IT Strategy Brief

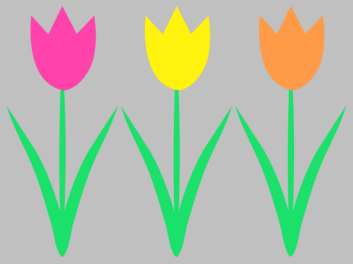
ISSUE 4 | VOL 4 | April 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:



How to Stay Cyber Safe This Tax Season

The growing digitization of personal information is contributing to several cybersecurity concerns, but individual tax data may be especially problematic for potential victims of cybercrime. Personal tax information is encompassing of several identifying details that can be valuable to hackers, including home addresses and Social Security identification numbers. This data can be harvested by cybercriminals for identity theft purposes, such as allowing them to claim tax returns in your name. It can also be sold off online to others looking to profit off of your personal information.

The increasing adoption of social engineering tactics is allowing hackers to single out potential victims much more efficiently, and the sheer volume of data that is exchanged online during tax season offers many possible targets. The IRS warns that criminals targeting tax information are becoming increasingly sophisticated in who they target and how. This includes extending their attacks to new delivery methods and shifting focus to tax professionals and tax preparation software. In addition to scams involving fake calls from the IRS, phishing emails have risen in prominence to contribute to the overall increase in attempted tax fraud.

Phishing for personal tax data has become so pervasive that the IRS has implemented several campaigns to raise awareness among tax professionals. The federal agency has reported on multiple scams in recent years that specifically target tax preparers through phishing emails. These include the false software download messages previously mentioned, which appear as a legitimate email from their tax software provider that directs the recipient to a website with malware disguised as an update for their product.

This malicious software may have a filename that looks virtually similar to the actual tax program, and once downloaded it records keystrokes to extract passwords and other login information. There have even been reports of similar programs that take complete control of the tax professionals machine to remotely allow the hacker to access this data themselves. This approach has also been applied by some cybercriminals to break into personal tax software installed on home computers. Hackers send a similar phishing email that follows some of the same steps to gain entry into the program. At that point, they can obtain the data directly from the source.

Continued on page 2...

What our clients are saying: Giuliano, Miller & Company LLC

"I was working from home and could not get my laptop to connect to my computer at the office. With contractors in my home in the background replacing a window and running into their own issues, SWK walked me patiently through the process of getting and staying connected even with the interruptions. I had to call back a second time with another question and they were just as patient with the issue I had."

Donna Dileo
Giuliano, Miller & Company 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:

Kristen Thorsen
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 **May 4th** to get your name in the hat.

You could win a $25 Gift Card!

How to Stay Cyber Safe This Tax Season

Continued from page 1...

Scammers have conducted several other phishing campaigns that have targeted potential victims with fake email subject lines such as asking for IRS e-Services registration renewal or threatening action if tax returns are not refunded. In addition to federal employees and tax software providers, hackers may masquerade as representatives of banks and credit card companies in order to trick their victims. These attacks are not regulated to tax preparers, but also may often target human resources personnel and those working for educational institutions.

Organizations handling financial data have become big targets for hackers due to the value of the information they store digitally. Cybercriminals are developing their tactics to be able to target gatekeepers of sensitive data more effectively. The availability of personal information online through avenues such as social media enable attackers to seek out and identify potential hacking victims, to the point of being able to build profiles around valuable targets.

If you suspect you may have been a victim of a phishing tax scam, you should inform the IRS right away. If your organization manages financial information for your clients, or if you just want to better protect your data, then contact us to find out about our Phishing Defender solution to ensure you and your employees do not become a victim of a phishing scam.

Employees Don't Realize They're a Cybersecurity Threat

A study released by Kaspersky Labs early in 2018 revealed that out of almost 8000 employees surveyed by the antivirus provider, they found that a little over a tenth were actively informed on their organization's cybersecurity guidelines. 49 percent responded that they saw cyberthreat protection as a responsibility for all company personnel, and almost a quarter said that they were unaware that their organizations even had network security policies in place. Kaspersky had earlier reported in 2017 that they had found that nearly half of IT security incidents experienced by enterprises each year were caused by employees. They also discovered that approximately 40 percent of businesses worldwide had found employees concealing cybersecurity breaches to avoid being penalized, with about 42 percent of the SMBs surveyed included in this segment.

