IT Strategy Brief

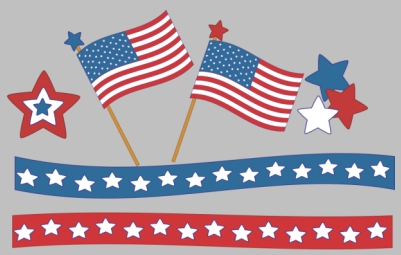
ISSUE 7 | VOL 5 | July 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:



Philadelphia Online Court Network Shut Down by Infection

Not long after Baltimore, MD was hit with a malware attack that crippled several of their city government's systems for weeks, Philadelphia's First Judicial District (FJD) discovered their network had been compromised by their own malware infection. Though the city government has yet to reveal the exact details of the digital culprit, it is known that the online domain first went down sometime May 21, with the Philly court system making it known through social media the following day. After a few false starts, the city confirmed that it restored most of their web properties by June 26, with the exception of three online portals.

Unknown Culprit

City officials have remained unclear on how the attack occurred or what type of infection it was, or even to what extent the FJD's system was compromised. The only details they have revealed are that a portion of the machines on their network were found with a yet-to-named virus that forced them to shut down their website and user portals. Some officials have given conflicting reports on the origins of the virus, with at least one claiming it came from Russian hackers.

Back to Paper and Slow Lines

Wherever the cyber attack came from, the result remains the same – the FJD cut off electronic access to the majority of its resources, forcing attorneys, administrative personnel and citizens to revert to paper filings and face-to-face bureaucracy. Despite some leeway promised by the Philly courts' Twitter account, several residents were held at the mercy of the city's communication blackout and the disconnect between the various government branches.

City Cyber Attacks

Baltimore, Philadelphia, and now Key Biscayne, Riviera Beach and Lake City in Florida are the latest in a long line of US municipalities that have been targeted by malware attacks. The most common vehicle has been ransomware, with hackers encrypting critical files and demanding payment in cryptocurrency. One such infection occurred in Newark, NJ in 2017, which was eventually traced back to two Iranian cybercriminals who had been previously targeting NJ businesses before they moved onto the public sector.

According to CNN, at least 170 government systems have been targeted by hackers since 2013. The report they site also emphasizes that many ransomware attacks go unreported, contributing to the lack of security awareness among public entities. Mayor of Atlanta, Keisha Lance – whose city was also a victim of the same Iranian ransomware that hit Newark – went before a congressional subcommittee to raise awareness on the need for better cybersecurity among city governments.

Continued on page 3...

What our clients are saying: Scirocco Financial Group

"One of the key issues for us is being able to consistently maintain our data, back up, have all information at hand at a moment's notice, and with that, SWK has performed a very, very big and helpful service to our organization in knowing the stability's there for us to have that information on an ongoing basis."

John Scirocco
Scirocco Financial Group

SCIROCCO GROUP INSURANCE

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Cindy Daley
Friendly Planet Travel

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

You could win a $25 Gift Card!

Most Data Breaches Come from Privileged Credential Abuse

As it turns out, having the same password for every account may not be the best idea. 74% of data breaches start with privilege credential abuse. Privileged credentials are the user names and passwords that are given administrative privileges- the accounts used by your IT resources, executives and accounting personnel. Hackers are getting access into these accounts through methods such as phishing scams, key loggers, etc., and using them to steal data or money from the organization. What measures your company takes to protect against these attacks can be the difference between a minor inconvenience and bankruptcy.

Multi-Factor Authentication
So why is this happening? Well, for starters, only 21% of companies have Multi-Factor Authentication (MFA). MFA is a quickly growing cyber defense method which is increasingly becoming more and more vital to protecting your company.

Multi-Factor Authentication can prevent data breaches from privileged credential abuse by creating an extra step between having a password and logging into an account. Multi-Factored Authentication is a must especially if you are based in the US, as a survey has found that U.S companies tend to lose $3 million more than the global average from data breaches.

Internal Data Breaches
Hackers aren't the only problem that you have to watch out for - sometimes a data breach can be intentional from within your own company. 18% of healthcare employees are willing to sell data to unauthorized parties, which could include your social security number, health records, and phone number. This 18% said they would be willing to sell this data for as little as $500 to $1,000, a small profit for a transaction that could cost your business millions. Having a secondary step to log in, even after a password has been sold or stolen, can stop any malicious intent dead in its tracks.

