IT Strategy Brief

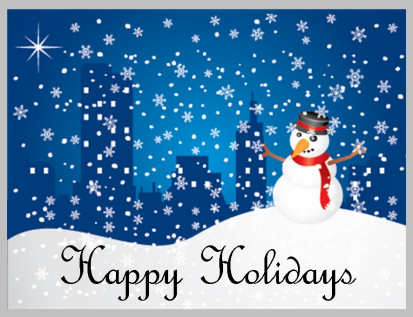
ISSUE 12 | VOL 4 | December 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:



Shoppers and Retailers Targeted by Cyber Scams This Holiday Season

The 2018 holiday shopping season is predicted to generate almost $130 billion in online sales, which is bringing the attention of cybercriminals to e-commerce transactions and omnichannel interfaces. Both retailers and shoppers will become targets of opportunities for hackers seeking to take advantage of any stage where money (or, more importantly, banking credentials) changes hands electronically. This period has historically seen similar increases in attacks, such as during the infamous Target Black Friday breach in 2013, but the sheer amount of cash and financial data involved will likely spur attackers to make more concentrated efforts.

Perfect Storm of Social Engineering

Attack methods and channels vary, but the majority of attempts consistently involve phishing as it is the easiest and most cost-effective technique to deploy in volume. Sophisticated cybercriminals can augment this approach with research into their targets that significantly increases the credibility of the fabricated message to its intended victim. Attackers leverage the fast pace of holiday shopping to lower their target's inhibitions, especially for last minute gift purchases.

Cybercriminals will employ strategies such as shadowing your purchasing journey to hijack it at a critical juncture, including sending an email as either the vendor or distributor asking for credit card numbers or login information. Some take advantage of payment portal websites or mobile applications to place their own malicious landing pages or apps to capture e-commerce traffic. These duplicates may be used as vehicles for malware such as a trojan virus that will give hackers deeper access.

Mobile as an Attack Vector

Mobile e-commerce provides a potentially lucrative channel for attackers to exploit as smartphones become the preferred online shopping tool while device security remains stagnant. Research has repeatedly shown that both professional and personal mobile security practices compound gaps already present in smartphone devices against malware infections. Other existing weaknesses in mobile phones offer hackers an easier time to leverage socially engineered attacks against targets.

Continued on page 3...

What our clients are saying: Family Resource Network

"My favorite thing about SWK is the peace of mind I have when logging into my remote server and knowing that someone is just a phone call away that can help me with an IT issue. If I do have an issue the technicians are not only knowledgeable, but also friendly, patient and easy to speak with."

Barry McManaman
Family Resource Network

The Family Resource Network
Providing families with access, answers and action

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Jerry Ramirez
Beth Ward Studios

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.

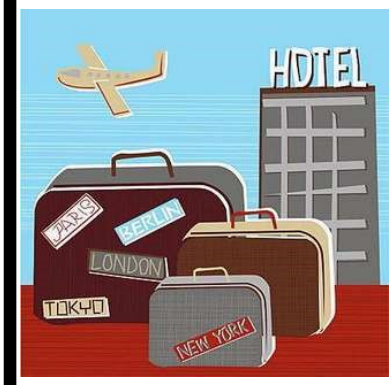
3. What are the biggest benefits you've received or experienced since hiring us?

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

You could win a $25 Gift Card!

Study Finds Traveling Employees a Serious Cybersecurity Risk



A majority of your employees may be exposing your system to threats while traveling, a recent study found. A threat management firm surveyed 1000 US employees to gauge their understanding of cybersecurity best practices while working remotely. 3 out of 4 of every respondents claimed that they knowingly used public Wi-Fi connections while on company-provided devices, and about 3 out of every 5 said they accessed their work-related emails and devices as well. 1 out of 5 had previously left work devices unattended while traveling.

Vulnerability from Cybersecurity Ignorance
The study highlights a reality among employees concerning cybersecurity best practices while traveling or even working remotely day-to-day. Though about half of those surveyed claimed they knew there were existing guidelines for the use of their devices outside of the office, the other results indicate that either they were unaware of the basic obligations or knowingly ignored them. More often than not, the former accounts for most cybersecurity guideline noncompliance and even those that claimed awareness were actually misinformed.

