

IT Strategy Brief

ISSUE 2 | VOL 3 | February 2017

INTEGRATE SEAMLESSLY

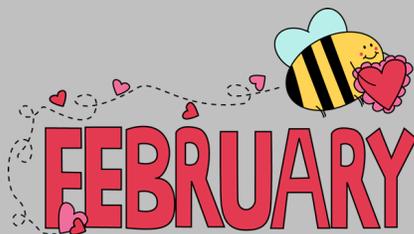


SWK
TECHNOLOGIES

“Useful Technology Ideas for Your Business”

What’s Inside:

St Louis libraries under attack by hackers using ransomware	Page 1
What our clients are saying	Page 1
Survey chance to win a gift card!	Page 2
Choosing storage: OneDrive vs SharePoint	Page 2
Gooligan virus attacks Android users	Page 3
Shiny gadget of the month: Nintendo Switch	Page 3
TRIVIA	Page 3
Services we offer	Page 4
Hackers hold UK hospitals hostage	Page 4



St Louis libraries under attack by hackers using ransomware

In late January the St Louis library system fell under attack. The libraries were brought to a complete stand still while borrowers were unable to return, borrow, or use the computers at any of the 16 branches. Their system had been hacked and infected with ransomware with the hackers demanding a ransom of \$35,000 in the form of bitcoin. Approximately 700 computers were infected across the 16 public libraries in the system.



The library authority refused to pay and as a result will wipe its entire computer system and rebuild it, which will take a quite some time to accomplish. During this time the libraries will remain open, but computers will off limits. An attack like this takes a toll on more than just the library system, but also those who rely on the library system for school as well as those who need the library for internet access.

As we have discussed before ransomware has become an extremely popular method of hacking. Could you even imagine having to wipe your computer system and having to start from scratch? It could end a business. The way most occurrences take place is through clicking a link in an email that downloads the virus onto the computer system. Remember to always be cautious and only open emails from reputable sources.

If you have any questions about keeping your network secure let us know!

What our clients are saying: Cooper Wilbert Vault Co.

When asked about what she liked about our services:

“The quick response. Having SWK is like having your own IT Department that you can count on. Our computer system is a big part of our business and having SWK gives us a piece of mind that if something goes down we have a team of individuals that are going to help us get back up in running in minimal time. Time is money and if the computers/server goes down the clock is ticking. Each “computer guy” we have encountered is extremely knowledgeable and pleasant to deal with.”

Beth Cooper
Cooper Wilbert Vault Co.



Get More Free Tips, Tools, and Services on Our Website: www.swktech.com

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:
Peggy Harrington
LM Service Co.

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

- 1. What do you like most about our services?**
- 2. Tell us about a specific experience with us that you were happy with.**
- 3. What are the biggest benefits you've received or experienced since hiring us?**
- 4. What can we improve?**

Email Jon Stiles
 (jonathan.stiles@swktech.com) with your responses
 OR

Fill out our online form:
<http://bit.ly/nwsnews-survey>
 before **March 6th** to get your name in the hat.

You could win a \$25 Gift Card!



Choosing storage: OneDrive vs SharePoint



Digital Storage options with Office 365 provide business owners with convenient and efficient data management. But with new software added daily, it is easy to get overwhelmed by the variety of options. Keep reading to find out which Office 365 program will be your best option for organizing and sharing information: SharePoint or OneDrive.

Similarities between OneDrive and SharePoint

Both OneDrive and SharePoint applications utilize

Office 365 to help businesses organize information and share it with employees and company heads. Documents are stored in a cloud drive for security, so employees can track changes between edited versions, as well as make comments and add information when necessary. This real-time collaboration is one of the favorite benefits of online file management. Since data can be synchronized to various forms of technology, it is portable and usable everywhere.

OneDrive provides personal attention

OneDrive uses a SharePoint backdrop in order to run, making the two programs inherently connected. However, there are distinct features that business owners will notice with their OneDrive account. The OneDrive program is utilized by individuals, and control is still maintained by the individual even if it is shared across a department. Changes are synced to a chosen device, allowing departments to work on projects together. As an administrator, you can share the document by way of a secure link, and you can allow some people to edit and leave others in a position to view only.

SharePoint is a wider group share program

If OneDrive is the perfect individualized sharing option, then SharePoint takes a wider stance. An administrator or company head can save a document online, allowing employees throughout the company to view and edit the document. Every change is tracked to give higher-ups an idea of who is contributing to the company projects. SharePoint is a good application to use for human resource surveys or updates that need to be completed by team members in other departments.

Office 365 encourages businesses to increase their employees' usage of online storage and data options. SharePoint and OneDrive are just two of the many programs provided to improve how your business is run. For more information on how online document sharing programs can help you increase your company's visibility and productivity, contact us today.

