HAPPY EASTER!

Tech Times

Solutions Unlimited, LLC

5 security concerns to explore; security is no joke

Security is at the forefront of every business owners mind. Keeping your physical location safe for patrons is difficult but, the Internet poses an unseen internal threat. How can you make sure your company information stays safe?

NEWS
Over 822 million records exposed in 2013

"2013 Data breaches exposed over 822 million records nearly doubling the previous record high…" *reports the Digital Journal. The 2013 exposures reached an all-time high over previous years. With over 2,164 incidents of breaches, over 822 million records were appropriated by attackers last year and almost half of those were right here in the U.S.*

Security breaches are a very real threat. It seems like second nature to hear about a security breach on the morning news at some large

corporation. We even have a few friends who were tied up in the data theft issues at Target last winter. In this incident, 110 million records from Target shoppers were exposed all because their HVAC company didn't use a good antivirus program. Adobe topped the Target debacle with over 152 million records swiped last year.

Giant companies are not the only ones in the spotlight. Regardless of the size of your organization or type of clients you serve, keeping your company data safe is essential to keep your company in business. Technology can give you the upper hand over your competition, but it can also mean the end of your operations when it's not properly managed.

Solutions Unlimited, LLC
100 Corporate Dr Ste N
Spartanburg, SC 29303
864.599.8678
www.suisc.com

What's inside...

Before computers

Remember when...

Memory was something you lost as you aged?

Programs were shown on TV?

A hard drive was a long road trip?

A keyboard was a piano?

Cursor meant a mouth full of soap?

An application was used for employment?

A broken disk really hurt?

Bunnies, baskets, and reverence

This holiday brings a flood of shopping deals, family activities, and religious events. One common denominator though, everywhere you turn is reverence.

Easter takes over the retail world. Every place where anything can be sold displays Easter baskets, chocolate eggs, grass, and jelly beans in March and April. You can find great deals on clothing, cars, even electronics. Some retailers even display advertisements for graduates around the Easter holidays.

There's another side to April though, the reverent side. Whether or not people attend church on other Sundays, Easter is the most popular day to go. In the past, attendance at church on Easter was even required. In the Roman Catholic church before 1963, you weren't considered a member unless you attended church on Easter.

The Jewish Passover is another April event.

5 security concerns to explore...

(Continued from page 1)

What should I be managing? Ask yourself, "What do we have to protect? What would impact our company the most?" Look at things like the types of information you collect from your clients. Do you store payment information or personal data? Does your business have an internal network, wireless network, remote access, or Internet based programs? Do you have work devices that leave the office like smartphones or laptops? Consider these five security concerns to explore to keep your company safe.

1. *Educate your employees.* Train your employees to recognize the risks associated with infections, online fraud, scams, and social engineering. Make sure personal devices used at the office are properly maintained and free from infection before they are allowed on the company network. Even charging a smartphone or using a flash drive with a virus on it can let hackers right in your back door.

2. *Keep your applications, software, and hardware licenses/warranties updated.* All your systems would be updated in a timely fashion with continual monitoring, patches and upgrades as they become available. Falling behind on this standard IT maintenance can mean a rift of exposure in your organization.

3. *Lock down your network.* If you have a Wireless Local Area Network (WLAN) at your location for your clients and guests to use, separate it completely from your company operations. Lock down your organization so the traffic from your public network cannot travel into your internal systems.

4. *Encrypt your sensitive data.* Your clients expect you to keep their information safe. They trust in your business for products or services as well as privacy and security.

5. *Backup and secure your internal systems.* Use a strong authentication method to keep your data safe from intrusions and malicious attacks. We recommend a robust filtering system, a firewall, anti-virus protection for every computer and server as well as 24/7/365 monitoring and offsite data backup. This may seem like a lot, but think of the consequences if your data is lost, stolen, or corrupted. Could your business survive? *OH NO! Are you worried?* If you have questions racing in your head after reading this article, give us a call. We offer a FREE Network & Security Audit to help you identify and address the risks your business is facing. 864.599.8678

"Mom, when you need parenting help, do you call grandma for tech support?"

