IT Strategy Brief

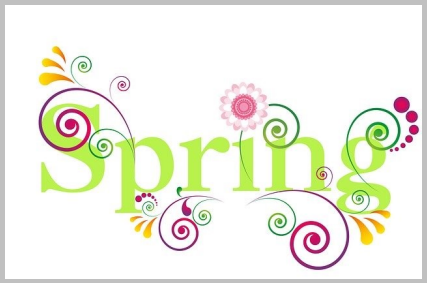
ISSUE 4 | VOL 6 | April 2020

INTEGRATE SEAMLESSLY

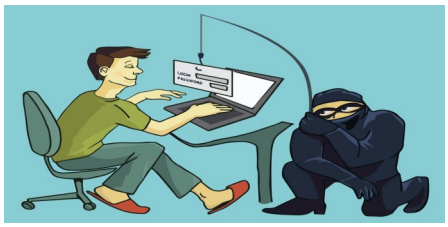
SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:



Defend Yourself Against Coronavirus Phishing Scams



Hackers and cyber scammers are trying to take advantage of the coronavirus disruption to hack into your network while you work from home. Telecommuting requires a different approach to cybersecurity than traditional models, and even in the best of times remote work requires a rethinking of security posture. Cybercriminals know that many are trying to adjust to new realities and are moving fast to exploit ignorance and fear around COVID-19 disruptions before their victims learn how to spot the signs.

Using COVID-19 as a Phishing Lure

Many federal cybersecurity agencies and private research teams have raised alarms about the emergence of phishing attacks leveraging coronavirus concerns. At least one firm claims that four out of five cyber scams exploited the virus in some shape or form as of April 2020. These ranged from simpler types of wire fraud schemes with bitcoin wallets to full-fledged malware campaigns that included thousands of malicious URLs and attached files.

Cybercriminals posed as distraught victims and individual healthcare workers needing additional funds, mask and sanitizer manufacturers and retailers, and even World Health Organization and CDC officials. Hackers have deployed all types of programs, from trojans to keyloggers, and March saw a surge of webpages being registered with mentions of coronavirus. Authorities suspect the latter are tied to illicit activities and are likely part of phishing domains.

A Whole New Ransomware Surge Mid-Pandemic

2020 had already promised to bring a whole new wave of ransomware attacks against unsuspecting victims, but the COVID-19 pandemic prompted some hacker gangs to double down on common targets. Chief among those are hospitals and other healthcare providers, including quite a few on the frontlines of treating infected patients. The situation has become so dire that Interpol has stepped in to aid regional law enforcement in investigating ransom cases, as well as technical support and guidance for the medical industry.

In a surprising turn of events, online outlet BleepingComputer managed to contact several of the malware syndicates behind some of the most notorious forms of ransomware. All denied ever having targeted any hospital or any other public service institution, and a few claimed that the only healthcare industry victims they had ever pursued were pharmaceutical companies. However, experts have already questioned the sincerity of those promises not to impede medical centers and warned everyone to remain on guard.

Continued on page...2

What our clients are saying: BCA Watson Rice LLP

"When we got infected with a virus, SWK worked immediately to restore all of our networks. The response and recovery time was superb. Most of our IT issues are answered and resolved as soon as possible with very little time lost."

Gina Bidaisee-Santo
BCA Watson Rice LLP

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

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 **April 30th** to get your name in the hat.

You could win a $25 Gift Card!

Defend Yourself Against Coronavirus Phishing Scams

Continued from page 1…

Cybersecurity and Working from Home
There are two things hackers are keenly aware of right now: first, people are distracted, and secondly that even before the novel coronavirus, many businesses were not taking the right steps for telecommuting securely. Cybersecurity is a big concern when working from home, and the mass shift to an enduring remote work model has inadvertently expanded the attack surface of many companies. Unprepared employees are using home devices and open Wi-Fi signals to log into corporate networks, with simple usernames and passwords that have been re-used a hundred times.

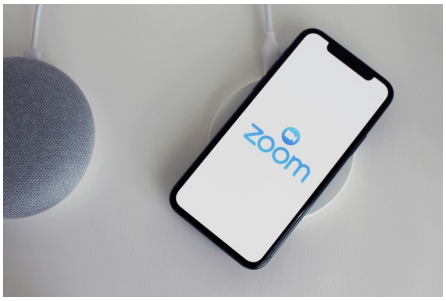
This is the perfect time to launch a phishing campaign, with millions of unsecure computers and unsuspecting victims everywhere. Even in the best of times, social engineering and spoofed emails delivering malware can catch all but the wariest off-guard. The key to migrating to a cybersecure work from home environment during these uncertain times is making sure all endpoints are protected - and that means educating users and managers on how to do so.