Gooligan virus attacks Android users



If you own an older Android, you might have already experienced the impact of the Gooligan Malware virus. Since August, the infection has struck an estimated

1.3 million Android phones, and it shows no signs of stopping. For those unaware of the Gooligan strain, here are a few key details you need to know right away.

It is estimated that since Gooligan's August 2016 appearance, the malware has infected more than 1.3 million Google accounts — one of the largest single thefts in recent history.

With the range of personal data available in Google accounts, it is interesting to note that Gooligan's purpose isn't to steal the valuable information; instead, it's to distribute advertising fraud. With as much as \$320,000 a month going into the pockets of Gooligan developers, it is obvious that the play is working.

How Gooligan is Moving Through the Internet

Consumers are falling prey to the virus when they attempt to download a fake app from a third-party app store. Instead of getting the program that they were promised, they inadvertently allow the Gooligan malware to root into their Android OS and take control of it. Once in control, the virus downloads apps using your Google information. These apps are infused with ads that belong to Gooligan developers, bringing them a never-ending stream of income.

Where Gooligan Came from and Where it's Going

Gooligan appears to be a variation of the 2015 Ghost Push malware, which was also wildly successful at infecting Android users. Google is currently working with Android engineers and Internet security firms to stop the malware; they believe that through cooperative efforts, it will disappear from public attention. As it is, those who have updated Android versions of 6.0 or greater are not affected by the malware.

You can lower your chances of contracting the Gooligan malware by downloading apps only from Google Play and checking your system through the security firm Check Point to ensure your Android hasn't already been infected.

Shiny gadget of the month: Nintendo Switch

Video game consoles have been a fixture in our society for a while now. Most people have played (or at least watched someone play) a game on a console, a PC, or a handheld device at one point or another. On March 3rd Nintendo will be releasing their latest gaming system the Nintendo Switch, however, this one is breaking away from the traditional game consoles.



The Switch will be different from the Xbox and PlayStation because not only can you play it on a TV with a controller, but you can then take the console (which is essentially like a tablet) out of its docking station and attach the provided controllers to it making it into a handheld system that you can take on the go. Since the tablet is the brains of the system it lets you pick up where you left off whether you are playing on the TV, or on the go as a handheld using the same game. In the past these would be two separate devices that required different games, now it's all in one place.

That is not all, there is another option where you can take the tablet piece and remove the controllers from it where they each become separate controllers and the tablet part is like a mini TV for local multiplayer on to share with friends no matter where you are. The little controllers that snap on and off of the screen are also quite the little pieces of technology. They can function together as a single controller or be used separately as two mini controllers for sharing. They also come packed with features and motion sensors for using the motion of the controller to control characters in game similar to how the Wii works, but with improved

technology. There's even a tiny IR motion camera packed in there that will be used for games too.

While there are so many features and things that have been told about the Switch, but there are still many that are unknown. There have even been rumors that Nintendo plans to use the hardware from this system to expand into virtual reality in the future. Since it does not come out until March we don't know exactly what to expect just yet, but it certainly seems like an interesting concept and something that could change things up a little in the video game world. You can see more for yourself and some examples of how Nintendo plans for the switch to be used on their website <http://www.nintendo.com/switch/>.



Gift Card Trivia!

This month's question is:

How many public libraries were infected by the ransomware in St. Louis? *(Hint: The answer is in this newsletter.)*

- 12
- 16
- 4
- 25

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **March 6th**, in order to be placed in the running for this month's gift card prize!

We can help you with:

- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.

South Jersey

1120 Crown Point Road
Westville, NJ 08093

North Jersey

5 Regent Street, Suite 520
Livingston, NJ 07039

Phone: 856.956.5800

Fax: 856.845.6466

Visit us on the web at

www.swktech.com



Hackers hold UK hospitals hostage

If you had thought you heard the last of hackers taking over a hospital's computer systems you were wrong. In late January three North Lincolnshire hospitals were infected with ransomware. Not only did the ransomware hold the system hostage, it forced them to cancel ALL appointments for two days. That would be a serious loss for any business. The infection went as far as even affecting the car parking barriers.

The hospitals did not end up paying, but did have to take their system down in order to remove the virus. Doing so is a costly and time consuming process, one that will take the hospitals some time to recover. While attacks like this can be crippling to a business, the business is not all that could suffer...

Experts are fearing that it is only a matter of time before they target equipment, such as machines used to regulate medicine intake or pacemakers. In fact a cybersecurity firm Bishop Fox claims that some home monitors can be hacked to be used as a weapon against cardiac devices, where they could drain the battery, turn the device on or off, or depending on the device... even deliver a shock.

As technology progresses, we too must keep pace with it. That means taking cyber security seriously and not thinking "that will never happen to me". As we have seen the number of people it is reaching grows every day.