishri**, CEO of Simplicit Technologies.

Our Mission :
"Helping people by simplifying their use of technology"

If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses either overlook cyber security or just don't put enough money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has insufficient IT security – or the business does have some security but its users **lack the training** on how to handle the risks out there.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want (passwords, information on deals, W2/1099 info etc). All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data (**Sony Studios** in 2014, **Marine community clinic** in 2019 to name a few examples).

Continued from pg.1

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability. But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, cyber Security training, mutli-factor-authentication, encryption, cyber security insurance and working with a dedicated IT company that's dedicated to security. There are so many options available to secure your business.

"The reality is that cyber - security should be a normal, everyday part of any business."

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?" When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

Help Us Out and We'll Give You a Brand-New iPad as a Token of Our Appreciation

If you're happy with **SimplicIT** services we want to give back to you. A huge part of our goal is to grow the **SimplicIT** family and offer our services to other companies. Finding an IT provider that is the right fit can be difficult for any organization. When you refer our services, they will get the peace of mind for choosing a trusted IT provider. When our services are recommended by you, we want to make sure that you're rewarded for helping our family grow.

Simply refer any company with 10 or more computers to our office to receive a **FREE computer network assessment**. If the company signs a 12 month contract, we will **rush YOU a FREE iPad. If they don't sign a contract, we will give you a $25.00 Amazon gift card as a token of our appreciation.**

Simply call us at **800-245-5210** or e-mail us at **contact@simplicit365.com** with your referral's name and contact information today!

End of Life Windows 7 and Server 2008

If your organization is still running Windows 7 on computers in your office or running Windows Server 2008, you need to know about the **dangerous security threat to your organization is facing right now.**

Microsoft has officially retired support on the Windows 7 operating system and Windows Server 2008 R2 last January 14, 2020.

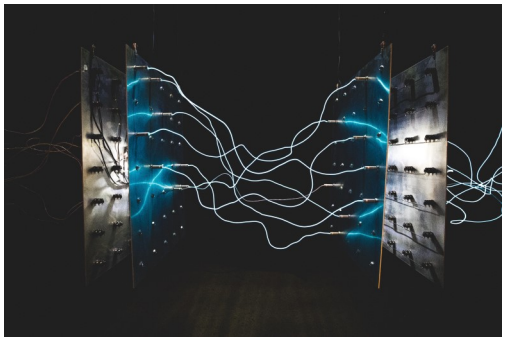
Any computer or server with these operating systems installed **is completely exposed to serious hacker attacks** aimed at:

- **Taking control of your network**
- **Stealing company data**
- **Crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with**

Give us a call now **at (800) 245-5210** and we will put together a customized migration plan and show you how to painlessly upgrade your old Windows Server 2008 and Windows 7 machines.

Frightening Data Breach Facts

Data breaches occurs almost every day, disclosing our credentials, banking, credit card information, and other sensitive data.
The sad part is, majority of us do not understand the impact of the situation until it gets to a point where it affects us personally through identity theft or other malicious activities.



The amount of identity related crime is exploding. In a recent study, its is believed that **there is a new victim of identity theft every 2 seconds in the United States alone.**

Here are the common cyber-attacks used in data breaches:

1. Ransomware- A software that locks down the computer or threatens to publish the victim's data unless a ransom is paid
2. Malware– Otherwise known as "malicious software", it is designed to disrupt or gain unauthorize access to the system. An example of a malware attack is a warning message that pop-up, and convinces the victim to download a software. The software then steals data and hijack computer functions.
3. Phishing- This involves sending fraudulent emails that appear to be from a reputable company, with the goal of tricking victims into clicking on a malicious link or infected attachment, with the goal of stealing financials or sensitive information.
4. Denial of Service (DoS)- A denial-of-service attack is a cyber-attack in which the attacker makes a machine or network resource unavailable to its intended users by disrupting services of a host connected to the Internet. One of the most common target of these type of attacks are banks

Here is a list of high-profile data breaches in 2019 from *Identity Force*:

Microsoft - Confirmed a data breach of its non-corporate email services, such as @msn.com and @hotmail.com. The breach, which lasted from January 1 to March 28, 2019, allowed hackers to access email accounts by misusing Microsoft's customer support portal .
Facebook- An unprotected server containing over 419 million records of Facebook users was discovered, giving hackers access to Facebook users' unique ID and phone numbers.
Disney+- Users of the newly released Disney+ streaming services were locked out of their accounts after being hijacked by fraudsters. Disney+ members' login credentials, including usernames and passwords, were found up for sale on the Dark Web starting at $3 per record.
Fortnight- On January 16, 2019, a flaw within the popular video game Fortnite exposed players to being hacked. The game has 200 million users worldwide, 80 million of whom are active each month.

Here are some action plans to utilize in order to help prevent data breaches in your organization:

Automate Processes- You can implement automated programs. An example is a system that routinely examines passwords and reminders to change them periodically or set-up 2 Factor Authorization as a log-in requirement for employees. Also, set-up email and website filtering programs. In that way, there's an extra protection in place to prevent employees from unknowingly clicking on a fraudulent websites or malicious emails.
Staff Education and Training-Making employees aware and training them is a very important preventative tool in keeping a company safe from a possible data breach or cyber-attack.
Patch Management -Patching vulnerabilities in computer software is vital, especially considering that most successful computer attacks exploit well-known vulnerabilities for which patches exist.
Regular Audits & Assessments- Schedule system assessments and audits regularly. Periodically scan contents of all system in the network to capture threats and have all your bases covered to prepare of cyber-attacks.

From:

Simplicit Technologies
22222 Sherman Way
Suite # 200
Canoga Park, CA 91303

Postage

To:

Beware of Phishing Email Regarding Kobe Bryant Tragedy

Recently, news broke that sports icon **Kobe Bryant** and his daughter Gigi died in a helicopter crash. **Scammers** are going to take advantage of this shocking and tragic celebrity death in a number of ways. Be careful if you receive or see anything related to Kobe Bryant's death. These includes emails, hyperlinks, attachments, social media, texts on your phone etc. Please be vigilant before you click!

Here are some helpful tips from the Better Business Bureau:

- **Look at the sender's email address** before clicking on anything in the email. If it's someone you're not familiar with, delete it.

- **Don't click links in any email** unless you are positive they go to a reputable address. Hover over the link to see where it will take you.

- **Don't take the bait**. Stay away from promotions of "exclusive," "shocking" or "sensational" footage. If it sounds too outlandish to be true, it is probably a scam.

- **Hover over a link to see its true destination**. Before you click, mouse over the link to see where it will take you. Don't click on links leading to unfamiliar websites.