# IT Strategy Brief

ISSUE 7 | VOL 6 | July 2020

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

## What's Inside:



## Top Cybersecurity Lessons Learned from COVID-19

The COVID-19 pandemic and resulting shutdowns have imparted many lessons in cybersecurity for businesses and organizations across the US. The massive migration to working from home for many institutions and groups has created a new normal of digital communication and data transfer. Many of the network security issues that have risen to the top are not new, but the crisis has served to either amplify or moderately transform the threat factor posed by these developments.

Here are six of the top cybersecurity lessons we have learned from the COVID-19 pandemic:

**Cybercrime Still Using the Same Tricks**
It should come as no surprise that hackers and cyber scammers are falling back on their more common tactics, but it is still worth noting that they seem to be regrouping around these older strategies. Cybercriminals are susceptible to same disruptions affecting everyone else, and may even be seeing newcomers seeking to replace lost income sources join their ranks. The traditional methodologies have proven themselves effective precisely because they rely on the thing it is always hardest to defend against - human error.

**Phishing Reigns Supreme**
It is also not surprising that phishing emails are still the preferred technique for network breaches. Business email compromise is still one of the most efficient vehicles for breaking through (or, more accurately, slipping through) safeguards and gaining direct access to users and their data. This avenue presents many options for execution to a persistent hacker, from credential stealing to malware delivery. This is also one of the reasons that ransomware became prolific, as it can be transmitted silently through the right spoofed email or phony domain, and just as quietly move to lock down files before even being noticed.

**Hackers Rely on Emotions - Panic, Desperation, Anxiety**
The COVID-19 crisis has certainly made clear just how predatory cybercriminals can be, with hospitals and healthcare workers on the frontline of the pandemic often being the hardest hit. Many have also tried to leverage the fear, uncertainty and misinformation surrounding both the coronavirus itself and the disruptions it has caused. Phishing emails that have gone out since shutdowns began to be implemented have included language around cures, tax relief and unemployment loans, seeking to take advantage of those trying desperately to find the right information.

**Data is in Everyone's Hands**
With many companies having the majority of their employees work from home for the first time, it is becoming increasingly clear just how important the user is in data protection strategy. Millions of remote workers are logging into remote computers and cloud servers, potentially with unsecured personal devices and network connections. Data is being shared between several internal and possibly even external parties, including partners and former employees.

Continued on page 2...

## 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:

**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?**

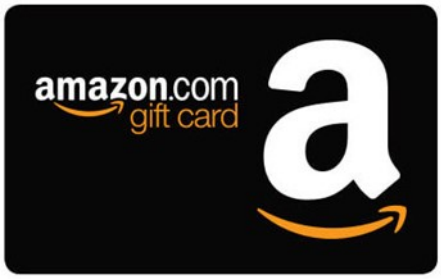
**2. Tell us about a specific experience with us that you were happy with.**

**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 **August 3rd** to get your name in the hat.

## You could win a $25 Gift Card!




# Avoid the New Jersey Shore Rental Scams this Summer

Learn how to avoid the shore house and other rental scams already being seen this summer in New Jersey and neighboring states. Cybercriminals will lure people in with affordable rental deals for promising homes, which often they do not own or simply don't exist. With the Spring of 2020 being practically stolen by COVID-19 and social distancing requirements, scammers know that people are desperate for both time away and cost savings on vacation homes, offering plenty of potential victims.

***Fake Online Listings for Rentals***
Jersey shore rental scams have operated for years with many different perpetrators and victims, though the general layout of the grift is often the same. The scammer will take the information of an actual home from existing listings, previous listings or just from a general search of potential houses. The scam listing will then be placed on a site such as Craigslist, though AirBnB rentals have started to appear as an easier con vehicle (more on that later).

One unfortunate victim fell for a fairly sophisticated version of this scam that offered a home in Forked River, wherein the scammer used the real owner's identity and sent realistic-looking documentation to sell the con. In Wildwood, a local realtor stumbled across a former client's home being rented online in a suspicious-looking listing, and proactively contacted the owner to discover that it was indeed fake. In both of these cases, the scammers had access to just enough information and resources to fool anyone who had only done a cursory search of the property.