Prevent Your Privileged Credentials from Being Abused
In today's IT landscape, not taking essential precautions to protect your business is borderline negligent and could cost you millions. Simple measures to protect against the leading cause of data breaches, privileged credential abuse, such as having a password vault or using multi-factored authentication go a long way and are a must have for adequate security. Make the simple and easy choice, reinforce your security to protect your business.

Click here to learn more about how Multi-Factored Authentication can not only offer you more security, but could one day stop a hacker from breaching your data

New hacking techniques developing on mobile and an old one on the rise

When it comes to trying to infiltrate a network there is only one method that cybercriminals truly care about…the one that works. While new methods are always being devised, sometimes the old methods get just as many results, if not more. Phishing remains one of the most popular infiltration techniques and scammers have access to many tried and true methodologies, yet seem to always develop better versions every year.

Phishing Domains
Researchers at Proofpoint revealed in the *2019 Domain Fraud Report* that the number of fraudulent and malicious domains continues to grow. These websites are often used in conjunction with phishing schemes and will use tactics like creating a legitimate website with a single typo in the URL so that at a glance you would never notice, or will use two letters together like an "r" and "n" so it appears like an "m" at a glance.

You may not realize you are on a fraudulent website and could enter in your credentials giving the hacker access to your real account or login. These types of scams are not new, but the numbers show they continue to be used.

Mobile Site Phishing
A new scam takes these fraudulent websites into account but uses your phone as the point of access. Scammers are coming up with push notifications that will pop up on your phone directing you to a fake website where you may be asked to enter credentials. This new technique was detected by the mobile security company, Lookout, in recent months.

It is still fairly new, but they have discovered examples of this where a Chrome notification pops up alerting them to a missed call or display a logo that leads to a fraudulent site. Researchers have also detected examples where based on the width of the screen it will take you to the real website (if you are on a desktop), but if it is a mobile device it will send you to a fake site. The aim here is to use people's trust in mobile devices against them, with the rising numbers of mobile users it only makes sense they will start to emphasize mobile as a target more.

Continued on page 3...

Shiny gadget of the month: Chill Cooler

It is officially summer and that means spending more time outside. Whether that means taking a vacation, a day trip, or just a barbeque in a backyard people like to enjoy the warm weather. It also means people like to back food and beverages in coolers to help them beat the heat and that means loading it up with ice which inevitably takes up space and melts turning into a pool which can be troublesome if you have food in there. Well that doesn't have to be the case anymore, gosun has created a solar cooler that doesn't need ice and aptly named "Chill".

Chill is essentially a solar refrigerator. It will keep everything clean and dry since no ice is needed, it even boasts temperature control so it is cold enough to make ice inside it should you still want some. Also, since you don't need ice it leaves more room (fits 55 cans) for extra stuff! The power bank in it can last up to 24 hours and since it has solar capabilities you can have it last even longer should you need it. The power bank can detach so you can use it to power other devices when you don't need the cooler. If you're worried it might be too big and heavy or cumbersome don't worry it comes with a telescoping handle and wheels so you can easily bring it on your travels. There really are so many features and details packed into this gadget that you will have to check out more for yourself on their website https://www.gosun.co/pages/chill.

The Chill really seems like it would be pretty awesome to have, not only as a cooler, but the added multi-functioning power bank is useful too. While the price may seem steep at $579 (currently a discount for pre-orders) when you think about it compared to something like a similar sized Yeti cooler it really isn't that bad of a deal. It would certainly be something unique to show off at your next barbeque and would be amazing for camping where you may not have access to keep things cool for a weekend otherwise. This could be a really cool gadget to have, what do you think?

Philadelphia Online Court Network Shut Down by Infection

Continued from page 1…

Data Protection
As the victims of the ransomware epidemic unfortunately continue to demonstrate, coming back from a successful attack can be expensive. Despite this, many public and private institutions allow themselves to remain at risk by not following data security best practices and ignoring critical loopholes in their network defense. Any combination of higher data file volume and endpoint proliferation creates a serious network vulnerability, such as in a legal system defined by consistent technology use.

The reality is that we live in an increasingly online world, and while that may have been a novel concept a decade ago, we are now subject to the fast pace of the digital age. Internet connections deliver everything quickly, including malware. Your data is no longer a collection of spreadsheets and folders sitting on a desktop – it is a valuable asset that can be stolen, deleted, or exploited.