Let Your Remote Workers Telecommute Securely
Phishing is not going away for a long while, as even without a huge telecommuting surge, hackers know that there are so many easy victims to exploit. Let SWK Technologies help you educate your employees on how to spot the red flags of a spoofed email, and teach your business all the tricks of working from home securely.

Sign up for our Phishing Defender service to receive the latest in employee training, educational tools and more to protect your business against COVID-19 cybercrime.

The Cybersecurity Problems with Zoom Video App

The Zoom video communications app has had a documented history of cybersecurity concerns, but the rush to adopt conferencing software for telecommuting has brought these issues back to the forefront. As the COVID-19 shutdown forces everyone to practice social distancing, many have flocked to these types of applications for remote work or personal use. The surge in downloads have only exacerbated the persistent security gaps in the platform to the point where many institutions are questioning its installation on their networked computers.



Universal Naming Convention and Remote Code Vulnerabilities
The vulnerabilities in Zoom mostly center around poor data security controls, including several serious examples in both Windows and MacOS machines. Many of these come from remote code or other external pathways that provide easy network backdoors for hackers to exploit. SWK previously reported on the RCE (remote code execution) bug putting nearly a million Apple computers at risk in 2019, but the Universal Naming Convention (UNC) error in Microsoft devices could expose exponentially more Zoom users.

The UNC vulnerability essentially creates a file path from a hyperlink in the chatbox to a remote site protocol, which is relatively easy to hack once it's sent out. Though Zoom is releasing a patch, the bug has put the tens of millions of Windows users running the app every day at risk already. In fact, it is likely that this vulnerability, or something very similar, is the exploit that led to the surge of "Zoombombing" recently.

Zoom Data Mining for LinkedIn and Facebook
Though not technically falling into the category of hacking, additional irregularities were found in the video app's user information controls, namely data mining for social media platforms. Zoom was found on separate occasions to be silently and automatically providing personal details to both LinkedIn and Facebook - without the user's permission, or even without the presence of a connected social profile.

What makes this practice suspect, and potentially illicit, is that there was little to no mention of this type of third-party file sharing in Zoom's privacy policy. Such a trend does not bode well for the program's security posture overall, either, as it reflects similar red flags that proceeded the FaceApp scandal.

Shiny gadget of the month: Adjustable Laptop Stand



Since most of the country is working from home due to the coronavirus we are going to take a look at a gadget that is a little more low tech than usual, but could be extremely helpful to anyone who is experiencing a life change while working from home. The gadget is the adjustable laptop stand.

There is no one particular brand or type to focus on for this, to each their own, and with the demand for home office supplies it is best to keep your options open. A quick search for a "adjustable laptop stand" on Amazon or Google should do the trick. These devices are relatively inexpensive compared to a standing desk and offer a lot of the same flexibility (compare $50 to $200+).

The way many of these stands work is by having legs with multiple hinges on them that can be adjusted to different angles. It can take a little trial and error to figure out the optimal configuration depending on what you are aiming to do, but it is simple enough that it only takes a few seconds. If you're uncomfortable and need to stand for a little no problem, just adjust the legs and it can be propped up to function as a standing desk. If you want to sit on the couch just a couple more adjustments and it can comfortably sit over your lap. Some of these even come with a rest for the mouse so you can easily use it regardless of the positioning. Being able to move around and stretch your legs is important. If you are forced into suboptimal conditions like sitting at a kitchen table in a regular chair it can get uncomfortable, so being able to stand for periods of time can help change things up for you.

In a time where we are all adjusting it is important to try and make the most of your situation. If it means adapting your kitchen table or a spare bedroom into an office, little things like comfort go a long way. Finding a way to make your new space you designated for an office a little more comfortable can help boost productivity and overall happiness. Hopefully you are able to find ways to do just that, and hopefully little ideas like the adjustable laptop stand can help aid you.

Cybersecurity and Working from Home During Coronavirus

How to Work from Home with Cybersecurity in COVID-19 Times

The coronavirus pandemic is not going to give you a break from cybersecurity – it is even more important when working from home. Hackers are already trying to take advantage of both the uncertainty and the laxer workspace environment to launch renewed phishing and ransomware campaigns. Your network security practices and solutions are key components for business continuity during the COVID-19 outbreak and transitioning to a remote workforce.

You are going to face many questions when it comes to your cybersecurity posture – How many devices use your network? Is your accounting or ERP software protected? Are you using a secure cloud platform? What data security regulations affect your compliance processes? To name a few. As a solution and managed service provider (MSP), SWK Technologies is here to help you answer these questions with our Business Survival Guide on working from home with network and information security.
Here is a list of the biggest individual factors that will help you determine how to cybersecure your remote workforce during the novel coronavirus pandemic:

Ransomware and Phishing Increase in 2020
Even before the COVID-19 outbreak, cyber threats such as general phishing and targeted ransomware attacks were on the rise for 2020. In many cases, the former was a popular vehicle for the latter as a proven technique for breaching networks. The current situation has only upped the incentives for hackers increase deployment of both these and many more types of cyber attack. The shift away from better secured corporate networks leaves remote workers vulnerable to more discreet hacking methods.