There are several cybersecurity dangers that may arise from uninformed employees, including networks being exposed to malware from phishing emails or dummy websites. The widespread use of mobile devices among personnel also creates serious vulnerabilities, as employees may use their smartphones to access or transfer company data. Many organizations often ignore or overlook data protection for personal and company mobile devices, which leads to an increased level of exposure to external threats in this area. As smartphones and tablets are essentially smaller computers, they are just as susceptible – if not more so – as desktop machines to becoming infected with malware.

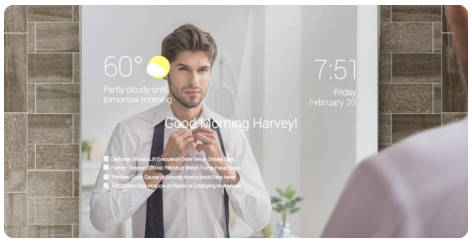
Hackers have transitioned to social engineering strategies to identify and lure in targets, which allows them to more carefully select company personnel who will provide them with a greater return for their efforts. Employees that act as gatekeepers of sensitive organizational data are more valuable potential victims of a phishing attack since they will have login access to this digital information. Human resources, accounting, and other staff that have to manage critical corporate data to fulfill their roles are the most likely candidates. Executives are also more liable to become targets of hackers seeking entryways into company databases, and cybercriminals have developed special campaigns around attempting to breach the cyber defenses of c-level officers.

Cybersecurity ignorance among employees at every level of your organization represents a significant vulnerability that can be exploited by attackers looking to acquire either your or your clients' data. Managing network security is effectively a case of maintaining the strength of the weakest link. Every employee whose role requires them to be connected to the network has to know what can expose them to cyber threats, what techniques can be used to overcome vulnerabilities, and what are the signs of a possible cyber attack. Most importantly, everyone must be ready to report a breach if they believe they might have been hacked.

One of the first lines of defense against network is employee cyber readiness, and that can only be achieved with the right training. Sign up for our Phishing Defender solution to receive access to cybersecurity training resources and employee testing that will help prepare your personnel for potential cyber attack.

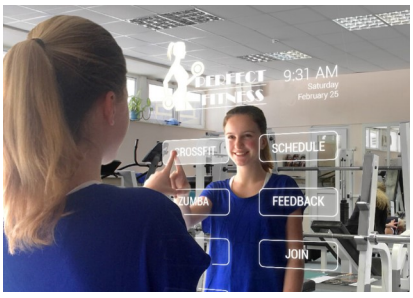
Shiny gadget of the month:
MirrorVue – Smart Touch Mirror

http://evervuetv.com/smartmirror.html



Get ready to step into the future. In this age of information and technology we can never seem to get enough, especially with the busy lives we all live. What would you say to having a computer built into your mirror to display news, weather, and so much more? Brushing your teeth at night wondering what the weather might be the next morning? Maybe you are getting ready for work and want to see what you have on your agenda or get the latest news? The MirrorVue is your answer.

Evervue, a company that offers a variety of display products from smart mirrors, to outdoor all weather TV's has their MirrorVue products that range from a bathroom mirror to commercial products such as mirrors for stores or, as in one example, a gym's mirror wall. Their list of examples are all truly fascinating to think about. A bathroom vanity for home use, a salon smart mirror that you could use for so many applications from entertainment to styling, a conference room mirror that would be sure to impress, even clubs, malls, and hospitals. They possibilities are endless and they all have potential for a unique twist. Perhaps my favorite is the example of using it for a mirror wall at a gym that would have different workouts loaded into it. Even for a home gym, it would be like having a personal trainer to feed you work outs and it would be so convenient to have it right there on the wall.



Almost everyone has multiple mirrors around their home or office, the MirrorVue is a neat gadget that could transform these spaces and would certainly impress. Given how unique this product is you might expect an outrageous price point, but it comes in starting at $999 with the option to add on upgrades, so while it is not cheap it is not strictly for the very wealthy as sometimes these futuristic gadgets are.

