

# IT Strategy Brief

ISSUE 10 | VOL 4 | October 2018

INTEGRATE SEAMLESSLY

"Useful Technology Ideas for Your Business"

## What's Inside:

|   |             |
|---|-------------|
| SMBs Exposed to Cyber Attack – and It's Their Fault                   | .....Page 1 |
| What our clients are saying .....                                     | Page 1      |
| Time-saving tips for Microsoft Word                                   | .....Page 2 |
| Survey chance to win a gift card! .....                               | Page 2      |
| Shiny gadget of the month:<br>Saent – The Productivity Booster        | .....Page 3 |
| Title Agents Can Lose Millions from Scams Not Even the FBI Can Detect | .....Page 3 |
| TRIVIA .....  | Page 3      |
| Services we offer.....  | Page 4      |



**SWK**  
TECHNOLOGIES

## SMBs Exposed to Cyber Attack – and It's Their Fault

Research into cybersecurity for small-and-medium-sized-businesses repeatedly reveals two things: [SMBs are increasingly at risk of a cyber attack year over year](#), and [a majority of SMB leaders and employees remain ignorant to the former](#). The number of SMBs which have experienced network breaches continues to grow, as does the frequency of these attacks and the amount of damage [that successful data penetrations or system infections cause](#). The factors behind these trends remain relatively consistent, including a lack of individual and organizational best practices, budgetary concerns when it comes to personnel and tools, and opportunity for hackers in the form of said lack of best practices and tools.



Concerning the widespread lack of best practices, surveys show that employees (including those on the executive level) [consistently remain the biggest gap in an any organization's network security](#). C-suite officers provide the most valuable targets to hackers, but anyone with some level of access to data controls offers an opportunity to exploit in a cyber attack. Cybercriminals seeking a better return from compromising an individual's personal information, but not willing to risk breaching a larger corporation's network security will begin looking for an entryway into an SMB's systems through easy victims.

Social networking platforms are ubiquitous in the modern digital world and bestow a wealth of background information for any attacker to discover via a simple search engine. Hackers utilize social engineering as a cost-effective method of gathering enough data on targets of opportunity that can be pursued for a phishing campaign. The details they obtain allow them to craft increasingly sophisticated fraudulent messages; even if an email might contain a few errors in the copy or the sender's address, committed cybercriminals will ensure they are visually deceptive enough to drop the victim's guard.

Continued on page 2...

## What our clients are saying: BCA Watson Rice LLP

"When we got infected with a virus, SWK worked immediately to restore all of our networks. The response and recovery time was superb. Most of our IT issues are answered and resolved as soon as possible with very little time lost."

Gina Bidaisee-Santo  
BCA Watson Rice LLP



# Two ways to WIN a gift card!

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

## Last Month's Contest Winner:

**Patricia Caravello**  
**Chelsea Textiles**

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 **November 2nd** to get your name in the hat.

**You could win a \$25 Gift Card!**



## SMBs Exposed to Cyber Attack – and It's Their Fault

Continued from page 1...

Even if an attacker does not follow through with a phishing attempt, there are plenty of other ways for them to leverage personal data to breach a business's network security. Hackers may track a travelling executive relying on hotel Wi-Fi, crack weak passwords using social media information, or set up dummy versions of company websites laced with malware. Just knowing that you have data that you consider critical can be all an attacker needs to launch a ransomware campaign that will infect your system and lock down your files.

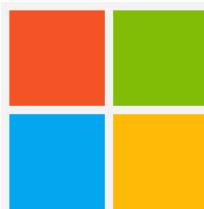
Cybercriminals seeking monetary gain do not present the only problem either, as "hacktivists," state-sponsored and cyberwarfare nation-state hackers [are targeting SMBs in certain sectors as well](#). Such groups based in Russia, China and North Korea are focusing on disrupting the manufacturing, energy and other industries to drive political outcomes and any business of any size is a legitimate target. Some of these nation-backed attackers seek both political and monetary gain simultaneously and poach data from America businesses for foreign governments or companies to increase their competitiveness in the world economy.

