IT Strategy Brief

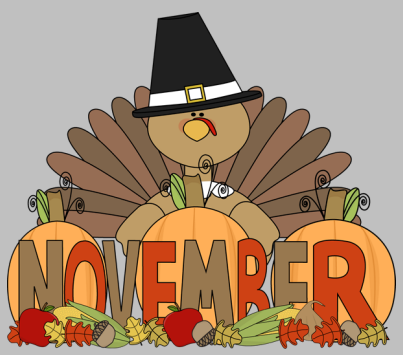
ISSUE 11 | VOL 4 | November 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

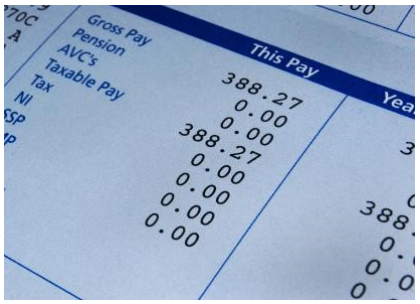
"Useful Technology Ideas for Your Business"

What's Inside:



FBI Warns NJ Employees of Paycheck Email Scam

NJ.com recently reported on an alert released by the FBI warning residents of a current phishing scam that is targeting employees in various industries, though the most affected sectors have been education, healthcare and commercial air transportation. The attackers send fraudulent emails to the victim seeking to gain access to their login credentials, and once those have been obtained they access the victim's employee payroll account.



According to the FBI alert, once the victim's account has been accessed, the attackers then begin to modify their banking information. They simultaneously redirect direct deposits made by the victim's employer to an account they control – usually tied to a prepaid card so they cannot be tracked – and suppress notifications so that the victim is not alerted to the withdrawals being made.

The hackers use social engineering tactics to gather information on potential victims and design the fraudulent messages to appear as if coming from their company's Human Resources department. The emails will make a request regarding their direct deposit that requires the victim to submit login information for their payroll system.

Hackers increasingly utilize social methods to identify and exploit employees, either for one-time gains or for deeper access into the company's network. More sophisticated and patient attackers will leverage special access privileges or related connections among personnel that may be overlooked by your business's security practices. These links can be used to dig deeper into the system and locate more valuable data.

Phishing, or business email compromise (BEC) as the FBI calls it, has become a continuous problem in NJ as hackers have deployed it as a common technique in a variety of areas, including finance, healthcare and real estate. BEC is a relatively easy-to-use method that can be utilized in volume until a promising return appears. Phishing scams can be hard to defend against and harder to spot if you do not know what to look for, and hackers are refining their approach as reflected in this new scam.

Read how SMBs are becoming increasingly exposed to techniques such as phishing and learn how you can protect your business's network from being breached.

What our clients are saying: Continental Food and Beverage, Inca Kola

"It was a serious issue in that it held hostage very important financial files for our business. One phone call to SWK, and they were able to come in and identify the exact time and place that the virus came in and the files it was attached to. If we weren't able to utilize the Datto solution and SWK's expertise to identify when and where that ransomware came in, we would have been lost. We would have lost a lot of business."

Randall Berman, Chief Operating Officer
Continental Food and Beverage, Inca Kola.

INCA KOLA DESDE 1935

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Barry McManaman
Family Resource Network

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

You could win a $25 Gift Card!

How to Gain Employee Buy-In on Cybersecurity

The Forbes Technology Council, a group of top-level CIOs, CTOs and other technology executives, recently released a list of seven recommendations for encouraging employee compliance with company cybersecurity practice implementation. Each suggestion was provided by a professional within their field who had applied the tactics illustrated firsthand in their industry.

1. **Begin with Employee Awareness**
2. **Establish Training Programs**
3. **Make Those Programs Relatable**
4. **Ensure Transparency**
5. **Use Video**
6. **Making Training Personal**
7. **Keep it Simple**

These recommendations can be simplified as the creation of a successful internal cybersecurity program requires promoting and maintaining employee engagement. As far as network security is concerned, your personnel are both your business's first and last line of defense. They are also simultaneously gatekeepers of and entryways to critical data; consequently, when employees are not engaged in cybersecurity best practices, your business becomes vulnerable.

Note that "employees" also includes C-suite executive personnel as well as other network users who can deliver access to decision-maker credentials, such as secretaries and assistants. As the recommendations provided by the Technology Council indicate, employee cybersecurity compliance is a company culture factor that must become second-nature to be effective.

