Holzsager Technology Services, LLC
P.O. Box 535
Fair Lawn, NJ 07410-0535
(201) 797-5050
info@tech4now.com

Volume 13, Issue 9

September 2021

**Celebrating over NINETEEN YEARS of Service and Satisfied Customers!**

**"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"**
**Fred Holzsager,**
**IT Director**
**Holzsager Technology Services**
**and**
**Publisher of**
***The Tech Insighter***

## Inside This Issue



**Snapple Real Fact #720**
"Fresh apples float because 25 percent of their volume is air."

**GO GREEN**: To help save a tree, please send us an e-mail to request electronic delivery. Kindly submit your request to **subscribe@tech4now.com**

# The Tech Insighter

"Insider Tips To Make Your Business Run Faster, Easier and More Profitably"

## Five Ways Your Systems Can Be Breached and Suggestions to Remedy Some Sources

When it comes to business IT security, many small- and medium-sized businesses like yours often struggle to protect their systems from cyberattacks. One primary step is to be aware of online threats. Here are five common ways your systems can be breached.

1. **You are tricked into installing malicious software**

There are countless ways you can be tricked into downloading and installing malware. One is by downloading software from torrent websites. When you visit these sites, you are told to download software in order for the site to load properly. Once downloaded, the malware that came with the software infects your system. In other cases, hackers send emails with a malware-infected attachment.

Fortunately, there are steps you can take to avoid accidentally installing malware:

*** Never download files from an untrusted source**. If a website is asking you to download something, make sure it's reputable and reliable. Double check the URL of the website as well, as hackers can spoof legitimate websites and use similar but slightly altered URLs, such as "www.g00gle.com" instead of "www.google.com." *If you are unsure, it's best to avoid downloading and installing the software*.

*** Always look at the name of the file before downloading**. A lot of malware is often deliberately given names similar to those of legitimate files, with only a slight spelling mistake or some unusual wording. *If you are unsure about the file, then don't download it. If you know the sender, you may contact them to verify the file's authenticity.*

*** Always scan a file before installing it**. *Use your*

*(Continued on page 2)*

## "We Love Referrals" 2021 Offer

**Keeping with the spirit of helping others,**
**if you refer a business to us and they become our customer,**
**we will donate $100 to your favorite charity.**

**At Holzsager Technology Services, we believe that referrals are the greatest form of flattery. By recommending your partners, associates, or professional contacts, you can help them enjoy worry-free IT and support a worthy cause of your choice!**

**For more information, please see our website at www.tech4now.com/we-love-referrals, contact us by phone at 201-797-5050**

## Quotations

*"Motivation is the art of getting people to do what you want them to do because they want to do it."*
**—Dwight D. Eisenhower**

*"Open your arms to change, but don't let go of your values."*
**—Dalai Lama**

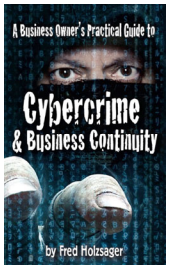
*"Change before you have to."*
**—Jack Welch**

***"**We may give without loving, but we cannot love without giving."*
**—Bernard Meltzer**

*"Don't judge each day by the harvest you reap but by the seeds that you plant."*
**—Robert Louis Stevenson**

*"If we have no peace, it is because we have forgotten that we belong to each other."*
**—Mother Theresa**

### Read Fred's Book!




**If you would like to have us speak to your organization and give away some free copies to attendees, give us a call.** For more details on the contents and how to get your own copy, please visit our special web page at ***www.tech4now.com/cybercrime***

***"We make all of your computer problems go away without the cost of a full-time I.T. staff"***

***Ask us about our fixed price services HTS Insight Hassle-Free Agreements—Computer Support at a flat monthly fee you can budget for just like rent!***

# 5 Ways Systems Can Be Breached

*(Continued from page 1)*

*antivirus scanner to check downloaded files before opening them.*

*** Stay away from sites with torrents, adult content, or those that stream pirated videos**. These sites often contain malware, so avoid them altogether.

2. **Hackers obtain admin privileges**

Many users are logged into their computers as local administrators. Being an administrator allows you to change settings, install programs, and manage other accounts. The problem with this is that if a hacker manages to access your computer with you as the admin, they will have full access to your computer. This means they can install other malicious software, change settings, or even completely hijack the machine.

Even worse is if a hacker gains access to a computer used to manage the overall IT network. Should this happen, they can control the entire network and do as they please.