Traveling Employees are a Hacking Target
Cybersecurity practices while traveling represents a bigger gap than many businesses might realize – some cybercriminals have specifically targeted people in transit. Hackers have gone as far as infiltrating hotel networks to spoof Wi-Fi connections or even install keylogger programs in business center computers. This indicates that attackers are very aware that visitors drop their safeguards while on business travel or vacation and can be more easily exploited.

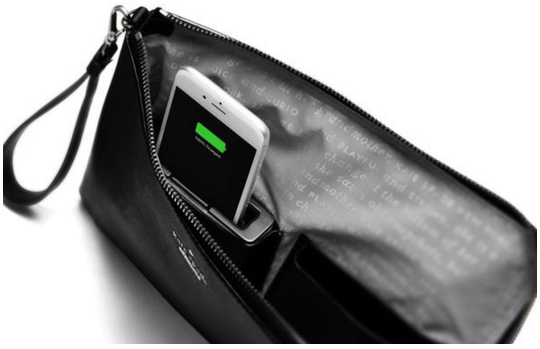
The rise of socially engineered hacking methodologies creates a danger of cybercriminals leveraging traveling personnel as a dedicated attack vector. Flippant use of social media, GPS-tracking software or any other channels that could provide snippets of personal identifiers permits hackers to build profiles on victims once they are able to piece together enough information.

More than Cybercrime
This also supplies hacktivists, nation-state hackers and any other politically-motivated cyber attackers with a means to bring down targets by conducting research into "weak link" employees with system access but less security. Committed surveillance of their social network or other online activity will allow hackers to plan for traveling periods and take advantage of the decreased security awareness to plant malware in their workplace devices.

Throughout 2018, federal agencies noted several private and public organizations fell victim to phishing attacks by Russian-backed hackers, and experts have seen a resurgence of corporate espionage by Chinese cyber actors since the beginning of the trade war. Both groups are aggressively seeking out vulnerabilities in American systems for a mix of monetary and political reasons, and employees of US companies are a primary target.

Educate Your Employees on the Risk
As demonstrated by the survey results, the lack of compliance with organizational cybersecurity practices while traveling likely stems from not having a true understanding of what this means. Ensuring employee buy-in on your security policies requires you to communicate these guidelines in a way that they can understand intimately.
Read through these seven methods for gaining employee buy-in for your cybersecurity practices to help you determine the best way to bring attention to this issue.

Shiny gadget of the month: Everpurse Kate Spade Handbags



Looking for a unique gift this holiday season? Tech and fashion have finally come together for a pretty cool new line of handbags. The Everpurse Kate Spade line of handbags are stylish handbags that are also on the go chargers for your iPhone.

It is a simple and quite practical concept. Sure, there have been batteries you can buy to plug a phone into and recharge, but they are bulky and have additional wires. The Everpurse handbags are a convenient solution where it is a simple as just sliding your phone into the bag and you are all set. The tech is hidden inside the bag behind the lining so you would never even know you are carrying around a gadget with you and it eliminates the extra clutter in your bag a wired charger would add.

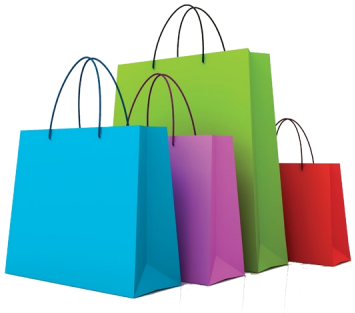
The bag uses patented docking technology to perfectly guide your phone to a lightning connector so no matter what iPhone you have it keeps you covered and can charge most iPhones up to 2.5 times in a single charge. When you get home you simply place the handbag on a charging mat and it will recharge the battery inside. It really is as simple as that. Just imagine, you may never be in jeopardy of having your phone run out of juice again!

The handbags come with everything you need right from the start, so there is no need to purchase additional adapters or a charging mat. These handbags look like they will be a hot item, which comes as no surprise since it is such a clever and practical idea. At of the time of writing this a number of the bags are already sold out on their website https://www.everpurse.com/. Check it out for yourself, or use it for a unique gift idea this holiday season.