Awareness
Your employees cannot defend against what they do not understand, and ignorance of the scope of threats is what hackers rely on to exploit your network vulnerabilities. All internal security programs should start with a basic education on cyber attacks.

Training
Just as with every other aspect of their roles in your business, employees must be trained in proper cybersecurity procedures to fully understand and be prepared for them.

Relatability
As said previously, ignorance is a key component of successful network breaching strategies. Ignorance of cybersecurity best practices often stems from a lack of understanding on the subject, so reframing the conversation in a way that makes sense to non-security personnel helps to bridge this gap.

Transparency
Implementing a network security strategy is the same as deploying any other organizational plan: buy-in requires transparency with key stakeholders, i.e. employees.

Presentation
Part of ensuring your strategy is relatable and makes sense to your employees is ensuring that it is delivered through channels they are connected to and a medium that grabs their attention. Whether it is through training videos or some other form of visual communication, the presentation will play a significant part in how well the knowledge sticks.

Personal
Another tactic for making your cybersecurity strategy relatable to your employees is to associate best practices with their personal lives. For example, you can provide your personnel with educational updates on mobile security practices and how these can affect their personal and professional lives.

Simplicity
It goes without saying that in order to successfully make your business's network security strategy relatable, transparent, and understandable to your employees, it is best to keep it as simple as possible. This may be harder to do with some vulnerabilities that may require some technical knowledge to fully understand how they may be exploited, but breaking down each step into an easy-to-follow process will be much more effective than forcing the knowledge wholesale onto each employee.

Cybersecurity is an Organizational Commitment
Adopting a network security strategy is not a superficial decision to be made, but a company-wide obligation that requires input from everyone it affects in order to be successful. As the Forbes article indicates, this is best done by ensuring each employee is informed and trained in cybersecurity best practices in a way that speaks to their role in your business.

Learn about our Phishing Defender solution our employee awareness training resources that helps prepare your employees for the inevitable breach attempt.

Shiny gadget of the month: Canary All-in-One Security Solution

It is probably safe to say that most people would feel better about having a security system in place in their home. However, that does not mean that most people actually have security systems. People can be off-put by the cost and complexity of getting a professional home security and monitoring system installed, but this does not have to be the case. For a smaller home the Canary All-in-One provides total home security and intelligence with a 1080p HD camera, 90 decibel siren, plus a built-in climate monitor for a small price.

The Canary comes loaded with features. It has two-way talk to communicate with family at home, or maybe just to keep your pets off the furniture, an alarm that you can sound to thwart intruders, live and recorded video, air quality monitor to tell you temperature, humidity, and understand how it can affect your health, and access to pre-populated numbers for first responders. It even works with Alexa for voice control… all this in a compact little gadget.

You can set up one, or multiple, devices to monitor your home. The wide angle lens will monitor things and if motion is detected it will send you an alert to your smartphone. From there you can view the motion and determine if you should set off the alarm and contact the authorities or not. The motion detection uses AI technology so that it can recognize your pets from an intruder so you are not inundated with alerts, but can still keep an eye on your furry friends. It also uses this technology to know if you're around and auto-arming if you are not, as well. It also comes with a privacy mode to shut down the camera and microphone at any time so you can still have privacy in your own home while you are there. Canary even comes with insurance benefits. Companies like State Farm, Liberty Mutual, and Allstate offer benefits for having a Canary device.

All these features packed into a tiny device. The Canary All-in-One is listed on their website for $169 with discounts for using their premium membership. To see more about what this nifty little gadget can do check out their website for more information https://canary.is/ .

Study Predicts Cyber Attacks Could Destabilize Economy

A paper published by the Brookings Institute of Columbia University found that despite greater widespread understanding of cyber risk and cyber defense, existing gaps in network security may still allow cyber attacks to occur consistently enough to lead to financial instability across the US. The paper is a result of two years of research and engagement by Columbia's School of International and Public Affairs with observers and operators within finance, cybersecurity, and industry compliance sectors.

The research conducted by the authors studied the relation between financial stability and cyber risk, the former as defined within the paper as the ability of the national financial system to sustain and manage risks and disruptions while continuing to enable monetary exchanges. The danger posed by cyber risk – or any other economic disturbance for that matter – is that incidents may lead to the creation of "systemic cycles that could severely weaken or shut down the economy."

