June 2019

microTECH Times

Happy Father's Day!

Covered I.T. 24/7—Never Worry Again!

Even Your Daddy Can't Save You From Data Loss So, Make Sure Your Cloud Storage Is Really Safe!

Gone are the days when your father would come home from the office with a huge stack of paperwork and file it in a bank box in the garage right along side the family photos and the lawn mower. Cloud storage has eliminated the need for printouts of everything for your business.

As businesses accumulate more digital documents, cloud storage has become essential, but is it really safe? Recent headlines involving data security breaches have created some doubt. A detailed look at the industry by the BBC reveals that large players, such as Amazon's Web Services (AWS), have more than 1,800 security controls. Dropbox uses a process called sharding which breaks a file into separate chunks and then stores those pieces in different places to avoid losses. Box, meanwhile, encourages users to send a link to the file to others that allow them to preview the content without actually downloading the document or image.

Cloud storage is more secure than local storage. Whatever the method, those within the industry contend that their methods are much more secure than storing files locally. In fact, the majority of the biggest breaches over the past few years, such as Target, have come from internal databases and not cloud-based storage. In general, storing your company data in an offsite location with a cloud provider will be safer and more accessible than an in-office solution.

Money doesn't grow on trees so do your homework. Many cloud providers nickel and dime you with migration fees, retrieval fees, additional back-up fees or even high usage fees. Be careful when you're shopping for a cloud solution for your business. Look for these key features to find a secure cloud service for your business:

- ***File Versioning:*** Many cloud providers don't offer additional versions of your file. Look for one that allows you to restore previous versions of your files if you need them.
- ***Automatic Synchronization.*** Keep your files updated regularly with automatic syncing. Just be sure you have the proper bandwidth require-

What's Inside

Dad Sayings

Here's a collection of Dad sayings for Father's Day. You could probably think of some too:

On business: Don't pull the trigger until you see the whites of their eyes

Upon leaving the house: Going to see a man about a horse.

On life: If you're gonna dance, you gotta pay the fiddler.

Also on life: When you make your bed you're the one that has to lay in it. So make it the best you can!

Happy Father's Day

June 16th is Father's Day. Take a look at this great list of the best techie gifts for your dad.

Gift giving is fun but can sometimes be a painful endeavor. What do you get for a man that has everything? Well, we have some great ideas for you. Take a look at the top Father's Day tech gifts for 2019.

1. Security cameras are great gifts for men who want to keep tabs on their homes or toys. If you dad is anything like mine, he's got a boat, old car or some fun ATV's hidden away in the garage. Security cameras have a million uses. Nest Cam is an indoor camera for just $169 that offers a remote application connection and includes speakers and a microphone.

2. Anker PowerWave Wireless Charger. If you're dad has joined the new age of cellular phones and has a newer style of smartphone, the Anker PowerWave runs about $30 on Amazon

(Continued on page 3)

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net

Even Your Daddy Can't Save You From Data Loss...

(Continued from page 1)

ments to load your files into your online storage.

- ***Flexible Storage Capacity:*** Check with your cloud provider to ensure you have options with various capacity offerings. Be sure you are only paying for what you are using.
- ***Quality Customer Service:*** There is nothing worse than losing a file and calling for support just to spend an hour explaining things. Call your cloud provider ahead of time and talk with them about support services.
- ***Security Features:*** Look for a privacy policy, encryption and file authentication to be sure your data is safe.

Your company's cloud security starts with strong passwords. With all of the technology utilized to protect cloud data, the New York Times reminds users that the password is still the weakest link in any security system. Strong passwords, changed regularly, coupled with the systems put in place by cloud storage companies can create an incredibly safe environment for your important files and photos.

Micro Enterprises LLC - 877-540 -6789

Why Internet Explorer Is Not Safe For Your Business

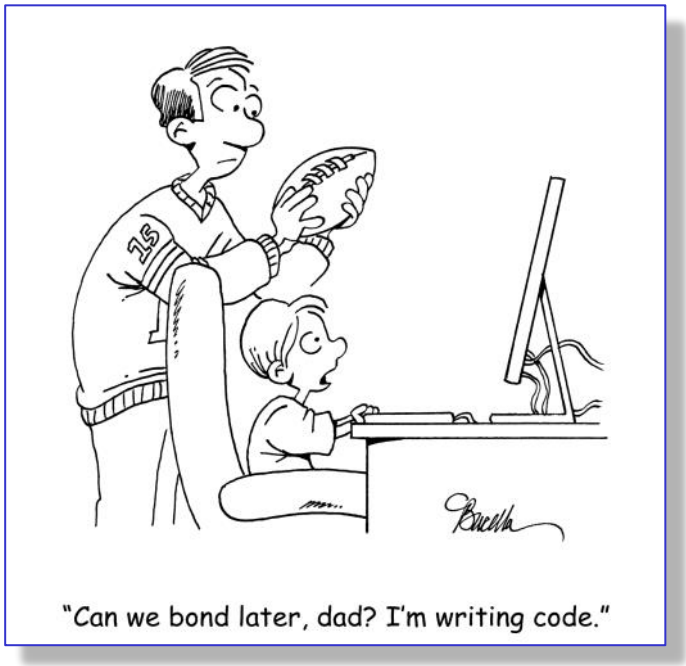
Experts say that using Internet Explorer can be dangerous. As you probably know that Microsoft is no longer updating Internet Explorer (IE), in favor of Microsoft Edge, but switching to another browser is not just a matter of preference, it's also a matter of security.

