*Happy International Coffee Day!*

# microTECH Times

## Covered I.T. 24/7—Never Worry Again!

# 7 Cyber Security Threats Confronting Businesses Today And How To Protect Your Company

*A recent Cyber Readiness Report from Hiscox revealed that 7 out of 10 businesses failed in their cyber-readiness test. One of the major reasons for these failures was the inability to adapt to new threats. Take a look at the top 7 cyber security threats this year and what you can do to protect your company.*

**Top 7 cyber security threats to watch for.** While there will always be new threats evolving, it's important to stay abreast of the most recent threats. Here is a list of the top seven threats we've found that are impacting businesses today.

*1. Crypto-Malware:* This type of malware was developed by engineers to mine crypto currency using the processing power of other peoples computers. It isn't directly harmful for the computers but, can be disruptive because it takes the computer's processing power over so it can be used to gather more crypto currency.

*2. Banking malware:* Banking malware was created to gather financial information from users in order to sell it to other hackers or use it to steal money. This type of malware is extremely

dangerous because it often works in the background gathering information undetected by the user. A new strand of banking malware known as Emotet, is especially difficult because it is able to change or adapt avoiding detection and it replicates itself too.

*3. Ransomware:* Everyone has heard of ransomware attacks and it has been on the rise for years. Today, it has become a more notable threat for businesses because of its ability to lock down a computer until a ransom is paid. This disabling infection can be terribly disruptive for businesses. I am sure you've heard of Cryptolocker? This nasty strain infected over 200,000 computers and claimed over $3 million.

*4. Fileless malware:* If you've never heard this term, let me explain. It is truly a pain. Fileless malware is just what it

## What's Inside

## A Spoon Full Of Wisdom...

Life is short, lick the spoon.
—
What happens when a spoon and a fork get into a fight?
~ Civilwar
—
Ugh, kids these days. I'm a wooden spoon, no bike helmet, garden hose drinking survivor.
—
Man: "Doctor, whenever I drink my coffee, I get a sharp pain in my eye. What should I do?"

Doctor: "Remove the spoon from your cup."

## International Coffee Day!

*Coffee has become big business in America today like rock n'roll or blue jeans. September 29th, 2019 is International Coffee Day. So take a few moments to learn a bit more about where coffee really came from and ways to celebrate.*

*Where did coffee come from?* No one really knows exactly where or when coffee was discovered but, there are many stories about its origin. Coffee growing is a worldwide industry with heritage back centuries. One legend traces coffee to Kaldi who noticed that his goats would become energized and not want to sleep after eating berries form a certain tree. He reported these findings to a local monastery and the monks started using the berries to make a drink that helped them stay awake for the long hours of evening prayer.

*Coffee spread around the world.* Trade for coffee began on the Arabian Peninsula by the 15th century and soon after was

**microenterprises**

**234 N Broadway Ste 2,
Pennsville, NJ 08070**

**877-540-6789
www.microent.net**

# 7 Cyber Security Threats Confronting Businesses...

sounds like. There are no real files to look for because they do not exist within a hard drive. These attacks latch on to the RAM in a computer and only become visible when programmers activate it to retrieve information. This type of infection is what hackers use to scam people through ATMs and payment terminals.

### 5. Zero-day threats:
We all use software everyday. I am using software right now to write this newsletter and you have probably used at least three pieces of software today too. However, software is not perfect. There are always security holes that developers work diligently to fix or patch, but some hackers make it their goal to find such vulnerabilities and attack them. These vulnerabilities are called a zero-day threats. Once hackers identify a zero-day threat, they exploit the security loophole using it to deliver ransomware files and other infections to the computers.

### 6. Phishing e-mail:
Some of you may have fist hand experience with this one. No company is safe from phishing scams these days. To some degree phishing e-mails are targeting people who don't pay attention, but these nasty scams can lead to ransomware or trojan horse virus outbreaks within your network. McAfee reported that 97% of people really cannot tell the difference between a phishing e-mail and a legitimate message.

### 7. Advanced persistent threats (APTs):
These types of threats are premeditated infections. Cybercriminals who use APTs have generally watched and gathered information about their target for some time before infiltrating the network. The scary thing about APTs is that the infection can go on for years without the victim even knowing. Once the attackers have gathered enough information to dig into the network of choice, they work on capturing information and transmitting it back to their own servers.

### How can I protect my company?
I know this is a lot to take in. Honestly, there is no surefire way to be 100% protected these days. The good news is, there are a few key steps you can take to proactively prevent these malicious attacks. First off, be aware and inform your staff of the variety of threats that are hot today. The more educated you are about the possible issues, the more capable you will be in identifying them. Secondly, be sure you have e-mail filtering, antivirus and malware solutions in place. Install a firewall to help filter content and be sure your backups are working.

