IT Strategy Brief

ISSUE 3 | VOL 3 | March 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Beware of Gmail spoofing attacks

Do you have a personal email account? Most people do, and if you are like me and many others you probably have at least one Gmail account as well. Lately hackers have been taking more creative approaches to obtain your user information and there have been recent reports of a particularly deceptive way to steal your information through Gmail.

There is a new trick hackers have been using that uses an existing conversation you have been having with someone through email to slip in their phishing attempt within your conversation. If they are successful not only will the hacker have your username and password, but then the hacker also emails your inbox with more infected emails.

The way this scam works is by having an email appear to be a part of an email chain with someone, keeping the same subject line and everything. This way it just appears as if it is an ongoing part of the conversation and appearing normal, not to raise any red flags. The difference in this is that there is an attachment that when attempting to open brings you to a new tab and prompts you to sign into your Gmail in order to view it. The fake site appears to be legitimate, but with close inspection you will see that it is not a secure site and in front (to the left) of the https:// there is actually text. The spoof site apparently even uses accounts.google.com in the URL which can fool people, so you have to pay particular attention to the https:// and if it is secure or has extra characters to the left of it.

A good practice with email is to always be wary of any attachment or link that prompts you for a password. Any time an email asks you for something, especially for sensitive information, that should draw a red flag. Most reputable places will not ask for sensitive information in an email. Another way to help protect against this type of attack is to set up two-factor authentication, where you get a call or text with a code that you input in addition to your password, so that the password alone will not give access to an account.

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:

Kelly Lau
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 **April 3rd** to get your name in the hat.

You could win a $25 Gift Card!

Cyber security and managed services

Cyber security is something you hear about a lot these days. Sometimes it's thrown around to scare business owners, other times it has proven to be a cautionary tale, one that small businesses can learn from to fend themselves from online threats that can leave devastating impact. What's certain is statistics don't lie, and as much as you'd like to believe your business is safe, the worst could happen at any time. Because antivirus software alone can only do so much to protect your business, managed services has become the solution. To make our case, here are several statistics that prove you need managed services from a technology provider.

The numbers
Small businesses are not only at risk of being attacked, but worse, they've already fallen victim to cyber threats. According to Small Business Trends, 55 percent of survey respondents say their companies have experienced cyber-attack sometime between 2015 and 2016. Not only that, 50 percent reported they have experienced data breaches with customer and employee information during that time, too. The aftermath of these incidents? These companies spent an average of $879,582 to fix the damages done to their IT assets and recover their data. To make matters worse, disruption to their daily operations cost an average of $955,429.

The attacks
So what types of attack did these businesses experience? The order from most to least common are as follows: Web-based attacks, phishing, general malware, SQL injection, stolen devices, denial of services, advanced malware, malicious insider, cross-site scripting, ransomware and others.

Why managed services?
Managed services is the most effective prevention and protection from these malicious threats. They include a full range of proactive IT support that focuses on advanced security such as around the clock monitoring, data encryption and backup, real-time threat prevention and elimination, network and firewall protection and more.

Not only that, but because managed services are designed to identify weak spots in your IT infrastructure and fix them, you'll enjoy other benefits including faster network performance, business continuity and disaster recovery as well as minimal downtime. One of the best things about managed services is the fact that you get a dedicated team of IT professionals ready to assist with any technology problems you might have. This is much more effective and budget-friendly than having an in-house personnel handling all your IT issues.

Being proactive when it comes to cyber security is the only way to protect what you've worked hard to build. If you'd like to know more about how managed services can benefit your business, just give us a call, we're sure we can help.

Shiny gadget of the month:
Digitsole : The smart shoes and insoles

During the latest CES (Consumer Electronics Show) in Las Vegas a company called Digitsole introduced their products that have been several years in the making...smart shoes and soles.