A sweet personal plan for protection

Put down that chocolate bunny and make a sweet plan to keep your personal data safe.
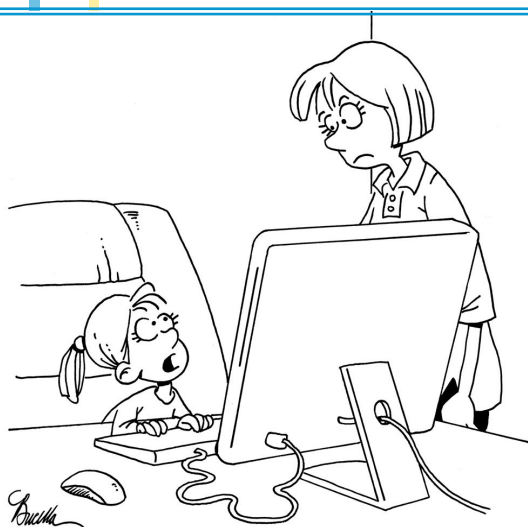
Don't kid yourself, your laptop doesn't have to be logged-in when it is stolen to be stripped. In fact, some savvy thieves have even found ways to steal your data while you surf online using Wi-Fi hotspots. That's right, you can use your computer while an attack is in progress.

Personal data breaches are everywhere! *Cybersecurity threats come in all types and sizes. In the last 18 months, attackers have focused on things like social media networks, photo sharing sites, e-mail providers, financial institutions and even data storage companies. If you use any of these things hear this…*

You are not sheltered from attacks! *Backup your personal data regularly, use a reputable antivirus protection program, and invest in a password manager to keep your personal information safe.*

Commit yourself to security. *Be smart about your habits. Keep your devices physically safe. Don't store them in your car or leave them on your desk, and never use devices that are not yours on your personal or work computer.*

Bunnies, baskets and reverence...

The reverence of Passover is the main event of April when Jewish families gather for seders. It is celebrated in Jewish homes throughout America and around the world.

Over time, all of this has led to something good that happened in our country. Instead of feeling separated from one another by our religious celebrations, we regard the events with mutual interest and respect. When you stop to think about it, it's a little like diversity in the workplace. When all kinds of people respect each other and work together a lot of good things happen.

Enjoy this season of reverence. Easter is a holiday everyone can enjoy. So, plan your weekend April 19th and 20th to include a little of everything. Don't miss the opportunity to spoil the little ones in your life with bunnies, baskets and candies. Visit a local church or charitable event to celebrate Easter with your family, friends, co-workers, or community. However you choose to celebrate, don't be shy. Show your respect and devotion to your family and friends this holiday season.

Happy Easter!

Don't put all your eggs in one basket; hire the best manager ever!

Do you ever feel like your brain is swimming with passwords? Are you tired of trying to make up hard passwords to keep your accounts secure? Try a password manager on for size. It's an eggcellent investment!

Password do's! We've all heard stories about users getting hacked because they use the same password for everything, right? Don't be a victim, use a variety of passwords for your accounts. Here are a few tips to create strong passwords:

1. *Make your passwords at least 8 characters long*
2. *Never use your username, company name, or real name as part of your password.*
3. *Use acronyms not common words from the dictionary.*
4. *Always use upper and lower case letters with numbers and characters or symbols. Even one of each will do the trick.*
5. *Be original! Never use similar passwords over and over.*

Easy, right? Now, follow these five steps for every account you have a login for and be sure to update the passwords every six months to keep your data safe.

This is the part where you say,

"NO!" All the tips to make my passwords safer won't help me remember them. I need more! Don't worry, that is what a password manager is for.

Hire the best manager to help you. Consider these popular password managers when securing your accounts:

- *MyLOK Personal ($89.95)*
- *RoboForm Desktop 7 ($29.95)*
- *1 Password for Windows ($49.95)*
- *F-secure Key ($15.99 yearly)*
- *Password Genie 4.0 ($15 yearly)*
- *LastPass 3.0 Premium ($12 yearly)*

Most of these have free versions you can hop in and test to see if you like them.