SMBs occupy a precarious place in the web of modern cybersecurity – too small for the expensive cybersecurity solutions of corporate giants like IBM, but too big for hackers to ignore. The research cited at the beginning of this article – and many other studies – indicate that the most common practice for a majority of SMBs is to simply rely on their smaller size as a deterrent against being targeted. The data above clearly demonstrates this is an ineffective strategy.

This is an especially dangerous for businesses on or approaching the "medium" side of SMB, where both new technology and growth bring additional touchpoints and network gaps that hackers can exploit. Any SMB doing business in the 21<sup>st</sup> century must no longer treat implementing a comprehensive cybersecurity plan as a luxury – a defended network is now a requirement to exist.

The first step to securing your network is determining how vulnerable it is – [sign up for a Network Vulnerability Test to gauge the strength of your current practices](#)

## Time-saving tips for Microsoft Word



Microsoft Word remains one of the most popular and user-friendly apps for business today. It is compatible with both Windows and Mac devices, and can be used to create a wide array of business documents. While millions of people use it every day, most don't know how to maximize Word's potential. And since it is constantly being updated, you need to check out these tips that will help you save time:

**Edit documents simultaneously**

You and your colleagues can now edit the same Word document at the same time. Word enables you to save the document to the cloud using **OneDrive**, click **Share**, then copy the link and send it to another user within your system. You'll even be able to see them editing in real-time.

**Pick up where you left off with Word Online**

Don't have the Word app on your computer, tablet, or smartphone device? Go to [word.office.com](#), sign in with your Microsoft account, and open **Word Online**, the browser version of Word. By utilizing the **Share** button, your colleagues can access your document using Word Online or the Word app, which means anyone with the link and an Internet connection can jump right in.

**Keep editorial control**

With the **Track Changes** function, Word monitors all edits that anyone makes to your document, so that you can go through the changes and accept or reject them accordingly. To turn on Track Changes, click on the **Review** tab then select **Track Changes**. When reviewing a colleague's edits, click on **Accept** or **Reject** as you see fit.

Continued on page 4...

## Shiny gadget of the month: Saent – The Productivity Booster



The world we live in continues to become increasingly connected. We all have multiple devices, we watch TV and surf the internet on our phones at the same time, our jobs keep us busy with multiple things constantly going on at once. Multitasking has become a way of life for many people. However, that does not mean that it is a good thing. Sometimes with too much going on at once it can be difficult to focus and actually be productive. If you are constantly being distracted by things you can never really get going on your main task. Well, the time has come that a device was created to help block out the other devices and distractions.

Saent (pronounced saint), was developed to help instantly boost your productivity and focus. Saent is a smart device and desktop app that work together to create an environment that enables you to accomplish your goals. Based on the pomodoro technique and the principles of Deep Work Saent helps you block distractions and find an optimal work rhythm. Let's be honest everyone gets distracted, think about how many times an hour you may be trying to set out to accomplish something, but then something else pulls your focus. The gadget has a distraction blocker that you can set to block certain websites or other digital distractions, as well as focus sessions – launch timed sessions to keep you focused, and smart breaks – to follow up focus sessions that automatically calculate how long you should recharge after each focus session. The physical device itself also acts as a do not disturb signal for your desk so coworkers can see you are in the middle of something.

Saent has been shown in Fast Company, Newsweek, Mashable, and many more publications. For \$60 I think this device could be worth it. Developing a rhythm to focus and also take a break is key. Finding that balance to maximize your productivity is important, whether you are not taking enough breaks to remain fresh, or you just need help to remove distractions. Saent has a quick little video on their website to see more of the gadget at [www.saent.com](http://www.saent.com).

## Title Agents Can Lose Millions from Scams Not Even the FBI Can Detect

Canyon Culinary, a restaurant group that owns several venues in Salt Lake City, was looking into expanding and [was on the verge of wiring over \\$1 million](#) to the owner of a parking lot they were interested in, when the group's Controller noticed some discrepancies in the last message they received with wiring instructions. They narrowly avoided becoming the victims of wire fraud [in yet another case of a hacker infiltrating email communications with a title agency](#). The thieves waited until the point where a transaction was needed to complete the deal and sent their own message with a bank account they owned.