Back Up Your Data to Defend Against Malware Infection
Ransomware was expected to diminish in 2019, but this latest string of attacks indicate that cybercriminals are only adjusting targets as they discover more vulnerable networks. The only way to protect against the harm of ransomware without giving to hackers' demands is to ensure your data is backed up and secured.

Download our report on backup and data protection practices for SMBs to learn why a backup solution is integral for any organization.

New hacking techniques developing on mobile and an old one on the rise

Continued from page 2…

Google Calendar Scam
Notifications are not the only mobile threat either. Another instance was identified by Kaspersky Labs in a report from *Wired*, in which bad actors are taking advantage of a Google Calendar from a setting that allowed anyone place event invites on another person's calendar. In this scam an event pops up on your calendar and the description will have some sort of offer prompting you to enter in personal information.

While this may draw red flags for some, others may not think as much of it since it is just an event on your calendar, and depending on your settings an alert from your calendar could pop up prompting you to act on it. There are also reports that in the details of the appointment lies a malicious link that looks like it's pointing you back to meet.google.com for more details - instead infects you with malware. However, users can guard against the attack by changing their Google Calendar privacy settings:

> "Open Google Calendar's settings on a desktop browser and go to **Event Settings > Automatically Add Invitations**, and then select the option 'No, only show invitations to which I've responded.' Also, under **View Options**, make sure that 'Show declined events' is unchecked, so malicious events don't haunt you even after you decline them."

The Common Trend in Every Phishing Attack - Timing
There will always be new gaps for a hacker to exploit simply due to technology evolving, but if you stay aware of techniques and use caution on the web you can protect yourself. SWK offers tips, tricks and other resources that will help you prepare yourself – and your business – for the modern threats in cyberspace.

Visit our blog to get the latest news and updates network security and the rest of the cyberworld.

Gift Card Trivia!

This month's question is:

How long was the Philadelphia court system computer network crippled? (Hint: The answer is in this newsletter.)

a. Less than a week
b. Over a month
c. Two Weeks
d. One Day

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

12th Annual MSP 501 Identifies Top Forward-Thinking Global MSPs & Leading Trends in Managed Services

SWK Technologies, Inc. has been named as one of the world's premier managed service providers on the 12th-annual Channel Futures MSP 501 rankings.

Every year, MSPs worldwide complete an extensive survey and application to report their product offerings, growth rates, annual total and recurring revenues, pricing structures, revenue mix and more. MSPs were ranked according to a unique methodology that weights revenue figures according to how well the applicant's business strategy anticipates trends in the fast-evolving channel ecosystem.

Channel Futures MSP 501 2019 WINNER

Channel Futures is pleased to name SWK to the 2019 MSP 501.

"The 2019 MSP 501 winners are the most elite, innovative and strategic IT service providers on the planet, and they stand as a model of excellence in the industry," says Kris Blackmon, Content Director of Channel Partners and Channel Futures and lead of the MSP 501 program. "As the MSP 501 Community grows, leagues of managed service providers learn from the successes of these winning companies, gaining insight into the best practices, strategies and technologies that elevate an MSP to the level of the 501 winners. Our heartfelt congratulations to the 2019 winners and gratitude to the thousands of MSPs that have contributed to the continuing growth and success of both the 501 and the thriving managed services sector."

"SWK continues to solidify our place as a top managed service provider that delivers the best in IT solutions to our customers," said Bill Michael, VP of Operations for SWK Network Services. "Our repeated placement on Channel Futures' MSP 501 selection reflects the effectiveness of our practices and the sustainability of our growth strategy."

In the 12 years since its inception, the MSP 501 has evolved from a competitive ranking list into a vibrant group of service providers, vendors, distributors, consultants and industry analysts working together to define the growing managed service opportunity.

Ten special award winners will be recognized at the MSP 501 Awards Gala at Channel Partners Evolution, held this year September 9-12 in Washington, D.C. Nominations for these special awards, including Digital Innovator of the Year, Executive of the Year and the Newcomer Award, were included in the MSP 501 application, and all candidates were encouraged to submit for them.

In addition to deciding the rankings, the survey drives the creation of an annual in-depth study of business and technology trends in the IT channel, released each year at the Channel Partners Evolution conference. The full MSP 501 Report leverages applicant responses, interviews with industry experts and historical data to give a well-rounded picture of the managed services opportunity.

The complete 2019 MSP 501 list is available at Channel Futures.