IT Strategy Brief

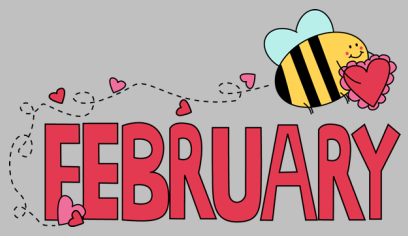
ISSUE 2 | VOL 4 | February 2018

INTEGRATE SEAMLESSLY

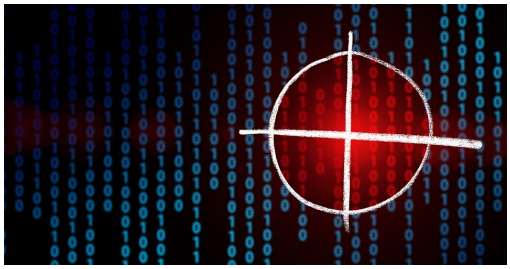
SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:



Why Executives are Big Targets and How to Protect Them



Given the spate of corporate cyber attacks within the past year, the conversation around cybersecurity has been shifting increasingly to employee education and training. However, one factor that has often been left out of this dialogue is the growing vulnerability of executives. C-level officers are inherently more desirable targets than most other personnel for hackers due to their greater access to sensitive data.

Cybercriminals often launch many of the same penetration attacks against executives as they do for other employees yet will also commit more time and resources to these targets since there is a bigger potential payoff. Conversely, they are often the least likely to follow established cybersecurity procedures, making them even more of a risk to a company's confidential information.

Phishing attacks are still a popular method of network breaching attempts, and this is still true for executive-level personnel. "Whaling," or phishing aimed at bigger targets, is being more carefully tailored to elicit responses from these particular types of victims. Whaling messages often appear more sophisticated or legitimate than normal phishing attempts. They are closer to spear phishing since they are crafted with one specific individual in mind, yet they are uniquely dangerous in the type of information they seek. Whaling attacks usually try to gain access to confidential company information. Successful whaling breaches will often lead to more attempts being made.

The danger can be aggravated by several other factors, including proclivity of travel for an executive and the access others in their department have to their credentials and information. Executive assistants are also targets due to their proximity to the c-suite, as is anyone else who supports boardroom functions. Additionally, officers in certain industries may be even more vulnerable than usual to attacks.

The need for executives to be protected will only grow as both hacking becomes more widespread and technology allows for greater interconnectivity. There is a lack of organizational knowledge on the subject for many businesses, and that is one of the key factors that hackers rely on.

Protection against whaling attacks must be twofold: executives need to be better educated about how they are at risk, and companies need the tools to safeguard their accounts. Some of our services can help you on both counts.

SWK Network Services provides an email hosting program with professional-level filtering to keep out viruses and encryption to better protect your confidential messages. We also offer Phishing Defender, a comprehensive employee awareness training to detect phishing attempts. If you would like to learn more, feel free to contact us online or call 856-956-5800.

What our clients are saying: Tangibl Consulting, LLC

"I am very pleased with the prompt service SWK provides Tangibl Consulting. Your staff are very personable and knowledgeable."

John M. Evanich
Electrical Designer / IT Services
Tangibl Consulting, LLC

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Robert M. Brown
American Asphalt

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 5th** to get your name in the hat.

You could win a $25 Gift Card!

The Far-Reaching EU Regulation You Might Not Have Heard Of

We previously wrote a list of cybersecurity predictions for 2018 that included an increase in IT regulations. We cited one such emerging provision as a sign of a beginning trend, the General Data Protection Regulation (GDPR). If you did not read further on the subject before, and if you do any sort of business online that involves anyone who has resided in Europe, then you will want to keep reading here.

The GDPR emerged from the Data Protection Directive 95/46/EC ratified by the European Union's governing bodies in 1995, which itself came from legislation pushed forward in the early 1980's. The idea behind this group of laws is to protect the personal data of European citizens while still allowing it to flow freely.