***Not Limited to Just the Shore - or NJ***
Unfortunately, these types of scams can be quite common throughout both the state and the country. In nearby Philadelphia, several would-be renters showed up on the same day to their new apartment - only to discover it was actually an AirBnb rental. The Internet allows for a degree of separation for private listings that scammers can leverage easily, especially during the social distancing requirements of COVID-19.

***Avoid Too Good to be True Deals and Check the Details***
Avoiding a rental scam is the same as avoiding most over cyber scams, including with phishing emails or domains. If something is too good to be true, it probably is, and no matter how badly you need that discount you should never wire a payment without physical confirmation. The request for wire payment itself is often a good indicator that the list is not legitimate, as wire fraud can be hard to trace before the perpetrators disappears with the money.

***Learn How to Protect Yourself from More Cyber Scams***
Whether it's a rental or your business data, scammers are always going to separate you from your money. Stay up to date with ways to spot the latest scams and how to quickly protect yourself from the fallout.

Contact SWK Technologies for more help with avoiding cyber scams.

# Top Cybersecurity Lessons Learned from COVID-19

Continued from page 1...

**Telecommuting Needs Cybersecurity Practice and Training**
Working from home is an entirely new environment for many, and it shows in just how many newly telecommuting employees are ignoring even standard cybersecurity procedures. So much education and training language focuses on the office worker's role in network security, with limited oversight for traveling and remote users. The new normal requires new ways of thinking, and the top of this list should include improved training for employees that work from home while still logging into a business account.

**Your Tools and Credentials Need to be Secure**
The Zoom video conferencing app saw an increase of several hundred million daily users once COVID-19 forced everyone to work from home - it also saw a huge surge in data security gaps and scrutiny. Digital communication tools have enabled everyone to adapt the pandemic and minimize disruption, but they also require network hardening and oversight to prevent being used by hackers. Webcams, microphones, and motion sensors can be exploited by malware and unpatched remote code execution (RCE), so keeping your software and hardware up to date is critical when telecommuting.

**Don't Let the Cybersecurity Lessons of COVID-19 Go to Waste**
There are many cybersecurity lessons being learning during COVID-19 and likely still more to come. However, often these just reinforce known truths about protecting your network and data. Ensure that you have all the support you need to defend against phishing, ransomware and more in this pandemic by engaging an MSP like SWK.

Contact SWK Technologies today to learn more lessons about protecting your IT investment.

## Shiny gadget of the month: Tube Runner


Summer is in full swing now and with options more limited than usual this summer people are looking for fun new ways to cool off. Fortunately, there is an fun new inflatable tube that is sure to be the talk of the pool, lake, river, or wherever you are able to get to the water.

PoolCandy Tube Runner is a motorized tube that is sure to be the envy of the water. This inflatable tube uses a joystick to control a propeller that is safely enclosed to prevent injury. It can go in 360 degrees for sharp turns, spins, and whatever else you want to do. On their website they show off the tube in action and it looks pretty fun. From being able to just motor around a pool, to playing bumper cars, going to retrieve a drink at the edge of the water, you can have some fun with this gadget.

It is a little surprising that this sort of thing has not been out for a while, it looks incredibly fun to use and is a simple design. You use a joystick to control the propeller direction and thrust. It is powered by 6 D batteries, has a enclosed propeller, and is large enough for an adult to sit comfortably in along with a drink holder. What more could you want?

At the moment the Tube Runner is up for pre-order and will be shipping later this summer. The only real drawback appears to be the price at $130. While it seems a little pricey for an inflatable pool toy it really is a fun idea. Who wouldn't want to spend a little extra to motor around the water on their float while everyone else is drifting around aimlessly? Would you buy one of these? See more for yourself on their website.