Check for security. Just a few things to look for if you go exploring; look for a program that will generate strong random passwords for you on demand, offers multifactor authentication (security features), and offers multiple device support so you can carry all your passwords over from your laptop to your smartphone or tablet too. Remember, your password manager is only as good as the password you use to secure it. Stay safe.

A Tweeting nation

Here is a little lighter news to make you smile.

A few translations for perspective. A "tweet" is an update of 140 characters or less posted on Twitter, a popular Social networking site. "Following" is when you elect to receive tweets others create. Having "followers" means other people receive your tweets. 'RT', short for "re-tweet", is when you are reporting a tweet to your followers that you found online. "Tweetup" is when Twitter users meet in person. "Hashtag's" are a # sign at the beginning of a word to show what the tweet is about and help others find topics they can enjoy.

Kids today... think things like this are common knowledge?
They even confuse their online vocabulary with standard terms and symbols on occasion. True story... A sixth grader in the northwest math class asked his teacher, "Why do you keep using hashtags in front of the problems on the board?

#1. 4 (6y)
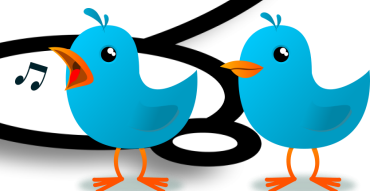
"We make all of your computer problems go away without the cost of a full-time I.T. staff!"

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

Inquiring Minds...

You're location is being tracked! **Don't get paranoid, but you are being watched. If you use a cellphone, you are broadcasting your presence and not just with calls and texts.**

Cellphones continuously tell your location **to whoever is listening, and people are listening. Private companies are listening and tracking cellphone location data to find out the preferences and activities of their customers.**

A cafe owner knows coffees are popular, but what else could he or she offer to customers that they might want? If the cafe owner knows 80 percent of customers go to a gym, maybe a gym shirt with the cafe logo might sell. New location companies are starting up to provide the cafe owner, or anyone will to pay, exactly this type of information.

Is it legal? **According to the Wall Street Journal, companies in the US do not have to get consent before collecting and sharing location data. Companies in the location tracking business say privacy concerns are overstated since tracking is not personal and not invasive. How do you feel about sharing your location with the world?**

A stand-up effort to collaborate. **These meetings are agile and held standing up. In an effort to reduce time spent in meetings, more companies are using these rules: Attendance is required, no casual chatting, and everyone has to stand up at the meeting. Anyone who's late has to do something like sing a song or pay a small fine. Some companies don't even allow tables, because those attending spend too much time leaning on their hands, playing with their cell phones or working on their laptops.**

Stand-up meetings are not a new idea, **but today's are based on the growing use of "Agile" in software development. It compresses projects into short pieces. As Agile has become more widely adopted, stand-ups have spread along with it, says The Wall Street Journal.**

In these Agile meetings, participants update their peers on what they did since yesterday's meeting; what they are doing today; and any obstacles that stand in the way of getting work done. Daily meetings take about five minutes to fifteen minutes depending on the size of the group.

Try short Agile meetings.
You will be surprised how they improve communication, embrace collaboration between teams or departments, and keep everyone accountable.

We'll be your eggheads

Feel like you're walking on egg shells with your current technicians and they constantly blame you for your IT troubles? If you feel like you have scrambled eggs for brains from your technology woes, it's time to seek out a professional team to watch over your technology needs. Our egghead staff is fully trained and 100% committed to your IT solutions. We will work with you to evaluate your current systems, create a sensible plan for your future, and put a little back in your nest egg. IT investments shouldn't leave you with egg on your face. Give us a call today and speak with a good egg.

Solutions Unlimited, LLC
864.599.8678

Solutions Unlimited, LLC
100 Corporate Dr Ste N
Spartanburg, SC 29303
864.599.8678
www.suisc.com