IT Strategy Brief

ISSUE 9 | VOL 4 | September 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Hackers Steal $379,000 in Oregon Wire Fraud Case .....Page 1

What our clients are saying .....Page 1

Industries That Need Virtualization .....Page 2

Survey chance to win a gift card! .....Page 2

Shiny gadget of the month: Samsung's 8K TV .....Page 3

Healthcare Cybersecurity Facing Serious Challenges .....Page 3

TRIVIA .....Page 3

Services we offer.....Page 4

Google Prevents Phishing with Security Keys .....Page 4

Hackers Steal $379,000 in Oregon Wire Fraud Case

An Oregon couple on the verge of purchasing their dream home mistakenly submitted funds meant for their real estate broker and the title insurance agency involved in the deal to scammers who had hijacked their email thread with both of the former. While still communicating electronically with representatives of both organizations, they suddenly received a message in the chain claiming that they needed to send the money immediately to avoid a delay on closing the property.

It was not long after that they contacted their broker to finalize the deal and found that they had lost their $379,000 in a case of wire fraud. "In this case, the emails and the directions on the wire (apparently) came from a trusted source," said Lebanon Police Det. Justin McCubbins.

According to data provided by the FBI, hackers targeted almost a billion dollars' worth of real estate transactions in 2017, which amounted to over a 5000 percent increase from the previous year. The FBI's Internet Crime Complaint Center reported that between 2015 and 2017, there were over 20,000 cases of Business Email Compromise (BEC) that amounted to over $1.6 billion dollars in losses. New information released by the FBI recently states that the volume of losses resulting from BEC and "E-mail Account Compromise" (EAC) from 2013 to 2018 has risen to almost $3 billion in the US and $12.5 billion worldwide.

A significant portion of these were concentrated in the real estate sector as cybercriminals have recently begun to target organizations in this industry due to the large digital transactions being made frequently. This threat is not limited to one area of the market, as demonstrated by a warning the New Jersey Department of Banking and Insurance issued to all businesses involved in mortgage lending in the state. In fact, NJ was one of the states that most frequently experienced wire fraud in 2017, after California, Florida and New York.

The NJDOBI's alert included much of the same information as the FBI's repeated warnings – and both mirrored almost the exact details of the wire fraud incident in Oregon. "There's been a lot of these cases," said Ken Westin, a senior security strategist and researcher in Portland. "I know hackers are going after either title companies or real estate agents. This is becoming pretty common."

Continued on page 2...

What our clients are saying: DiSabatino Landscaping

"The two things I like most about SWK Technologies's services are the immediate attention our calls and emails receive, as well as the benefits of reduced costs and less downtime ever since hiring your company.

We were particularly happy with how SWK Technologies switched out Chris DiSabatino's laptop that he wasn't satisfied with after buying it new.

It is nice to deal with a company that values customer service as much as our company does.

I can't think of anything you can improve. Keep up the good work!"

Tessa Marks
DiSabatino Landscaping

DiSABATINO LANDSCAPING

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

You could win a $25 Gift Card!

Hackers Steal $379,000 in Oregon Wire Fraud Case

Continued from page 1…

The couple managed to recoup a significant portion of the fraudulent wire transfer from Bank of America, which held the account which the hacker directed them to. However, this was only after they exposed the situation to the media and brought attention to the bank, as well as their broker's agency. The couple has since threatened to sue their former broker for imposing closing delay fees and failing to make up for their losses, but the broker contends the liability falls on their former clients.

Though the messages which entrapped the couple came from the same email thread the broker and title agency used to communicate with them, there were obvious grammatical errors and the broker claims that these were warning signs the clients ignored. However, certain factors may give the couple legal precedent to seek damages from the broker, as well as the title agency involved.

A similar incident affected another couple in Denver, who lost approximately $270,000 to wire fraud. They brought a lawsuit against Wells Fargo for not notifying the FBI of the fraudulent wire transfer in time to enact a "Financial Fraud Kill Chain," along with the real estate agent, the mortgage lender and the title agency who had overseen the deal for negligence.