End of Support for IE 10. Even Microsoft warned in March that using Internet Explorer as a default browser was perilous. Many apps are designed for IE but new apps and Websites are not. So new Websites won't even work with IE. Aside from that, Microsoft is poised to end support for IE 10 in January of 2020.

IE may leave a back door open. Now, according to the blog, HotforSecurity, an IE user who opens an .MHT attachment (an archive of a Web page) can let hackers into their system. Even opening a Web page archive you have made can do the same thing. Be careful of the version of IE you have on your computers at home and in the office. Don't fall victim to these back doors. Crafty hackers are just waiting to swoop in and take your data.

Only about 7% of desktop browsers still use Internet Explorer, but the app is usually installed on a Windows system. Security experts recommend completely uninstalling Internet Explorer from all your machines through the control panel and installing a new browser.

Spread the word. Notify everyone in your company of this danger. Be sure your staff have a safer browser on all of their devices. Laptops, tablets and towers are all at risk and may leave your company wide open for attack.



A Chip Off The Old Block

As I am sure you know microchips are the foundation of technology. They are tiny wafer looking pieces of semiconducting material used to make integrated circuits. What is the next revolution for these tiny chips?

Moore's Law of computing is a rule of thumb that says that the number of transistors in a processor will double every two years due to advancements in technology. The rule has dominated the computing world since the 1960s, but according to the Nature Journal of Science, it nearing the end of it is road.

Thinking outside the box. Chipmakers trying to double transistors have been forced to look at the problem a bit differently. They have been doubling value for the consumer every two years instead of speed. Placing tiny, energy-efficient processors into as many things as possible to provide more functionality will become the next era of computing innovation.

The newest types of microchips used in everything from cell phones and televisions to tracking devices and drones are truly a chip off the old block. The design and structure has changed very little but, become more efficient.

Father's Day...

(Continued from page 1)
and is a fantastic wireless charger stand. It allows you to charge your phone propped upright so you can check your notifications at a glance or grab-and-go when you're ready.

3. DJI Spark Portable Mini Drone. Looking for something a bit more fun? Go for the new DJI Spark Mini Drone. It has a powerful lens for capturing beautiful aerial photos and video. It is easy to control with a cell phone or even hand gestures. Amazon offers this drone for just $335.

4. Fitbit Ionic Watch. Trying to get good old dad back in shape? Try an all-around fitness watch. The Fitbit Ionic Watch tracks sleep, heart rate, steps and even comes standard with built-in GPS for running. You Dad can even store music too and rock out during his workouts. The Fitbit Ionic Watch runs about $218 on Amazon.

5. Earbuds. Yep, we said it... earbuds are a great gift! A new pair of AirPods or even a pair of the Bose SoundSport Wireless In-Ear Headphones will do the trick. Either, or, are a fantastic gift for a father on the go. Prices range from $200 to $300 for a nice wireless set.

Happy Father's Day!

IoT Attacks Increased 600% In Just One Year; 5 Tips To Secure Your IoT Devices Today

You are on vacation; wouldn't it be nice to check in on your office? Or you are just at home for the day with family; it would be nice to check to see if everything is going well at work. Thinking of installing security monitors to see what's happening? Take a look at these tips to keep your business safe.

What is an IoT device? Internet of Things (IoT) devices are basically smart devices that have an online connection and can interact with other devices over Internet and/or allow users to remotely manage the device.

Consequences of convenience. The convenience of security cameras and monitors make them an important part of the Internet of Things (IoT). But they can and do have security issues. Most security flaws involve software called iLnkP2P, which is often bundled with IoT devices like doorbells and video recorders. The software makes it easy to access remote devices from anywhere in the world, according to Krebs on Security. But they are easily hacked.

5 tips to secure your IoT devices. Here are a few great tips to help you protect your business from IoT attacks:

1. Avoid connecting devices to the Internet without a firewall or in front of a firewall. Keep IoT devices behind a firewall, such as is found on routers.

