IT Strategy Brief

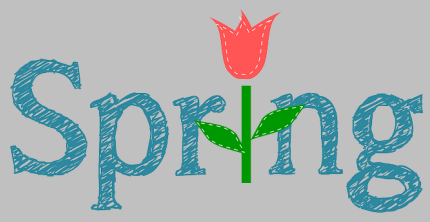
ISSUE 3 | VOL 6 | March 2020

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:



Using Big Tech Brands Can Expose You to Ransomware

Recent research reveals that ransomware hackers are increasingly impersonating big brand technology companies to breach enterprise networks. Specifically, those impersonated are often application providers such as Microsoft, with attackers masquerading as recognizably branded partners to phish unsuspecting SMB victims. Digital service systems - namely PayPal – that have expanded into the B2B space are also quickly gaining on and even surpassing many business suites as the vehicle for phishing malware.

Top Brands Used for Impersonation Phishing

Speaking to PYMNTS, Chief Solution Architect Adrien Gendre of Vade Secure claimed that hackers mimicking trusted brand names highlights a growing trend among phishing. Cybercriminals have historically relied on the mixture of faith and compulsion potential victims have when responding to messages that proclaim to represent a recognizable service. This can include a big corporate name as well as a government agency, the latter of which often generates an even greater urgency to respond.

According to Vade Secure, Microsoft saw the most popularity for being impersonated in Q4 2019, but PayPal saw the biggest increase overall last year. Given that the platform has extended its services into the B2B market, cybercriminals can take advantage of the decreased scrutiny for wire transfer or account credential requests. However, Microsoft's sudden surge correlates with a similar ransomware rise and may also result from Office 365's potential as a vehicle for malware, meaning that a data breach can grant control of a network to a smart hacker.

Continued on page...2

What our clients are saying: Foundation Title LLC

"SWK has been very helpful and polite when assisting with our technical issues while providing excellent service. I was having several issues last week with my computer after returning from medical leave and Michael M from tech support (supervisor) was extremely helpful in getting my problems solved."

Lori Lynch
Foundation Title LLC

FOUNDATION TITLE

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Anthony D'Agostino
Pee Jay's Fresh Fruit

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 31st** to get your name in the hat.

You could win a $25 Gift Card!

Using Big Tech Brands Can Expose You to Ransomware

Continued from page 1…

Business Email Compromise Used for Ransomware
Ransomware became the most commonly reported malware threat in 2019, and is expected to turn even more dangerous in 2020. Though trends have varied between frequency and ransom volume, there have been more and more cases of targeted spear-phishing campaigns used to deploy malware, especially ransomware. The evolution of breach, infection and ransom payment models seem to reflect a significant growth among hacker circles - in other words, some have gotten smarter about how they work.

Given that in 2018 business email compromise (BEC) was successful more often against employees of smaller companies, SMBs will likely face new phishing campaigns in the near future. The potentially crippling costs of downtime combined with lack of access to serious cybersecurity resources makes smaller businesses much easier targets for hackers. Compared to the damages from exposed data and unusable networks, whatever ransom they ask for will probably seem reasonable to the victim.

Watch Out for More Ransomware Threats in 2020
Ransomware infections increased by 41 percent in 2019, according to the New York Times. While phishing and business email compromise are not new, the network breaching possibilities are being increasingly leveraged by enterprising hackers that see a golden opportunity to make easy money.

Download our latest Ransomware Report to learn which trends to watch out for and how to better protect your vital data.

NY Proposes Banning Ransomware Payments

A bipartisan-sponsored bill was introduced in the New York State Senate earlier this year that would ban payments to ransomware hackers using taxpayer funds. Given that many of the (known) targets of ransom demands have been public institutions, this could effectively draw a line in the sand against paying off cybercriminals to unlock infected files in NY. The bill also contains provisions for establishing a cybersecurity improvement fund for smaller municipalities in the state.

NY State Senate Bill S7246 - Cybersecurity Revisions
The underlying theme of the proposed legislation (Senate Bill S7246) is to take charge of and completely revamp the state's response to ransomware. This will be achieved twofold by explicitly forbidding the use of taxpayer monies to pay ransoms after January 1, 2022, and by incentivizing investing in network security controls. "A small investment in local government cyber security now, can help stop cyber-criminals from profiting on the backs of New York State taxpayers…" as stated in the bill.

Under the current terms of the proposal, this "cyber security enhancement fund" will amount to $5 million and be available to local governments through "grants and other forms of financial assistance." While the fund will be managed by the state comptroller, the NY Division of Homeland Security and Emergency Services (DHSES) will be in charge of creating and overseeing the state cybersecurity training program.

Ransomware Targeting Local Governments and Schools
Many government agencies, school districts and other public institutions have been victimized by malware in recent years, with disruptive and expensive consequences even in many cases where ransom was paid. Network downtime brings all municipal activities to a grinding halt, preventing access to records and critical government functions. Data restoration is often the biggest expense for cities and towns that must ensure citizen information is up to date and accurate.

Continued on page...3

Shiny gadget of the month: Mobile Pixels DUEX Pro

Today's workforce is more mobile than ever. Many companies offer work from home options, or even if they don't just about everyone has worked out of the office for one reason or another. The one difficulty with working while traveling or taking your laptop home is that you might lose out on some of the amenities of working in an office, such as having multiple monitors. If you are used to having more than one monitor you can surely attest to the difficulty of adjusting to just a single laptop monitor when you go mobile and work outside the office. However, Mobile Pixels created the DUEX Pro to solve this very problem.