*To avoid these unfortunate situations, limit the admin role only to users who need to install applications or change settings on their computers. Installing antivirus software and keeping them up to date, as well as conducting regular scans, will also help reduce the chances of being infected.*

3. **Someone physically accesses your computer**

Your system can also get infected with malware or your data can get stolen because someone physically accessed your systems.

Let's say you leave your computer unlocked when you go out for lunch. Someone can just walk up to it and plug in a malware-infected USB drive, which can infect your system. They can also manually reset the password, thereby locking you out.

*An easy way to defend against this is to secure your computer with a password. You should also lock, turn off, or log off from your computer whenever you step away from it. You can also disable drives like CD/DVD and connections like USB if you don't use them*. Doing so will limit the chances of anyone using these removable media to infect your computer or steal data from it.

4. **Someone from within the company infects the system**

A disgruntled employee can compromise your IT systems. They can do so much damage such as deleting essential data or introducing highly destructive malware.

The most effective way to prevent this, aside from ensuring your employees are happy, is to limit access to systems. For example, you may find that people in marketing have access to finance files or even admin panels. *Revoke unnecessary access rights and ensure that employees only have access to the files they need.*

5. **Your password is compromised**

Passwords are typically the main verification method businesses use to access their accounts and systems. The issue with this is that many people have weak passwords that are easy to crack. To make matters worse, many people even use the same password for multiple accounts, which could lead to a massive breach.

*It is therefore important to use strong and different passwords for your accounts. It's best to also utilize multifactor authentication, which requires users to present more than one way to verify their identity such as a password plus a fingerprint or a one-time code.*

If you want to learn more about securing your systems, contact us today.
*—Published with permission from TechAdvisory.org.*

**Additional thoughts to help you protect yourself and your systems.** Too many businesses refuse to spend money on the tools necessary to protect themselves. The misunderstanding is that EVERYONE is a potential target. Although larger businesses are frequently on the radar of the news and have high profile breaches, taking the stance that it won't happen to you is naïve.

Take the measures that you can before you discover you have been attacked. Use strong passwords, use multifactor authentication, get yourself a secure password manager (not the one in your browser), and do consider strengthening your network and perimeter with tools your IT professional may recommend. They do it to keep you safe, so please give it more thought.

> **"An easy way to defend against this is to secure your computer with a password."**

# The Best Tips For Training New Hires

The hiring process is stressful. You put in a considerable amount of work training someone for their role and hope they'll become a responsible employee. As difficult as this process is, however, you can streamline it with these tips.

**Create A Scalable Guide For New Hires To Follow**

Document all the responsibilities of the role and put them together in a concrete guide for new hires. This documentation will work especially well for visual learners, for recent graduates who are used to learning through guides and for non-native English speakers. In truth, though, anyone can benefit from having a set of principles to refer to.

**Draw Examples From Real Life**

When training someone in what to do in a specific situation, provide actual examples of what you did in that particular situation in the past. New hires will have an easier time completing their work if they have a previous example that shows them what to do.

**Develop Your Interview Skills**

Like great teachers, great leaders ask great questions to surmise if new hires are understanding their role. This will ensure that nothing gets lost in translation throughout the onboarding process.

# Wordplay

This month, we return to wordplay, again, compliments of my little brother. Enjoy the quips!

- The fact that Kansas and Arkansas are pronounced differently bothers me way more than it should.
- You can drink a drink, but you cannot food a food.
- The word "queue" is just a Q followed by four silent letters.
- Why are Zoey and Zoe pronounced the same, but Joey and Joe aren't?
- If your car is running, I'm voting for it.
- Frog parking only. All others will be toad.
- I hate telling people I'm a taxidermist. When they ask what I do everyday, I say, "Y'know, Stuff."
- I want to grow my own food, but I can't find bacon seeds.
- This is my step ladder. I never knew my real ladder.
- My wife said, "I never listen to her," or something like that.
- Now that I've lived through an actual plague, I totally understand why Italian Renaissance paintings are full of naked fat people laying on couches.
- Don't use a big word when a singularly unloquacious and diminutive linguistic expression will satisfactorily accomplish the contemporary necessity.
- They're excavating the largest known dinosaur tibia to date. Apparently, it's a real ...shindig.
- What happens if you get scared half to death twice?
- Lockdown can only go four ways. You'll come out a monk, a hunk, a chunk or a drunk. Choose wisely!
- What time is it when you see cows lying down in a field? Pasture bedtime.
- I wouldn't date a pediatrician, they have little patience. Nor a cardiologist, they may discover my heart isn't in the right place.
- I was watching an Australian cooking show and the audience clapped when the chef made meringue. I was surprised, Australians normally boo meringue.
- Bread is like the sun. It rises in the yeast and sets in the waist.
- Do people in Australia call the rest of the world "Up-Over"?
- Lumberjack's name: Tim Burr

# Quick Tech Productivity Pointers

Over the years, we have reminded you how vital it is for you to practice **password hygiene**. Too often, we hear of compromises and breaches at both large and small companies due to the lax attention given to poor password usage.