### Worried about protecting your company?
If you have any concerns at all. Give us a call. We will come onsite and conduct a  Network Security Audit to help you get a good picture of your current structure. After the audit, we will also provide our best recommendations to help you proactively manage these scary cyber security threats.

*Micro Enterprises LLC*

*877-540 -6789*

---

---

## Is Your Network Really Safe?

*Is your network really safe? I know, you'd like to say yes, but the truth is a lot of business owners aren't watching their networks like they should or staying on top of regular maintenance.*

*Here are a few steps* to make sure you're network is safe and secure:

● *Firewall:* Make sure your firewall's security settings are updated to make sure you're protected from the latest hacker attacks, worms, and viruses.

● *Run a virus scan* and remove spyware that may be secretly stealing your company's bandwidth, jeopardizing the speed of your computer systems, and embezzling confidential information.

● *Backup regularly.* Verify that your network's back-up system is working properly and accurately backing up all of the critical files and information you never want to lose.

● *Get the most up-to-date security patches.* Updating your systems is essential to make sure your files and clients personal information is safe. Stay on top of all of these things so you don't end up costing yourself a boat load of time, money or even clients.

---

# Funny, Fake, And Somewhat Believable Phishing E-mails

Beware of these e-mail phishing attempts seen lately:

∂ Funny and fake: The director of the FBI needs your help for wiretapping the Internet! Evidently something you did with a bank was legal but because there are scams on the Internet, you are going to be sent $10.7 million. Go figure. Obviously, the FBI director is not going to contact you personally by e-mail or otherwise. That's not how the FBI rolls. And, the rest? You gotta feel sorry for the FBI if they are trying to wiretap the whole Internet. That would be a huge project.

∂ Somewhat believable: E-mail claims you have undelivered e-mail on your Outlook Web Mail service. The e-mail lists supposedly undelivered e-mails for things like payments. If you click on any link you go to a fake Outlook Web App that asks for your credentials. As with all links, make sure you examine the address before entering information. Don't click on links in e-mails you don't know!

## International Coffee Day...

known in Persia, Egypt and Turkey. The mid-1600's New Amsterdam had their first taste of coffee and fell in love. By the 17th century there were over 300 coffee houses in London and in 1714 the mayor of Amsterdam presented a coffee plant to King Louis XIV of France. From there, a young naval officer brought a seedling from the kings plan over to America. This one seedling flourished and over the next 50 years was the start of over 18 million coffee trees.

*The hot beverage of choice...* The Boston Tea Party in 1773 marks a true shift from tea drinking to coffee. John Adams officially started the new coffee drinking trend. He considered tea drinking to be unpatriotic after the Boston Tea Party. Tea drinking declined significantly during and after the Revolution too.

*No matter how you take your coffee...* stop in a coffee house on September 29th to enjoy the experience of fresh roasted beans, the vibrant social atmosphere, and maybe even some local artists. Many coffee chains observe this fun day with special deals too. Over 22 countries around the world will be sipping their coffee with you.

## 3 Common Ways Virtualization Fails And How You Can Avoid These Costly Mistakes

*There are many advantages to server virtualization. However, sometimes what seems like a simple task, can go so dramatically wrong. Here are the most common ways virtualization fails.*

*What is virtualization?* Virtualization is a method of running a virtual instance of a computer system in a layer. Imagine a cake. A server can host layers of data cakes with security in between them just like frosting protecting one layer from another. These virtual instances can run multiple operating systems at the same time. This is especially useful when specialty software requires a specific operating system to function properly.

*The benefits of virtualization.* Virtualization offers improved system utilization, workload flexibility, and simplified management. Business owners generally love how much money it saves since they don't have to keep buying hardware to expand their resources.

*The most common ways virtualization fails...* There are still some problems that can arise if you do not use it properly. Virtualization is a solution that requires ongoing attention:
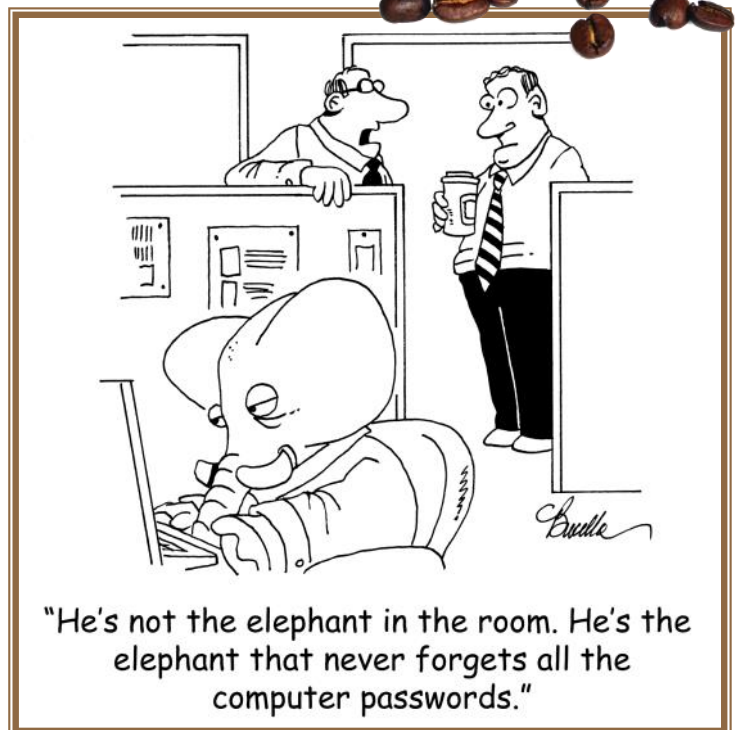
*1. Resource distribution issues:* Resource distribution problems often occur in the shift to virtualization and can be fixed by working on capacity planning with your service provider. You need to have someone to keep an eye on the servers to make sure that everything is properly distributed and when virtual growths happens you're equipped to adapt to that change.