2. Change the device's default credentials if you can. While some cameras and DVR's may not allow it, most have an option to enter a custom login. Change the standard credentials every six months.

3. Update the firmware when an update is available. Firmware updates can patch known vulnerabilities and fix issues the manufacturer has identified lately.

4. Disable Universal Plug and Play. Universal Plug and Play (UPnP) is programming that allows your device to automatically discover the presence of other devices and establish connections. Make sure to turn this feature off.

5. Don't buy Peer-to-Peer (P2P) devices. Peer-to-peer technology is engrained in millions of IoT devices allowing connectivity to the device without secure authentication.

The bottom line is, don't go cheap. Over 7 billion IoT devices are in use today. Don't go cheap if you're going to use remote monitoring in your office. Make sure to use a firewall, set a strong password, update your devices often, and be sure they are properly installed from the start to keep your company safe from harm.

It's Getting Hot In Here... Is Your Server Melting?

Well, this is one of those funny but, not so funny stories. A business owner was out to dinner with his family and he saw a notification from the thermostat in his office, the temperature had risen above the threshold he set. He was puzzled why but, turned down the temperature remotely and continued dinner. About an hour later, he checks the temperature again and it's climbed even higher.

What is going on? He tried to crank it down again, no luck. He quickly headed into the office only to find, the A/C is making some horrible chugging noises and isn't pushing cool air at all. Thankfully, he caught it early. The area where the server was stored was getting very hot! He set a fan inside the server room to keep things cooled while he called the repair company for the A/C unit.

If left unchecked, this issue could have cooked the hardware in the server room ruining the server, firewall or even Internet router taking down the office completely. While it's important to protect yourself when using smart products, they can be very helpful.

"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...

250 Antivirus Apps Tested And A Majority Failed.

A company called Antivirus Comparatives recently tested the antivirus (AV) apps in Google Play. They found that only 80 of the 250 AV apps they tested are capable of actually detecting the most common viruses. The company also noticed that many of the unsafe anti-virus apps had a four-star rating, according to GrahamCluely.com.

The actual test and findings. Out of 250 applications downloaded and tested, only 80 of them could detect over 30% of the infections they threw out there and only 23 products in that 80 tested could identify 100% of malware with zero false alarms.

Well-known brands performed best! Name brands like Kaspersky Lab, Sophos, AVG, Avast, and Trend Micro were in the list of applications that performed the best. Interested in learning more? Visit www.av-comparative.org to dive in deeper on recent antivirus software tests.

Looming Security Threat: Your Phone Number May Be A Vulnerability.

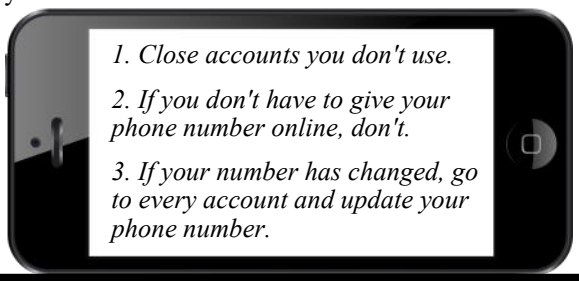
Suppose for some reason you lose your phone number. Then suppose it is recycled to people with bad intent. Could the number be used to fetch passwords? Could they get into your e-mail? You bet they could.

Millions of people get new phone numbers, some of which have been used before by someone else.

In the best case, the new owner gets lots of annoying FaceTime requests from teenagers. In the worst case, he gets a text every time the previous owner makes a bank deposit. Why? That someone hasn't changed his phone number with the bank. According to KrebsOnSecurity, that's just the tip of an enormous security iceberg. Many companies have built their user authentication programs around phone numbers.

One person who tested the security of phone numbers... got a new number then went to a large e-mail provider and typed the new number in the login. The provider then offered to reset his password and sent a SMS message with a code. He got in using the code. Except for one thing: He got into the e-mail of another person, the one who previously owned the phone number.

The fact is that phone numbers today are tied to a person's identity and attackers can use the number as an identity document. It's not just recycled phone numbers that can be vulnerable either, since there are hacks that allow the theft of numbers. That makes everyone with a phone vulnerable, but there are some things you can do:



PHISHING Pandemonium

Running a business is hard enough without a data breach. Did you know that 90% of data breaches these days stem from some kind of phishing scam? Phishing attempts have grown over 65% in the past year and it may take a month or more to even detect a breach! Give us a call today for a **Network Security Audit** and be 100% sure you don't have a breach in progress.

Micro Enterprises LLC 877-540 -6789

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net