Contagion
A primary concern regarding the effect of cyber incidents on financial stability is the risk of "contagion," meaning that a single occurrence or multiple isolates ones will generate additional economic consequences. While this danger is present for several other factors that determine financial stability, the nature of cybersecurity is such that it inherently poses a genuine hazard to the national economy if certain circumstances occur.

As the paper illustrates, both finance and cybersecurity rely on limited channels, sensitive data, and participant confidence to function. Any disruption in any of these areas presents a potential escalation that will produce continuous disturbances that will interrupt the entire system. In the case of network security trends, there is an added danger from external threats due to the proliferation of cyber attack methodologies and incentives, including cyber terrorism and cyber espionage.

Spread of Cyber Attack
The sophistication of cyber attack techniques has led to a real danger of financial stability being disrupted by hackers with monetary or political goals – or both. Cybercrime presents an opportunity for opposing nation states to hit adversaries while also benefiting financially, or to incentivize independent operators to carry out attacks on their behalf. Russian, China, North Korea, Iran and a few other countries have all been accused of funding either type of campaign to disrupt rival nations, with the US often being a prime target.

The internecine nature of modern cyberwarfare means that there are ample national players and individual operator networks available for collaborative efforts in taking down bigger targets. Even an attack designed for a one-time theft might cause significant damage for the sake of expediency, and the entire world economy could suffer from unforeseen consequences. However, the greater danger still lies with an attacker intentionally triggering a financial crisis to inflict the most economic disruption possible.

Improving Cybersecurity Practices
Despite the very real threat of cyber risk affecting financial stability, the good news is that the growing awareness of cyber threat on the federal, corporate and personal levels is contributing to improvements in existing economic safeguards. The rising number of data privacy regulations from state agencies as well as the more stringent guidelines being imposed by industry associations reflect a more serious approach to cybersecurity best practices emerging nationally. As the world becomes more interconnected through the Internet, opportunities for cyber risk will increase and so too will the standards designed to protect against it.

Read up on the most common hacking techniques to familiarize yourself with the signs of an attempted intrusion and prevent being caught off-guard.

Gift Card Trivia!

This month's question is:

In the phishing scam that the FBI has warned about, emails will make a request regarding their _____ that requires the victim to submit login information. (Hint: The answer is in this newsletter.)

a. Home Address
b. Work Log-in
c. Email
d. Direct Deposit

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **November 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 TECHNOLOGIES

The Disconnect Between Business and IT Leaders

Despite digital resources playing an ever greater role in the modern workplace, there is a clear disconnect between business and IT leadership according to Forbes and a 2017 study by Forrester. While other business units are actively integrated into organizational processes and objectives, CTOs, CIOs, and CISOs are often left out of the key planning discussions even though their departments are key to meeting operational goals.

Several factors contribute to this, including the lingering perception of the IT department as a money-draining luxury. However, having an IT resource on-hand is just as important as maintaining legal counsel or accounting team to ensure integral business processes can continue to function. Corporate culture still has not fully caught to quantifying IT as contributing to business value despite the increasing reliance on digital assets to conduct even basic transactions.

Part of the reason for this lag is that even with the progressive adoption of digital resources, IT is still overloaded with technical jargon that is not communicated succinctly or simply enough for many ground-level employees or executive decision-makers to understand. Contributing to this are the influxes of evolving cyber attack and data privacy regulations, which conversely also lead to desperate, often misinformed responses by business leadership to manage intrusions or comply with complex guidelines.

The first step to bridging this disconnect is to recharacterize the conversation around the purpose of IT to accurately define its value to your business:

“What digital resources do we use?”
“How much would it cost us if they went down?”
“If we suffer a breach, will client data be exposed?”

These are all questions you must answer to gauge the true value of your IT resources, yet obviously without firsthand knowledge of the full scope of your digital assets (which is generally delivered by IT resources), it will be hard to answer these points completely. This is a paradox that you must decide how to address with the answer to one last question – “Can my business survive without IT?” If the answer is no, then it goes without saying that you need IT input to provide the type of insight required to make informed decisions around your digital assets.

Read through our white paper on why price is the wrong criteria for selecting managed service providers to learn more about how dedicated network support will improve your value.