### What is a bad password?

First of all, a password represents your *key to the kingdom*. Just as you would lock the door to your home (which houses your personal prized possessions and family), you wish to protect and safeguard the content within. Well, the same is true for your electronic accounts. *Think about it for a moment...*, if you were to put a screen door on the front of your house without a lock, the door may limit access on a minor scale, mosquitos may be blocked and , perhaps, a random rodent, but any individual could readily gain access. In the days of honor and righteousness, this may have sufficed, but nowadays, you have a sturdy door with a lock(s), bolts, and an alarm system (often on the windows, too!). Your password works the same way—it limits entry to those authorized. The thought to ponder is "Do I have a ***screendoor*** password or an ***alarmed house*** password?"

### Consider the following...

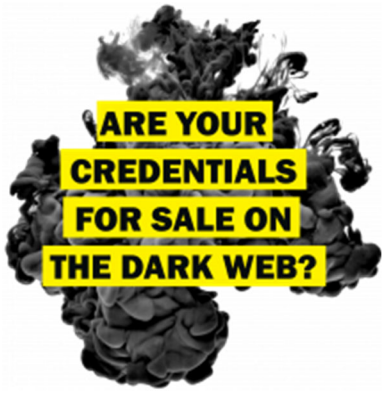
Is your password ***complex***? Does it use...
—***upper and lower case letters***?
—***numbers and symbols***?
—***personal details*** that are easily guessed?
—***reused passwords*** modified by changing one or a few characters?
Do I have my important accounts (*i.e.*, banking) protected using the same code as those that I may use for Facebook or some random account?
Is it easily guessable based on a dictionary *attack*?
[A dictionary attack is when the attacker uses a computer to apply words and phrases as the password to guess the value of your actual code. It is also referred to as a *brute force* method.]

### "Do I feel lucky? Well, do ya punk?"

Dirty Harry asked a simple question that should make you squirm if you don't feel lucky or are not sure about your immediate decision. So, how does a person keep track of all those codes? In a 2017 report from *LastPass*, it was indicated that the average business employee must keep track of 191 passwords. Keep in mind, that may or may not have included personal accounts, so to be fair—***could you reliably record and track about 200 complex passwords for all of your different accounts?*** How well do you think you would fare if you had them all jotted down in a notebook or on Post-it notes™ peppered around your home and/or office? Would that be a successful implementation? Do you think that would represent a secure method to protect your *keys to the kingdom?*

### A solution is at hand

You may have seen a security video that told you to protect your passwords or you may have signed an employee agreement to keep all your passwords secure, but do you have a plan? Keep in mind, 81% of confirmed data breaches are due to passwords. So, *what can you do*? Have you ever considered using a Password Manager? Password managers such as LastPass, DashLane and Keeper provide a facility for you to easily and reliably maintain and retrieve your passwords when you need them, where you need them. They enable you to store them in a cloud-based secure repository that is available on your desktop, browser and smartphone based on you using a complex MasterPassword and, optionally two-factor authentication. As you visit a site, it enables you to populate the credential fields with your passwords automatically. If you change them, it prompts you to update your list. It simplifies the process. If you are interested, we can provide LastPass Business to your organization. Additionally, for every license of the Business, you get 5 of LastPass Families. This way, you keep your passwords separate & secure. ***Call us***.




Find Out
with a Complimentary
Dark Web Scan

## Did you know...?

- Cyber-attacks have continued to grow in cost, size, and impact—causing 60% of SMBs to go out of business within 6 months of a cyber incident.
- Over 80% of data breaches leverage stolen passwords as the principal attack vector—often acquired on the *Dark Web*.
- Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement—but then, it's too late.
- To help keep your critical business assets safe from the compromises that lead to breach and theft, we are offering a complimentary, one-time scan with ***Dark Web ID***™ **Credential Monitoring**.