The DUEX Pro is a 12.5 inch second screen for your laptop. Now, when I say second screen it does not mean a separate monitor that you sit on a desk, but instead a monitor that is neatly tucked behind your existing laptop screen and slides out next to it, all while remaining attached to your laptop. At 1.7 lbs it is light weight and easily stows away with your laptop to make transportation simple as if it was never there. The DUEX Pro was designed to be energy efficient too so that you don't drain your battery.

The way it works is by using adhesive magnets you attach to the back of your laptop screen. The DUEX Pro has a housing that magnetizes to the back of the laptop screen. You then just attach the USB cable to the screen and you're all set. It has the ability to slide out to the side, or completely flip around to present your screen on the back for someone sitting in front of you too.

Mobile Pixels designed their DUEX Pro for just about everything. Work, play, travel, productivity, and most importantly affordability. They wanted everyone to have access to such a game changing gadget that they made it a point to keep pricing affordable. At $250 it is not something that breaks the bank, and has the utility of something you would expect to cost more. You can see more about the DUEX Pro on their website https://www.mobilepixels.us/. Is this something that you think would help with your productivity? Let us know!

NY Proposes Banning Ransomware Payments

Continued from page 2…

While several mayors and municipal leaders across the country have taken a stand against paying hackers their ransoms, there have been quite a few public executives that have simply complied. It is easy to see why, with the payment demands often seeming much less than the costs of doing nothing. As even many promising miracle technology solutions for removing ransomware have been caught sending payments as well, for some there appears to be no easier response than giving in.

Paying Off Hacker Ransoms
The question whether to pay off ransomware hackers is not limited to the public sector, as studies have shown that most executives of infected businesses often opt to pay the ransom. Yet the spread of the malware over the years, by the same culprits, reinforces the warnings made by the FBI and cybersecurity experts - the payments have only emboldened cybercriminals.

Time will tell whether Bill S7246 is a step in the right direction, but the idea behind the legislation certainly rings true. Unfortunately, there have been no proven consistent methods for breaking ransomware encryption, but paying the ransom in no way guarantees data retrieval - even if hackers act in good faith and return access, damage done by file locking can compromise information anyway. Only cybersecurity training and secure data backups have been able to mitigate the harm caused by malware.

Learn How to Fight Back Against Ransomware
Research shows that ransomware is picking up in 2020, and propelled by the success and profit of previous years, cybercriminals will deploy new and refined techniques for breaching your network. Learn how to protect your business against file encryption by securing your data against all forms of malware.

Download our free Ransomware Report to discover the trends for yourself and find out how to defend your data.

SWK Technologies Recognized on CRN 2020 MSP500 List

SWK Technologies, Inc. is pleased to announce that CRN®, a brand of The Channel Company has named SWK to its 2020 Managed Service Provider (MSP) 500 list in the MSP Elite 150 category. This popular list identifies North American solution providers that deliver operational efficiencies, IT system improvements, and a higher rate of return on investments for their customers.

SWK Technologies previously captured Elite 150 placement in 2019, 2018 and 2017 as well, along with multiple other CRN awards including the Solution Provider 500 and the Fast Growth 150. The MSP Elite 150 recognizes large, data center-focused MSPs with a strong mix of on-premise and off-premise services.

Continued on page...4

Gift Card Trivia!

This month's question is:

What company saw the biggest increase overall last year for being impersonated? (Hint: The answer is in this newsletter.)

a. Apple
b. Target
c. PayPal
d. Intel

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **March 31st**, 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 NETWORK SERVICES

SWK to Attend NJLTA Group Meeting March 25, 2020

SWK Technologies will be attending the next New Jersey Land Title Association (NJLTA) Group Meeting at the Forsgate Country Club in Monroe, NJ on March 25, 2020. SWK's Network Services (NWS) division will feature a booth at the event to meet with attendees and answer their questions on transaction and data security.

SWK NWS regularly attends events hosted by the NJLTA as well as other title insurance and real estate associations to be able to educate attendees on the cyber threats the industry faces, including:

- Phishing
- Data Loss
- Wire fraud
- Ransomware
- Hardware and Software Vulnerabilities
- And more

The title market in particular can be susceptible to network vulnerabilities and wire transfer fraud scams due to the social and communicative nature of the business. Constant email communication and big money transfers make title agencies tempting targets for hackers. With enough patience and skill, determined cybercriminals can stalk transaction email threads and phish buyers with spoofed messages that direct payment to an account of their choosing.

SWK provides several network and IT service solutions to multiple title insurance clients, including Fortune Title Agency of Roseland, NJ and Foundation Title, LLC of Mercerville. Our extensive experience in this sector allows us to best serve our clients' needs, protect their networks and even help solve financially damaging cyber threats for themselves as well as their own customers.

Stop by our booth at the NJLTA Group Meeting to learn more, or Contact Us here.

SWK Technologies Recognized on CRN 2020 MSP500 List

Continued from page 3…

"MSPs are the critical bridge for customers looking to assess, implement and migrate their IT and cloud solutions to drive efficiencies, lower costs and secure your environment," said Bob Skelley, CEO of The Channel Company. "On behalf of our team at The Channel Company, I want to congratulate the accomplished companies on CRN's 2020 MSP 500 list and thank them for their commitment to finding innovative solutions that move the IT channel forward."

"I'm grateful to CRN for continuing to recognize SWK's strong contribution to the MSP space," said Bill Michael, VP of Operations for SWK Network Services. "But most importantly, I'm proud that our team has continued to go above and beyond in providing technology solutions that deliver value to our customers while still protecting their networks against the many threats that lurk in cyberspace."

The MSP500 list will be featured in the February 2020 issue of CRN and online at www.crn.com/msp500.

THE CHANNEL CO. CRN MSP 500 2020