IT Strategy Brief

ISSUE 4 | VOL 3 | April 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Not even devices disconnected from the internet are safe

By now you have probably heard about dozens, if not hundreds of different ways hackers exploit computers and computer networks. Each way more crafty then the last. There is one theme that is usually common across these attempts...the internet. Hackers usually find their way into your network or connected device because of that "connected" part. When you are connected to the internet it is a gateway for anyone to potentially reach you. However, if you are trying to stay off the grid and protect sensitive data you might just say to yourself "I just won't connect that device to the internet and they can't get me". This seems like a pretty air tight concept, but of course someone somewhere found a way to bypass this.

Naturally the only way to get past all this is to find other ways to relay data other than the web. A group of researchers at Ben-Gurion's cybersecurity lab devised a way to obtain data from a computer that is secured in what is known as an "air gap" where the computer is disconnected from the internet. All they needed to do was get malware planted on the system. How? You just need to get an insider or a way to get the malware on the computer with a USB or SD card. Which could be as simple as paying someone to infect it, they don't have to go download the hard drives or do anything crazy either, just plant the malware on the device. The next step is to recover that information and you'll be shocked at how they did it...

Continued on page 3...

What our clients are saying: DiSabatino Landscaping

"The two things I like most about SWK Technologies's services are the immediate attention our calls and emails receive, as well as the benefits of reduced costs and less downtime ever since hiring your company.

We were particularly happy with how SWK Technologies switched out Chris DiSabatino's laptop that he wasn't satisfied with after buying it new.

It is nice to deal with a company that values customer service as much as our company does.

I can't think of anything you can improve. Keep up the good work!"

Tessa Marks
DiSabatino Landscaping

DiSABATINO LANDSCAPING

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Bob Lunny
ClientLink

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 **May 5th** to get your name in the hat.

You could win a $25 Gift Card!

Mobile malware on Android apps

Smartphones are basically palm-sized computers. As such, they deserve the same protection as desktops and laptops. While there is no need to install bulky security software to protect against cyber threats, there are steps users can take to prevent cybercriminals from penetrating these small computers.

Mobile malware MO
Malware and other threats pose risks that are as harmful as those that infect desktops and laptops. Some of the threats include messing up your phone bill, ruining your mobile phone's data, remotely locking and unlocking devices, intercepting messages, prompting fraudulent log-in commands, and sending fake notifications, among others.

Most malware comes from applications downloaded from third-party app stores. Once a phone is compromised, the hacker will have access to passwords, user accounts, and other sensitive personal data. Since some Android devices are linked, there is also more than a passing chance that bugs on one device find their way to linked devices.

Who is responsible?
The burden doesn't fall solely on smartphone users; app stores such as Google Play Store are responsible, too. Some of the infected banking and weather forecast apps that were widely reported were downloaded from the Google Play Store. Aside from taking swift action against the apps, infected companies were urged to provide as much information and updates as possible regarding the malicious applications so they could be removed from the store to protect users.

Of course, Android users are responsible for their own safety, and there are several measures they can take to avoid becoming victims.

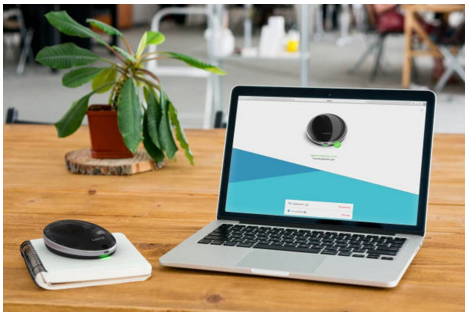
How to avoid being victimized by malware
Yes, the Google Play Store isn't 100% secure, but downloading from the Google store and other more established app stores — and not from little-known and less secure third-party stores — reduces the probability of downloading malicious apps. In case an infected app makes its way to the store and gets thousands of downloads, Google is usually quick to remove the threatening app from their environment and block other malicious entities.

It also pays to read the user reviews. Despite app stores' best efforts, the proliferation of apps in today's marketplace makes it nearly impossible to prevent mobile malware from getting through to the store and, afterwards, users' device.

If an app poses significant risks, someone is bound to post a review or a warning. Regularly updating your mobile device's software also helps prevent attacks, as the latest software version often comes with stronger security patches or quick fixes.

Malware doesn't discriminate. Regardless of your computing or communication device of choice, it will find a way to infect and destroy. Ascertain your business devices' safety by consulting our security experts today.