U.S. companies that may be affected by this law should note that "personal data" is generally defined more stringently in the EU, and covers virtually all digital information that can be used to determine the identity of the person the data originally belonged to. This also includes not only basic entries such as names, addresses and phone numbers, but also additional identifiers such as race, gender preference, and health data.

Tracking cookies and IP addresses are also considered personal data under EU law, the former if the information they collect can be used to identify the user. Under GDPR, this data must be consented to be given freely, at which it becomes the responsibility of the company who collects it. One of the stipulations of this regulation is that if they or someone else uses this information in a manner that invades the privacy of the individual it belongs to or was not utilized in a previously agreed-upon manner, then the collector of that data becomes legally liable for the consequences.

The comprehensive nature of this regulation means that even something as simple as a survey that reaches someone living in the Eurozone might make your company liable for any personal information you collect from the respondent. If found that you displayed intent to specifically market to EU citizens and/or to utilize any data collected, you will most likely be subject to the GDPR's requirements. Similarly, any money exchanged through the Web (and the corresponding financial information that facilitates that) for ecommerce purposes and employees based in the EU will also stipulate compliance with the GDPR.

The GDPR is very detailed legislation, so it might take some lengthy additional research into each article and a conversation with legal counsel before you can determine precisely which provisions apply to you. However, it may be prudent to take steps to meet these requirements regardless. As we indicated in our predictions for 2018, this type of policy will likely develop into the new standard gradually.

Facebook has already preemptively transformed its data mining procedures ahead of the May 25 deadline for compliance implementation of the GDPR to avoid the type of scrutiny (and fines) it has faced in the past for breaches of privacy. Though the U.S. has traditionally been relatively less strict about data protection on the legislative level than Europe, this mindsight will probably shift as the incidents that prompted the creation of the GDPR become more commonplace.

Despite this, recent studies indicate that many American businesses may not be prepared for or are unaware of what this type of regulation actually entails. Some surveys revealed several worrying trends, including widespread ignorance among quite a few employees of the nature of GDPR provisions and even what actually constitutes sensitive data, as well as the severity of the fines for failure to comply. Noncompliance can cost businesses up to 20 million euros (approximately 25 million USD) or up to 4 percent of their annual global revenue.

A primary obligation for compliance with the GDPR and similar regulations is the demonstration of the ability to consistently protect any and all personal data collected. This means that cybersecurity must become a greater focus for any business that digitally records the information of their customers. This can be problematic for SMBs that cannot afford to keep a dedicated IT department year-round, yet going by the current trend in U.S.-based data regulations, allowances are made for outsourcing cyber protection. Third party MSPs can conduct the required testing of your network security and maintain backups of your data while keeping costs manageable.

Contact us to find out how we may be able to help you keep your data secure and ensure you follow the best practices in network protection.

Shiny gadget of the month:
Samsung's The Wall

It is the month of the Super Bowl, the time of year many people upgrade their TV's for the big game. After seeing this at CES in January I'm sure there are plenty of people that wish Samsung had released their TV dubbed "The Wall" in time. Sure to be the ultimate TV to show off at any Super Bowl party this 146 inch TV is massive. That size translates into about 10 feet wide and nearly 6 feet tall, hence the name, "The Wall".

The Wall was on display at the CES event in January and was Samsung's example of a new module-based design. Meaning this technology allows for the TV to be smaller or even larger by using multiple smaller display panels to create the total size. It uses MicroLED technology, which is similar to OLED in the fact that the pixels do not require a backlight so you can get true blacks and product high contrast images. It is also brighter than most LED LCD displays with a 2,000 nit brightness which enhances the contrast for HDR display.

Samsung says that it will in fact hit the market at some point this year in a range of sizes, but there is no specified date. The new technology and sheer size means that it will likely not be cheap. It is aimed at being more of a home theater product, rather than your everyday TV. Right now Samsung says their major hurdle is manufacturing since it is such a precise process. It will be interesting to see if they are able to tackle it and if this makes it to market. Who knows, maybe next year you could have the Super Bowl up on your entire wall and be the envy of everyone at your party. You can read more about it on Samsung's website.