Wire fraud is one of several serious threats to title insurance agencies in the modern real estate market. Learning how to identify and prevent these differences can be the difference between being solvent and a huge loss.

Read our white paper "Common Threats to the Title Industry and How to Prevent Them," to discover how to protect your agency.

Industries That Need Virtualization

Apart from the cloud, one of today's biggest IT trends is virtualization. An emerging model of virtualization is virtual desktop infrastructure (VDI), which involves hosting a desktop operating system and making it available on almost any device. It is most effective in the following use cases:

Healthcare
In an industry where every file is sensitive, the importance of confidentiality cannot be overstated. With virtualization, rules and permissions can be customized based on the individual virtual desktop. As such, every medical professional can only view patient records relevant to them. It also allows them to log into their virtualized desktop while working across a variety of locations and devices.

Academic institutions
By leveraging virtualization, a school's IT team can create a virtual desktop — with the necessary restrictions implemented — for each student. If each classroom has a set of workstations, students' desktop experiences will be consistent throughout their day. Even though they will be using different hardware every hour or two, they will always see the same desktop.

Companies with shift workers
In most cases, shift employees do not need a single designated computer to fulfill their task because one machine is shared by multiple users. VDI makes it easy for companies to manage several desktop accounts on fewer devices. Workers can log into any devices, access their own virtual desktop, work as they do every day, and log off at the end of their shift.

Users with multiple computers
Depending on the nature of work, some positions require working with several computers on a regular basis. With VDI, they can integrate desktops and maintain it across two or more devices.

Field or remote staff
Employees that work remotely or in the field need access to tools and applications when on the job. A secure and reliable way to do it is through virtualization. A complete VDI solution makes access to a consistent desktop experience possible anytime, anywhere, and using any device. It allows your remote or field workforce to operate effectively, no matter the circumstances.

Of course, these are just a few situations where VDI is helpful. Any business can enjoy security and productivity enhancements with a team of virtualization experts on call. Contact us today to find out how we can help.

Shiny gadget of the month: Samsung's 8K TV

Fans of the latest and greatest technology rejoice! We all knew it was a matter of time. Those fancy 4K TVs are the latest and greatest in viewing technology, but sooner or later as with all technology the next advancement comes. This October Samsung will be the first to offer an 8K TV. In case 4K was not crisp enough for you this Fall you could be enjoying football on Sunday in 8K!

Samsung will be launching an 85-inch 8K QLED TV, quadrupling your current pixel count and using advanced AI-driven upscaling that will help you get the most out of the content you have. Their AI-powered upscaling is the real piece of impressive technology here. Since there is a lack of content that can really utilize this high-resolution Samsung was sure to put in the technology to make it worthwhile for consumers. According to those that saw the demo earlier this year the level of clarity and detail with the new upscaling is notably better than what current 4K TVs can do.

Another feature they packed in to try and get you the most out of your TV is to give it a low-powered ambient mode that lets you display art and real-time content like weather and news or other decorative images when not in use. They are also trying to minimize cable clutter have having Samsung's One Connect Box and Invisible Connection that uses a separate box for all your hookups and then connecting to the TV with a single cable (like a docking station).

The one unknown at this point is the price. It is said to be in line with the current QLED model line and due to its immense 85-inch size it is likely to be a five-figure number like their 88-inch 4K TV.

For those that want the latest and greatest this would be pretty cool. LG and Sony reportedly will also have 8K TVs coming soon too, but they have no launch date set just yet.

Healthcare Cybersecurity Facing Serious Challenges

Public institutions such as hospitals have become a favorite target of hackers in recent years, especially for those deploying ransomware. However, the state of healthcare cybersecurity is affecting the entire industry and challenges are emerging now and in the future that threaten the well-being of all medical organizations. These dangers have not gone unnoticed and global healthcare cybersecurity spending is predicted to exceed $65 billion in the next five years.