## Fight Over Zoom Encryption Gets More Complicated

The debate over the benefits and vulnerabilities of Zoom is becoming even more complicated as Zoom was forced to walk back a previous decision to deny End-to-End Encryption (E2E) for free users. As millions of new users took to the video conferencing tool during the coronavirus pandemic, it was quickly discovered that Zoom's cybersecurity features were not all that was promised. After several additional scandals and responses by the company's CEO, Zoom encryption is finally receiving an update in 2020.

***Mass Migration to Zoom During COVID-19***
COVID-19 and the shutdowns it caused in the name of social distancing saw many leverage video technology to continue personal interactions as well as work from home. Zoom quickly rose to the top of the list of preferred application as the company boasted it saw 300 million daily meeting participants in April 2020 (up from only 10 million in only five months). The relatively easy features and availability of the app saw it being used for multiple contact channels, from business meetings to classroom lectures, and even to government proceedings.

***Lack of Encryption and Cybersecurity Uncovered***
However, a practice labeled "Zoombombing," where victims were harassed by bad actors who had broken into their video calls, brought the state of Zoom's security into question. The app had had a few major exploitable bugs revealed publicly in recent years, but now that the user base had grown so exponentially, there was a much bigger backlash and considerable scrutiny followed. In reality, the consistent cybersecurity gaps hinted at a much bigger problem with the app's data security controls, but the extent was unknown the spotlight forced it to the forefront.

Zoom's marketing had misled customers - despite claims of sophisticated encryption through EE2E, any video chat actually had the same native security as a web browser. Actual data protection fell to the company itself, which had open access to all collected user information. While Zoom has sworn that it does not mine this data, additional findings provided implied they actually were selling personal information to advertisers and social networks.

***Zoom Plans to Remove Encryption for Free Users***
The backlash over the revelation forced Zoom to take steps to improve their cybersecurity stance; however, company representatives expressed stipulations of this plan that would cause even more controversy. In order to provide actual secure encryption, the company ostensibly needed information only included with paid accounts. Many observers either reinforced or questioned this reasoning, but the debate became even more muddled by Zoom itself when the CEO made additional claims that encryption would block the company from working with law enforcement.

***Data Privacy and Censorship Scandals***
The Zoom CEO's comments came in the middle of protests sparked by the killing of George Floyd by a Minneapolis police officer, and generated immediate backlash. This was further aggravated by additional revelations that Zoom had cooperated with China in suppressing activists with accounts on their platform. Though the company later joined others in blocking user data requests from the Chinese government, the damage was done - Zoom's ability - and willingness - to ensure user data privacy was called into question.

***Major Reversal Leads to Roll-out of New E2E Features***
The mounting backlash finally forced Zoom to include free users in its end-to-end encryption service, though with yet another caveat. As long as these accounts provide additional information that would allow verification of their identity, they will receive the same level of E2E as paid users do. As of this writing, the new security features are still being rolled out and tested in the real word, and we will have the full picture on their impact in the near future.

***The Cybersecurity Challenge of Video Apps***
Zoom is also still in the spotlight as of this writing, with delays in delivering a promised transparency report on how it provides data to governments. This scrutiny is not likely to end soon given the precedent created by Zoom itself, as well as by similar hardware-connected apps. The age of digital transformation continues to remind the public that everything with an Internet connection is inextricably linked, and this lesson will undoubtedly be on display again when the next hot tech company drops the data privacy ball.

Many of these apps inevitably contain exploitable backdoor connections, for a variety of reasons but mostly boiling down to money. Whether because the cost of operating end-to-end security on the developer's end is too great, or because the data mining applications are too lucrative, there will always be an element of exposure in many digital applications on the market. Most importantly, no technology will ever be full proof against human error.

***Let SWK Help You Secure Zoom or Find an Alternative***
SWK Technologies has experience with providing customers with security solutions for many software and network vulnerabilities. We can help you cybersecure your existing applications, or direct to a better alternative for video communications, like Microsoft Teams.

Contact SWK today to learn how we can enable you to avoid the cybersecurity pitfalls of Zoom and other unsecure apps.