If you are interested in learning more about the risks involved in ignoring your password security, give us a call at (201) 797-5050 or visit our website at

https://www.tech4now.com/dwid
or www.tech4now.com/bullphish

Holzsager Technology Services, LLC
P.O. Box 535
Fair Lawn, NJ 07410-0535
(201) 797-5050
info@tech4now.com

**Celebrating over NINETEEN YEARS of Service and Satisfied Customers!**

**IT Solutions for YOUR Business!**

**Feedback & Suggestions…**

Is there a topic or feature you would like to include in a future issue? Opinions and feedback are welcome and encouraged. Please send us an e-mail or call our direct line.

**E-mail: info@tech4now.com**
**Phone: (201) 797-5050**

## 5 Reasons To Choose A Hosted VoIP Phone System

**1. COST SAVINGS**
**2. ANSWER CALLS ANYWHERE**
**3. ON-DEMAND SCALABILITY**
**4. WORLD-CLASS FEATURES**
**5. ENHANCED PRODUCTIVITY**

As a small business, you need every advantage to be as efficient and productive as possible. **Holzsager Technology Services** is proud to provide our clients with a cost-effective, feature-rich, world-class phone system that is easy to use and sure to enhance your business productivity.

**For more information order our:**

**FREE REPORT**
"The Ultimate Guide to Choosing the RIGHT **VoIP** Phone System"


**Contact us at**
**(201) 797-5050 or**
**www.tech4now.com/services/voip-phones**

## Services We Offer:

- ✓ **Hassle-Free IT** *powered by* **HTS Insight** Managed Services
- ✓ General Network Repair and Troubleshooting
- ✓ Onsite and Offsite Backup
- ✓ Disaster Recovery and Business Continuity Planning
- ✓ Virus Protection & Removal and Dark Web Monitoring
- ✓ Network Security and Online Employee Security Training
- ✓ Mobile and Hosted "Cloud" Computing
- ✓ E-mail & Internet Solutions
- ✓ Wireless Networking
- ✓ Spam Filtering and E-mail Archiving Solutions
- ✓ Storage Solutions and File Sharing
- ✓ System Audits, Network Documentation, and Dark Web Scans
- ✓ Voice over IP phone systems

**"We make all of your computer problems go away without the cost of a full-time I.T. staff"**
*Ask us about our fixed price service agreements—Computer support at a flat monthly fee you can budget for just like rent!*

*"Utilizing Holzsager Technology Services is a "NO BRAINER", always answers the phone right away and is very detailed in his work. Always takes the time to explain everything. Jumps right on and fixes your computer issues."* —**Randy Green**, *Valley Technical Sales, Inc.*, Ho-ho-kus, NJ

**September 2021**

# The Lighter Side...

*For Entertainment Purposes ONLY!*

**Just checking...**

*My wife yelled from upstairs and asked, "Do you ever get a shooting pain across your body, like someone's got a voodoo doll of you and they're stabbing it?"*
*I replied, "No...."*
*She responded, "How about now?"*

**At the Fruit Stand**

*An old man was selling watermelons. His pricelist read:*

**Watermelons: 1 for $3 or 3 for $10**

*A young man stopped by and bought 3 watermelons one by one paying $3 for each. As the young man was walking away, he turns around and says, "Hey, old man! Do you realize I just bought three watermelons for $9 instead of $10? Maybe business is not your thing." The old man smiled and mumbled to himself, "People are funny. Every time they buy three watermelons instead of one, yet they keep trying to teach ME how to do business..."*

**During the Power Outage**

*Due to a power outage, the house was very dark, so the paramedic asked Annie, a three year old girl, to hold a flashlight high over her Mommy, so he could see while he helped deliver the baby. Finally, Little Connor was born. The paramedic lifted him by his feet and spanked him on his bottom and he began to cry. The paramedic then asked the wide eyed 3 year old what she thought about what she had just witnessed. She quickly replied, "He shouldn't have crawled in there in the first place, spank him again!"*

————————————————————-

**After reading the the sentence, you are now aware that the the human brain often does not inform you that the the word 'the' has been repeated twice every time.**!

————————————————————-!

*An old lady was standing at the railing of a cruise ship holding her hat on tight so that it would not blow off in the wind.*
*A gentleman approached her and said, "Pardon me, madam. I do not intend to be forward, but did you know that your dress is blowing up in this high wind?"*
*"Yes, I know," said the lady. "I need both hands to hold onto this hat."*
*"But, madam, you are not wearing anything under your dress, and your privates are exposed!" said the gentleman in earnest.*
*The woman looked down, then back up at the man and replied...*
*"Sir, anything you see down there is 85 years old. I just bought this hat yesterday!"*