The particular vulnerability of the healthcare industry stems from several factors: larger than average amounts of critical and sensitive data, extensive and complex infrastructures, and expanding attack surfaces from new digital technology. Healthcare organizations often manage so many patient files that their databases are overloaded and not properly organized, and larger medical facilities must maintain such high staffing volumes – including outside contractors – that magnify the attack surface available to hackers.

In 2017, healthcare organizations experienced an average of 32,000 attacks per day. It was not uncommon for back-to-back breaches to occur day after day every month of the year. The number of people affected by each attack ranged from several hundred at the lowest to millions of patients whose records were stolen or made public.

Ransomware played a significant part in many attacks between 2016 and 2017, but there was a variety of methods employed by hackers to extract money from their victims. In several instances the attackers simply stole the sensitive data, and some of those files were found being sold on Dark Web forums or in other venues. The ultimate fate of the rest of the data is unknown, but personal health information (PHI) is valuable to cybercriminals (at an average of $20,000 per record) as it not only includes standard identifiers, but also offers insurance details and medical history that can be used for more advanced identify theft and fraud activities.

Regulatory agencies are taking the safety of PHI much more seriously and even accidental exposure of information can be heavily punished. Earlier this year, the New Jersey Attorney General fined Virtua Medial Group (VMG), a regional healthcare network, over $400,000 for a data leak that caused the medical records of over 1600 patients to go public online. Even though the leak was caused by an error committed by an outside contractor, VMG was found liable as the ultimate custodian of those files. This sets precedent for greater scrutiny on healthcare professionals to meet compliance with data privacy regulations that designate medical facilities as the caretakers of PHI.

If you work in healthcare or another industry that is similarly beset by mounting cybersecurity concerns and lacks the scalability to address them, then a Network Vulnerability Test would benefit you greatly in measuring the strength of your network security. Visit our website or contact us to sign up today.

Gift Card Trivia!

This month's question is:

According to data provided by the FBI, hackers targeted almost a billion dollars' worth of real estate transactions in 2017, which amounted to over a _____ percent increase from the previous year (Hint: The answer is in this newsletter.)

a. 400
b. 1000
c. 75
d. 5000

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **October 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

SWK TECHNOLOGIES

Google Prevents Phishing with Security Keys

Google confirmed this past July that it has found a currently full-proof method for ensuring its employees do not compromise the network by being phished: physical security keys. All 85,000 personnel employed by Google have been required to utilize USB-based authenticator devices since 2017. Google claims that since implementing the policy, there has not been a single instance of a successful phishing attack.

"We have had no reported or confirmed account takeovers since implementing security keys at Google," said a spokesperson for the company. "Users might be asked to authenticate using their security key for many different apps/reasons. It all depends on the sensitivity of the app and the risk of the user at that point in time."

The Security Keys used by Google are similar to flash drive memory sticks in that they are designed to be plugged into a USB port. Once inserted, the user simply has to press a button to complete their login. As opposed to the multi-step process in two-factor authentication, Security Keys utilize what is called "Universal 2nd Factor" (U2F) that does not require any extra processes or special software drivers to approve access.

Phishing attacks generally either deliver malware through links to an infected landing page or prompt the victim to submit their credentials. In the latter case this information is sought for the purposes of identity theft or to gain access to more valuable data in the case of corporate passwords. Technology entities such as Google are a prime target for such attacks and tech employees surveyed previously have displayed a susceptibility to phishing, along with those of manufacturing and insurance companies.

Two-factor authentication has been increasingly adopted by businesses seeking an extra layer of protection for their physical interfaces. They require users to carry out a second step for logging into the system after they have submitted their password. These vary from push notifications to automated phone calls. However, research has shown that SMS notifications contain loopholes that still allow them to be retrieved by hackers, negating the additional security.

One of the best ways to prevent phishing is to create and enforce cybersecurity best practices in the workplace. Employee awareness can be just as valuable (if not more so) as applying technology solutions to meet evolving trends. Phishing attacks rely foremost on ignorance, distraction and trust to successfully penetrate your network, so ensuring that everyone in your organization knows what to look for should be your first and last line of defense.

Sign up for our Phishing Defender service to get access to training and resources that will prepare you for the next attack.