The best defense against spoofed emails, dummy domains and links, and other phishing techniques is cybersecurity awareness training and monitoring. Human cyber intelligence is the best way to spot bad actors in your system; however, in the event you are hit with a malware infection, backing up your data in secure cloud storage lets you restore your network faster. Even if ransomware corrupts your files, backups ensure you can recover your critical information and return to business.

Remote Worker Network and Device Endpoint Security
Remote workers and distributed teams can deliver several benefits, but a downside is the lack of physical oversight and equipment monitoring. It might seem advantageous for both employee and employer to rely on personal computers, smartphones and Wi-Fi routers, but these device endpoints are rarely as secure as they would be in a business IT network. Personal usage of networked devices, whether private or company-provided, will also expand your cybersecurity attack surface as you have no control over who uses the machines and what programs gain access to your data.

Preventing your system from being breached through backend means deploying more dedicated endpoint security tools and better practices. Users in your network will need improved guidance as well as additional layers of protection for all of their devices. Minimal safeguards like passwords can be breached easily, but multiple login steps will help deter attackers from leveraging your remote employees as gateways to your data storage. e Vulnerabilities of Video and Web Apps and Firewalls

Security gaps can form in any device that uses unsecured external applications, and basic security controls often are not enough to protect networked computers 24/7. With the rush to download web apps for video communications, hackers are going to be exploiting every legacy RDP (remote desktop protocol) bug they can get their hands on. Individual firewall software programs are not built to identify attacks from the inside, and typically cannot handle more sophisticated cybercriminal techniques.

The reality is you will not be ably to track down every single unsecured app in your user network, but you can encrypt your data and monitor your system diligently for anomalous activity. Unfortunately, your internal resources can quickly be overwhelmed securing your expanding distributed workforce. That is why this is a good time to consider outsourcing your IT or hosting your software applications through a cloud service with security built-in.

Cybersecurity Insurance and Regulatory Compliance
The surge of data breaches last decade made information security regulations and cybersecurity insurance a reality of doing business online. However, do you actually know the extent of your compliance footprint and how much your policy protects you if you are fined? Many data privacy laws and cyber insurance policies were not written with the level of telecommuting COVID-19 has forced in mind.

Information security is an organizational responsibility – your company is the steward of all customer and employee data, so it is everyone's job to protect it against leaks. Every remote worker is a user endpoint that can be exploited for greater network access. Educate yourself on privacy regulations and your cybersecurity insurance policies quickly or consider engaging SWK to help automate your network security compliance.

Gift Card Trivia!

This month's question is:

What is the best defense against spoofed emails, dummy domains and links, and other phishing techniques? (Hint: The answer is in this newsletter.)

a. Firewall
b. Anti-virus
c. Employee Awareness Training
d. Multi-factor Authentication

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **April 30th**, 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

The Cybersecurity Problems with Zoom Video App

Misleading Messaging and Online Meeting Encryption Claims
Suspicion around Zoom does not end at the data mining and remote access bugs – their entire cybersecurity approach is coming into question with the discovery of misleading encryption claims. Despite attributed end-to-end (E2E) encrypting for meetings and messages made through the platform, Zoom was forced to admit that it was a technological impossibility for the app. The encryption service that it actually uses is the same as a standard web browser, but more importantly, it gave the company open access to user data.

Governments and Companies Blocking Zoom Video App Use
Given all the above and many other security vulnerabilities and bad practice by Zoom besides, the video app's use has come under heavy scrutiny. Private businesses and public agencies have questioned whether the software is secure enough to use for their customers and constituents. Some companies and whole governments have even gone as far as to ban its internal use totally, including the Singapore school system, the government of Taiwan, and tech giant Google.

Weak Service and App Cybersecurity Puts Passwords at Risk
Zoom joins a long line of web applications and services that have been caught promising the moon when it comes to cybersecurity, only to leave their customers ignorant of and exposed to cyber threats. Oftentimes developers and providers will not properly communicate all the dangers consumers face from hackers, and even they may not be aware of every bug in their products or gaps in the network. Zoom's CEO has at least admitted to the company's security failings, but their reputation is permanently scarred as the lid has been lifted off for how weak their cybersecurity commitment has been.

Let SWK Provide an Extra Layer of Cybersecurity
Zoom, Ring, and even your smartphone's OS - these vulnerabilities are popping up all the time because security postures have still not caught up to technology. You can no longer afford to rely just on a login and password to protect your network - you need to have multiple layers of cyber defense to protect yourself from all of the threats out there.

Talk to the experts SWK Technologies and find out how our service can improve your cybersecurity stance against hackers, especially during COVID-19.