These mirrors look like they would be pretty neat. How would you use one?

Dark Web Breaches Can Affect Your Compliance With GDPR

The "Dark Web" is a portion of the Internet that cannot be found using traditional search engine programs, which has made it into a hub for illegal black market transactions. These include illicit items that can be bought and sold physically, as well as digital items such as ransomware and other malicious software. The Dark Web is also a place where individuals can buy and sell corporate data often obtained illegally through network breaches. There have been a few instances where information acquired in high profile hacks, such as the Uber breach last year, was found being sold on the Dark Web.

Though not all data breaches may be inherently linked to the Dark Web, its status as the inevitable marketplace for the information mined in such attacks means that it is irrevocably tied to modern cybersecurity concerns. As by definition it cannot be indexed by search engines, the Dark Web represents a blind spot in cyber defense. Data being sold here will not be discoverable through standard means, which may allow breaches to go unnoticed for some time.

This can become a complicating factor in establishing compliance with the European Union's upcoming General Data Protection Regulation (GDPR), which mandates a complete redefinition of what constitutes personal information. It establishes that any data that can be used to identify an individual will become their personal property and that organizations must make every effort to inform EU citizens if they intend to collect such information from them. Another key provision of the new law stipulates that companies must immediately alert anyone whose data they store of a suspected breach.

Once data appears on the Dark Web, it may be ruled as visible under the GDPR and be grounds for penalization. As data grows in value, attempted cybersecurity breaches for the sake of mining sensitive information will only increase. Many networks have several loopholes that can be exploited quietly by hackers using techniques such as phishing. Your data can be stolen without any major signs that a breach occurred.

Maintaining compliance with the GDPR means not only taking every measure to secure your network, but also to proactively determine if you may have ever been the victim of a data breach. Contact us to learn more about our Dark Web ID scan which may help you discover if any of your information is out there in the Dark Web.

Gift Card Trivia!

This month's question is:

What is the Dark Web? *(Hint: The answer is in this newsletter.)*

a. An offline version of the internet
b. A new search engine
c. A portion of the Internet that cannot be found using traditional search engine programs
d. When you surf the internet with no lights on

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **May 4th**, 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

SWK NWS Recognized for Excellence in Managed IT Services

SWK Technologies, Inc. recently announced that CRN®, a brand of The Channel Company, has named SWK's Network Services has been named to the 2018 Managed Service Provider (MSP) 500 list in the Elite 150 category by CRN®. This annual list recognizes North American solution providers with cutting-edge approaches to delivering managed services. Their offerings help companies navigate the complex and ever-changing landscape of IT, improve operational efficiencies, and maximize their return on IT investments.

In today's fast-paced business environments, MSPs play an important role in helping companies leverage new technologies without straining their budgets or losing focus on their core business. CRN's MSP 500 list shines a light on the most forward-thinking and innovative of these key organizations.

The list is divided into three categories: the MSP Pioneer 250, recognizing companies with business models weighted toward managed services and largely focused on the SMB market; the MSP Elite 150, recognizing large, data center-focused MSPs with a strong mix of on-premises and off-premises services; and the Managed Security 100, recognizing MSPs focused primarily on off-premise, cloud-based security services.

"We're proud to be named to the CRN MSP500 Elite 150," said Mark Meller, CEO of SWK. "The SWK NWS team, under the leadership of John McPoyle, Kevin Snyder, Deivid Pinto and others, has done a tremendous job of helping our customers navigate the challenges and complexities of today's cyber environment. Our team demonstrates every day how we delight our customers by providing solutions and expertise that transform their businesses and enable success. Through innovation and best practices, I expect we will climb even higher in 2019."

"Managed service providers have become integral to the success of businesses everywhere, both large and small," said Bob Skelley, CEO of The Channel Company. "Capable MSPs enable companies to take their cloud computing to the next level, streamline spending, effectively allocate limited resources and navigate the vast field of available technologies. The companies on CRN's 2018 MSP 500 list stand out for their innovative services, excellence in adapting to customers' changing needs and demonstrated ability to help businesses get the most out of their IT investments."