*2. Poor management:* You should look at how virtual machines will be managed, who will be doing what, and what systems you're going to use. One of the optimal times to develop an overall management plan is when you're in a testing phase, before migration.

*3. Compatibility struggles:* Always make sure that your software is compatible. Compatibility issues can be very frustrating and difficult to solve. Virtualization service providers can help you with what will be compatible and what will not.

*Our best advice to avoid these three basic blunders.* Always keep a back up of your files. Just because they are stored virtually doesn't mean they can't get lost. Security should be the most important thing for any business. You want your files safe and secure to ensure your data and your client's data doesn't get out to anyone. Depending on the server provider, they may offer a service for this already. Remember, managing your virtualized server isn't a one time task, it should be ongoing. Conduct regular checks to ensure your resources are being allocated properly, machines are created and shut down properly, and apps and systems are updated regularly to keep your company safe.

*Ready to virtualize?* Have you been considering moving some of your shared resources to a virtual server for more flexibility? Or just not sure if virtualization is right for your business? Give us a call. We can take a look at your current environment and help you determine a plan to virtualize your resources and avoid these three most common failures.



"He's not the elephant in the room. He's the elephant that never forgets all the computer passwords."

## "We make all of your computer problems go away without adding additional full-time I.T. staff!"

**Ask about our fixed price service agreements — Computer support at a flat monthly fee you can budget for, just like payroll!**

## Inquiring Minds...

*Make Sure It's Really Tech Support.* Recently a hacker was sentenced to three years in federal prison for impersonating an Apple employee and scamming rappers and sports stars out of $322,000. It wasn't even much of an impersonation since the thief did not even have an Apple e-mail address. Nonetheless, he managed to get sports and music stars (his area of specialization) to fork over their usernames and passwords.

*Other celebrated tech support scams* include the many hacks of Quicken and other major software. Websites galore say they offer Quicken technical support. Quicken technical support is free, but many tech support sites charge big for services they may or may not render. Here are a few tips to avoid the fakes.

*Unsolicited phone calls or e-mail.* Thieves pose as support from a company and insist they have to run diagnostic tests on your computer. They may ask you to download a small screen share file so they can access your system and help you identify and remediate issues on your computer.

*Popup warnings.* These can range from update notices (You must update Flash now!) to apparent operating system errors with a phone number. Real computer errors do not include phone numbers. Don't click links or call phone numbers that appear in a pop-up.

*2019 Windows 10 Update Features.* This update has tools, apps, and features to help your business be more productive than before. It will also help you as the user have a better experience while you are working in Windows 10.

*There is a new light feature* that is great for those of you who do not like the dark mode. The way to set this up is to go to the Settings app, click on Personalization > Colors, then select the Light option from the "Choose your color" drop-down menu.

*The start menu is also new,* it looks a lot less cluttered too. The apps and shortcuts are now arranged in one column instead of two as it was previously. If you're using a Windows user account or computer, the number of pinned apps have been reduced and grouped together. This makes it easier to unpin them all at once.

*Uninstall some of those preloaded apps you'll never use.* Go to the Start menu and right-click on the app's shortcut, then select Uninstall. Don't worry, if you decide you want the app again, you can always get it from the Windows store for free.

*Cortana now has a separate box from the search box.* So, now you won't accidentally click Cortana when you're trying to search for something! Additionally, you can now see your most used apps, recent files, and activities along with options to filter search results by apps, documents, e-mail, and web results. This new update also offers an automatic backup folder for your computer if you have OneDrive setup. It allows you to specify which folder you want to sync to Microsoft's cloud storage service. In order to set this up, click the OneDrive icon on the right side of the taskbar, then go to More > Settings. On the AutoSave tab, click Update folders and choose the folders you'd like to automatically sync. Make sure your computer is up-to-date to take advantage of these great new features.

**microenterprises**

**234 N Broadway Ste 2, Pennsville, NJ 08070**

**877-540-6789**

**www.microent.net**