Shiny gadget of the month:
Keezel : the mobile VPN for security on the go



If you have read our newsletters in the past or have paid attention to the news by now you have probably heard about the risks involved with using Free or Public WiFi. It can be great to have access to WiFi in a hotel or in an airport while you are waiting on a flight, but the problem is everyone else has access to that internet connection too. That means that a crafty hacker could potentially snoop on your device and see what you are up to.

This is where the Keezel comes in. It acts as a portable VPN (virtual private network) that secures your connection. It works on any WiFi connections and connects to your favorite devices. You just simply connect the Keezel to WiFi and you are good to go, no need for any software. Not only does it provide privacy but it can be used to enjoy content wherever you are in the world by using a server in a local area to access content that may be geographically restricted. You can even charge your devices using its large power bank. Setting it up is an easy three steps, just hit the power button, connect to the Keezel in your WiFi settings, and then use the internet. It is that easy.

The devices also comes with two levels of service. You can subscribe to their Premium service for $5 a month that allows you access to higher speeds and more servers throughout the world. The basic service is free but comes with less servers to access and lower speeds, which is fine for email and browsing, but not for streaming HD video. The Keezel is still in the pre-order stage where that you can view on their Indiegogo page http://bit.ly/keezel-gadget . They are supposed to start shipping this summer with a few different versions. It starts out at $144 for a basic package that is just simply the Keezel device. The $179 premium package comes with the device and a year of service. They range all the way up to a $479 premium lifelong package that gives you the premium service forever.

In today's world with an increasing number of threats and more and more WiFi access this seems like it could be a very handy device to have, especially for those who frequently travel.

Not even devices disconnected from the internet are safe

Continued from page 1...

The research team from Ben-Gurion University took a drone and used it to fly up to the window of an office building and view the computer's hard drive indicator light. That tiny little light that blinks when your hard drive is in use is all that they needed to transmit data and steal information off of the computer in the "air gap". You can even see for yourself with this YouTube video how they did it http://bit.ly/air-gap.

Each blink of the indicator light is like a morse-code signal that a drone, or even a telescopic lens could view and use as information. While the data transfer rate is not exactly high speed internet (only about a megabyte every half hour) it is fast enough to grab an encryption key in a couple seconds.

As mentioned before this is not some operation you see in the movies with someone breaking in and having to download files and get out or your screen gets locked up with a virus. In fact this is so covert that you would likely have no idea it is happening. The hard drive light is always blinking so that would never tip you off. All someone needs is a simple smartphone camera which can capture data at around 60 bits per second or as advanced as a high -frequency light sensor it could capture data at 4,000 bits per second. The light could even blink so briefly, that with a high-frequency sensor it would be undetectable with human eyes.

The good part about all of this is that there are some easy ways to avoid this type of attack. For one avoid keeping any devices you are keeping in the "air gap" (disconnected from the internet) in a room away from windows. Another way is just cover the LED indicator light, plain and simple. So while the solutions might be pretty simple to prevent something like this, the idea is to keep your mind open about the fact that hackers will always be searching for new ways into your devices.

Gift Card Trivia!

This month's question is:

When a computer is disconnected from the internet it is also known as being kept in ____? *(Hint: The answer is in this newsletter.)*

a. The Stone Age
b. Purgatory
c. A Bubble
d. An Air Gap

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **May 5th**, 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

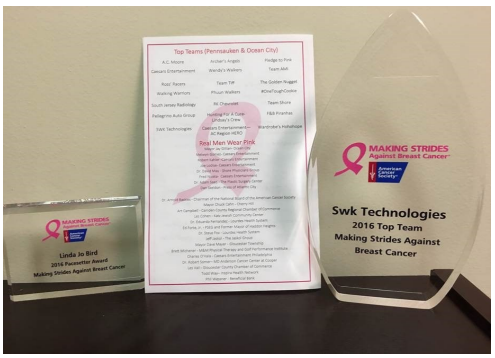
North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swktech.com

SWK TECHNOLOGIES

SWK a top team for Making Strides Against Breast Cancer



Each year SWK participates in the Making Strides Against Breast Cancer 5k in October. For our 3rd year in a row, SWK Technologies received a Top Team award for raising money for Making Strides Against Breast Cancer. On February 16th, Linda Jo (LJ) Bird and Cathy Lyons attended the celebration of gratitude dinner and accepted the team award. LJ also received a personal award for hitting Pacesetter status for the first time, raising over $2,500.

SWK had our biggest team participation in 2016 and raised over a whopping $7,700. To blow your mind even more, we have raised a total of $30,250 for this organization since first participating in 2011.

A special congratulations to LJ for all of her hard work for this event year round. Congratulations and thank you all for your hard work in fundraising.

Please save the date for the next event at Cooper River Park:
Sunday, October 22, 2017.