With all the wearables and smart technology it was only a matter of time. The thing that sticks out to me the most is that these are not just fitness trackers, they can also be used to heat your shoes, or in the case of the shoe, tighten them for you. Since we are coming to the end of winter, and having spent the past months in the cold, the idea of self-heating shoes sounds very appealing. When spending extended time out in the cold one of the first places that gets cold usually is your feet and toes. Even sitting in an office at your desk feet tend to get cold easily. The idea that all I would need to do it pull up an app on my phone and I can get nice toasty feet sounds wonderful.

The full lineup as shown on their website includes a Smart Sole, Heated Sole, Smart Shoe, and Smart Sneaker. The smart sole being the most basic with pretty detailed feedback about running analysis, it points out injury risks, audio coaching, and measures your performance. The heated sole naturally provides heating as well as movement tracking. The Smart sneaker provides similar features to the soles, but is a complete shoe and has longer lasting battery. The smart shoe is basically an upgraded version of the sneaker but looks more futuristic and has self-tightening (think automatic lacing) as well as wireless charging.

All of these devices are controlled through an app for your phone for both iOS and Android. It will allow you to control the heat for each foot individually as well as use voice commands.

While these smart footwear products are available overseas now they are expected to make landfall in the US this year around September with price ranging from $149 - $350. For a more detailed look at these products take a look at their website www.digitsole.com.

Security breaches: tips for prevention

As long as businesses host valuable data, cyber criminals will continue to bypass the security protocols meant to protect this data. The causes of security breaches range from device theft or loss, weak and stolen credentials, malware, and outdated systems that use ineffective security measures. And with these five tips, you can take the first step toward making sure a security breach never strikes at your precious business data.

Limitation of lateral data transfers
Employees not being educated on data sharing and security is one of the biggest reasons for internal data breaches. It's a good idea to limit access to important data and information by restricting access privileges to only a small number of individuals. Also, you can decide to use network segmentation to cut unnecessary communication from your own network to others.

Keeping your machines and devices updated
Internal breaches might also occur when employees work with unguarded or unprotected machines. They might unknowingly download malware, which normally wouldn't be a problem if machines were properly managed. Updating your operating systems, antivirus software, business software, and firewalls as often as possible will go a long way toward solidifying your defense systems.

Use monitoring and machine learning to sniff out abnormalities
It's not all on your employees, however. Network administrators should employ monitoring software to prevent breaches by analyzing what is "normal" behavior and comparing that to what appears to be suspicious behavior. Cyber criminals often hide in networks to exploit them over a long period of time. Even if you miss them the first time, you should monitor suspicious activity so you can recognize impropriety and amend security policies before it goes any further.

Continued on page 4....

Gift Card Trivia!

This month's question is:

How do hackers attempt direct you to a fake site to steal your Gmail credentials? *(Hint: The answer is in this newsletter.)*

a. By the time you open the email, it's too late
b. Secret Question
c. A virus
d. An attachment

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **April 3rd**, 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
- 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
1120 Crown Point Road
Westville, NJ 08093

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.swktech.com

SWK TECHNOLOGIES

Security breaches: tips for prevention

Continued from page 3...

Creating strong security passwords and credentials

No matter how often we say it, there's always room for improvement when it comes to your passwords and login procedures. In addition to text-based credentials, you should require other methods whenever possible. Great for fortifying your network, fingerprints and smart cards, for example, are much harder for cyber criminals to fake. Regardless of which factors are used, they must be frequently updated to prevent breaches, accidental or otherwise.

Security Insurance

In the end, no system is perfect. Zero-day attacks exploit unknown gaps in security, and human error, accidental or otherwise, can never be totally prevented. And for this reason, businesses need to start embracing cyber insurance policies. These policies help cover the damages that might occur even under a top-of-the-line security infrastructure. Considerations for selecting a policy include legal fees, first and third-party coverage, and coverage for reputation rehabilitation.

The field of cyber security is overwhelming — even for seasoned IT professionals. But not for us. We spend our days researching and experimenting to craft the best security solutions on the market. If you're interested in one of our cutting-edge network support plans, call us today.