The Most Common Hacking Attacks

The past few years have brought a lot of attention to several high-profile hacking attempts against big name companies and government agencies. However, some might not be aware of the more common cyber attacks that occur every day, and primarily target individuals and SMBs. The two are not mutually exclusive, and many smaller and mid-sized organizations may be chosen because of the expectation that they will have a harder time protecting themselves.

Perhaps the most widespread goal among the majority of breach attempts is the acquisition of login credentials. Password cracking is often the first step to compromising a system as it allows an attacker access to privileged data. There are many different techniques employed by hackers to discover passwords, quite a few of which require only a certain amount of effort and can be carried out repeatedly.

Socially engineered attacks are becoming one of the most popular new methods for illegally collecting digital information in the current era of the Internet. Cybercriminals are increasingly devoting efforts to studying potential victims and predicting their habits. These types of attempts involve building a delivery system that will not immediately raise suspicion while also usually communicating a sense of urgency. This includes messages from coworkers or c-level officers asking for financial transactions for company purposes, or government agencies threatening legal consequences if their orders are not quickly followed.

Phishing emails are fairly ubiquitous now and are not always easy to spot, but even an accidental click on a message that gets past spam filters can leak information. Spear phishing is a particularly dangerous form of a socially engineered attack that is tailored towards a specific individual, often a gatekeeper for greater access to a company's data. Using information that is available online, hackers can build messages that their victims are more likely to take seriously.

Social media provides an easy way for attackers to identify and study potential targets as people often give away too much of their personal information through their public profiles, including company details. However, social media can also be a vector of attack for malware through fake friend requests or third-party applications.

Attackers also often use fake webpages to spread malware, and even if someone manages to avoid clicking suspicious links in spam emails, there is a chance that they will come across one while surfing the Web. Socially engineered malware adds another danger with websites set up to trap particular individuals based on their preferences. If these sites are visited from a company computer with software that is not fully patched, then the entire network may become infected.

Cyber attacks are becoming more common with each year and they are only going to increase. More frequent, lower-profile threats are growing in popularity among hackers and attempts against SMBs are going to become commonplace. You should find out how safe your business really is with a Network Vulnerability Test, you can even educate employee's to detect these phishing attempts described above with our Phishing Defender service. Or just contact us to find out more.

Gift Card Trivia!

This month's question is:

If your company does business with anyone in Europe what is the name of the new regulation that will take effect this year to protect European citizens information? *(Hint: The answer is in this newsletter.)*

a. NYCRR
b. PCI
c. SWKNWS
d. GDPR

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **March 5th**, 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

Fixes for the Major Intel Chip Bugs Already Experiencing Problems

Only a few days into the new year we saw one of the biggest incidents in cyber security become public. It was discovered that two huge flaws affecting a wide number of Intel computer chips could allow open access to hackers under the right circumstances. It was revealed shortly after that these bugs affect Intel's competitors as well, meaning that these vulnerabilities are present in most modern computing machines, specifically most of the popular PCs, smartphones and servers in use today.

There are in reality three bugs, but two are grouped together to form the "Spectre" flaw, while the third has been labeled "Meltdown." The former can be used to essentially exploit modern processors' predictive functions, while the latter effectively opens up kernel memory locations such as passwords and login information. The nature of these vulnerabilities means that they affect many operating systems, including Windows, macOS, and Linux. The holes were discovered by Google's Project Zero research team in June 2017, and is thought to have existed for at least the past decade.

These bugs create major vulnerabilities on the hardware side, which makes their late discovery that much more impactful. Software will have to be rewritten to better protect against the loopholes if it was originally based on an assumption of security provided by these chips. Intel's own released fixes are being criticized for not doing enough and causing slowdowns for many computers. The situation is further complicated by fake patch downloads being launched by hackers that can infect machines with malware.

Despite the sudden reveal of these bugs, developers are quickly distributing their own updates to deal with the potential threats. Microsoft, Apple, Google and many others have already released patches and will continue to upgrade their software as need be. If you would like to learn more about these vulnerabilities and what we are doing to protect against them, feel free to contact us.