## Gift Card Trivia!

This month's question is:

*What change is Zoom planning to make to free user accounts? ( Hint: The answer is in this newsletter.)*

a. No longer free accounts
b. No Changes
c. Ad Supported
d. Removing Encryption

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **August 3rd,** in order to be placed in the running for this month's gift card prize!

# We can help you with:

- Cybersecurity
- IaaS
- 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

## Password Security is Still Your Biggest Cyber Threat

Lax password security still represents the biggest cyber threat your business will face, especially in the new normal. Multiple studies reveal that users continue to ignore secure login best practice, which has only been exacerbated by the shift to working from home. As millions of newly remote workers have switched to accessing their business data outside of the office, hackers have stepped up efforts to exploit these potential victims as gateways to valuable corporate databases.

Here are some of the top reasons why password security is still your biggest cyber threat and network vulnerability:

***Cybersecurity vs Convenience and Productivity***
Many factors hamper good password security practice even in the most stable of times, including ignorance, stress and just plain forgetfulness. However, convenience and timeliness (or lack thereof) account for a sizable portion of bad practice influence as users devote only so much time to creating - and remembering - their plethora of passwords. Many already have such a high quantity of personal passwords to remember that they cannot generate the variation required for their business logins as well.

Having so many employees working from home can amplify security gaps, as remote workers are often forced to deal with increased distractions and lack of equipment as opposed to being in the office. Those without a company computer will use their own devices, and without the right cybersecurity training will likely expose business accounts to connected personal logins. With the pandemic causing significant shifts in operations for almost everyone, it will be that much harder to enforce proper password security practice at an organizational scale.

***People are Still Reusing the Same Weak Passwords***
Tech companies have also been gathering leaked passwords from data dumps in order to take their own steps to protect their users. This past June, a computer student based in Cyprus managed to consolidate this data to conduct their own study and reveal some of the most common patterns. Perhaps the most alarming is that the over 1 billion set of credentials contained only 17% (168,919,919) unique passwords - "123456" accounted for 7 million passwords by itself.

Microsoft conducts their own password security survey at the end of every year, and 2019's revealed that up to 44 million of Windows users were still reusing compromised passwords. This report also highlighted the dangers inherent in these practices for Microsoft products and services, which are some of the most popular yet consequently some of the most targeted in the world. Hackers are increasingly going after users on Office 365 or Azure to take advantage of their lack of familiarity with cloud security practices.

***Cloud Security is Password Security***
Even before COVID-19 forced a shift to cloud-hosted platforms, instant remote communication, access and data sharing were becoming popular benefits for many businesses. Now that organizations across the world implementing contactless operations, SaaS connections are becoming almost ubiquitous. Everyone that leverages a Microsoft Office 365 or Google G Suite application to enable remote work is already engaging with a hosted server - indeed, working from home at this current scale would have been impossible without considerable previous infrastructure investments.

This means that the cyber threat generated by weak password security can mushroom into a company-wide attack surface expansion. If a hacker breaches one account, then they can try to access the connected servers. Attacker success depends on many factors - including the security infrastructure of the technology and service provider - but there is enough role segmentation on the user side to still make it dangerous to your internal network.

***Multi-Factor Authentication Use is Growing***
Research has revealed some good news - Multi-Factor Authentication (MFA) adoption is expanding significantly. This is because MFA deploys a whole new layer of cybersecurity between passwords and database access, which can make all the difference in the world for a hacker seeking an easy score. Utilizing an authentication like DUO can make up considerably for the pitfalls your remote workers face for proper password procedures.

***Don't Let Weak Passwords Be Your Last Line of Defense***
There are plenty of new stories out there about SNAFUs at enterprise-level and SMB companies alike exposing heaps of sensitive corporate and customer data. What is often buried in these tales is that the majority originated through exploited credentials - don't let a bad password be what breaks your company after surviving COVID-19.

Download our white paper here to learn more about how SWK's MFA solution will augment your password security protocols.