This is an emerging tactic that not even the FBI has been able to prevent or track effectively. Wire fraud of this type is not necessarily new, but there has been a resurgence in the past few years [according to the National Association of Realtors](#) and it is becoming more refined in application. Canyon Culinary was a lucky exception that avoided adding to the estimated \$5 million lost in similar scams last year in Utah alone. "It's a simple scam for the hacker to pull off, and that's the scary thing," said Adam Kirkham, the head of the Salt Lake Board of Realtors.

Even experienced real estate and title agents can be caught off-guard by this type of scam. Rich Hopen, a broker based in New Jersey, [lost over \\$200,000 during a personal deal](#) when the title agency he was communicating with sent the funds to a hacker that had hijacked their conversation and posed as Hopen. The bank where the account that received the money was hosted was unable to retrieve it in time, and the buyer, mortgage lender, and title company all became involved in lawsuits as a result.

Wire fraud cases of this type are complicated by several factors, one of the most prominent being that the banks can (or will) take only limited action within a certain timeframe. When investigated, the accounts will often be found to have originated overseas so that domestic agencies will have a harder time pursuing the culprits. The FBI can potentially stop the transaction, but only within a certain period and if notified by the bank. This means that all of the parties directly affected the wire fraud will quickly lose control of the entire situation if they do not recognize it fast enough.

Title insurance agencies are just as affect by the wire fraud epidemic as everyone else in the real estate market, and can experience loss of revenue from funds directly lost to scammers or reparations required by victims. Title agencies are also vulnerable to hackers posing as their representatives, which as seen in Hopen's incident and several others, exposes title agents and their organizations to legal liabilities.

To protect against the consequences of email breaches and wire fraud, title agencies must be able to secure and manage their network security on a consistent basis. [Download our white paper](#), "Common Threats to the Title Industry and How to Prevent Them," to learn more about the dangers of not protecting your system and what you can do to defend against them.

### Gift Card Trivia!

This month's question is:

*What do SMB's (incorrectly) tend to rely on as a deterrent for hackers as their cybersecurity (Hint: The answer is in this newsletter.)*

- a. Their smaller size making them not a target
- b. Antivirus
- c. Managed Service Provider
- d. Firewall

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **November 2nd**, 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
- Employee awareness training
- 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**

650 Grove Road, Suite 106  
West Deptford, NJ 08066

#### **North Jersey**

120 Eagle Rock Ave., Suite 330  
East Hanover, NJ 07936

Phone: 856.956.5800

Fax: 856.845.6466

Visit us on the web at  
[www.swknetworkservices.com](http://www.swknetworkservices.com)



## Time-saving tips for Microsoft Word

Continued from page 1...

### **Format the easy way**

The **Style Gallery** in Word makes it easy to format your document, despite the huge number of font types, sizes, colors, and effects to choose from. After finishing writing and editing your document, click the **Home** tab and you will see the **Style Gallery** prominently on top. Select the appropriate Headings in the font, size, and color that you like, and change any other text in any way you like.

### **Insert photos faster, more conveniently**

No need to open your browser to look for photos for your document. Just place the cursor on the area where you intend to insert the photo, click on the **Insert** tab, select **Online Pictures** (type “clip art” on the search box if that’s what you need), select a photo, then click **Insert**.

### **Edit a PDF file**

Click on the **File** menu, select **Open**, and choose **Browse**. Highlight the PDF you want to edit, then click **Open**. Word will convert files to the new format using text recognition, so double-check if the conversion is correct. Make the appropriate changes, then click **File**, then **Save As**, then **Browse**. A “Save as type:” dropdown menu will appear at which point you will choose “PDF” then click **Save**.

These tips may seem straightforward, but over time they can make a big difference in helping you work faster. Want to learn more Word [tricks and tips?](#) [Get in touch with our Microsoft Office experts today!](#)