Shoppers and Retailers Targeted by Cyber Scams This Holiday Season

Continued from page 1...

Retailer Cybersecurity
Retailers occupy an even more vulnerable place as both potential victims and attack vectors. Client data collected through payment portals or other platforms can be even more valuable than their purchases since cybercriminals can either utilize this information themselves or sell it through the Dark Web. Once an attacker hacks into the vendor's systems they will be able to position themselves to go after customers when the opportunity arises.



Customer Personal Information
The loss of customer personal information represents the greatest danger for most retailers as not only does it result in a loss of consumer and investor trust, which can bring very real financial penalties in declining stock prices and lost business, but it can also breach existing and emerging compliance laws. In the wake of successive network breaches and the EU's GDPR, regulatory agencies have shown an increasingly stringent response to data leaks.

Non-public personal information (NPI) collected by organizations, especially personally identifiable information (PII) that can give access to bank credentials, has consequently taken on a greater importance in the eyes of government bodies and trade associations. Companies can be found liable for data breaches, either for creating the circumstances in which they occur or for not reporting them in time, and be directly penalized. Even if third parties, such as outside contractors or trading partners, made the breach possible, it falls under the responsibility of the organization who had primary ownership of the data.

Review Your Network Security
Protecting yourself from hackers this and future holiday shopping seasons means not becoming an easy target. Cybercriminals rely on the volume of transactions happening, the faster pace of this retail cycle and the desperation of both retailers and shoppers to get past safeguards and common sense.

As a consumer, you must rely on being better safe than sorry and recognizing the red flags when they appear. As a retailer, you must ensure your system can handle the number of customers you will receive and that it can handle intrusion attempts.

Sign up for a Network Vulnerability Test to receive a penetration testing for your system and review how well it can hold up to attacks.

Gift Card Trivia!

This month's question is:

In a survey __ out of 4 of every respondents claimed that they knowingly used public Wi-Fi connections while on company-provided devices (Hint: The answer is in this newsletter.)

a. 4
b. 1
c. 2
d. 3

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

SEC Determines Companies Must Reevaluate Cyber Threat Controls

A report released by the Securities and Exchange Commission recently warns public companies in several industries of the need to review existing internal accounting controls, specifically in response to cyber threats. The SEC Enforcement Division, who compiled the report, found that business email compromise (BEC) – a form of phishing – accounted for $5 billion in losses for the companies investigated by the Division since 2013. In 2017 alone, there were $675 million in losses due to cyber fraud recorded.

The investigation that spawned the report delved into existing accounting controls for nine entities which had been the victim of phishing and contributed to the $5 billion total. Some of those surveyed had targeted repeatedly and made multiple transfers to fraudulent accounts before the duplicity was discovered. One company had lost over $45 million to the scam over the course of 14 wire payments before they were alerted by a bank overseas.

The phishing emails typically involved a fake account purporting to be either an executive or a vendor with whom the organization was conducting business. A worrying trend the SEC found in cases involving the former was that the emails were sent specifically to accounting personnel who generally had little or no interaction with the executive being spoofed. They also used the names of actual law firms and individual attorneys to pressure the victims into believing the wire transfer requests were urgent and to give the messages an air of legitimacy.

The SEC has been increasingly demonstrating a more committed approach to investigating cyber fraud, and has signaled a stricter stance on enforcing cybersecurity practices among financial and real estate organizations. Both federal and state agencies are taking the threat of cybercrime much more seriously as it pertains to financial controls, but more importantly by how much customer data is at risk if a network is breached. The sterner regulatory attitudes will place greater compliance requirements on organizations in areas such as retail, finance and real estate that will include displaying at least basic network security best practices.

Read our blog, **Title Agents Can lose Millions from Scams Not Even the FBI Can Detect**, to learn more about how BEC can affect title insurance agents and how severe the damage can become.

If you're interested in learning about how you can train employee's how to spot phishing emails to protect against these types of attacks read about our phishing defender employee awareness training.