IT Strategy Brief

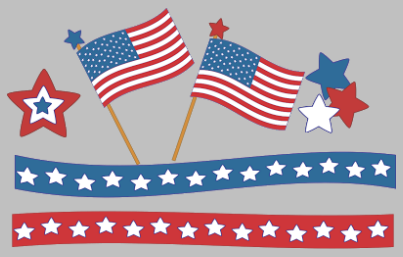
ISSUE 7 | VOL 3 | July 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

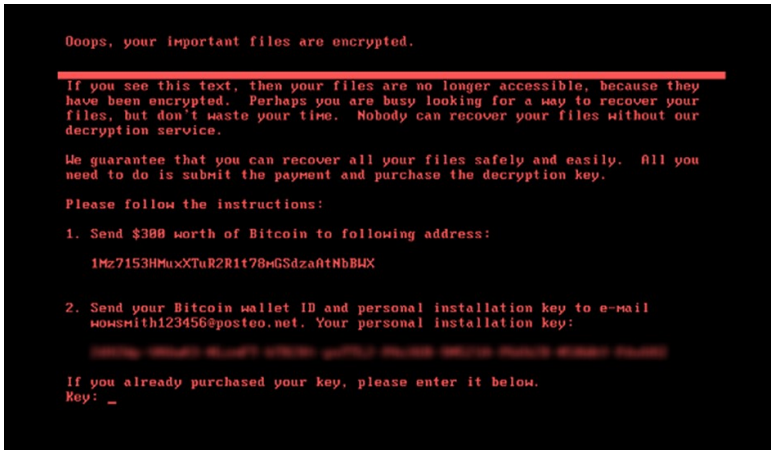
"Useful Technology Ideas for Your Business"

What's Inside:



GoldenEye Attack: Was it just ransomware, or something more?

GoldenEye, Petya, NotPeyta are probably names you have heard thrown around this past month and they all are referring to the same thing... the latest and greatest iteration of ransomware. At the very end of June the GoldenEye strain of the Petya ransomware made headlines worldwide. The attack started out in the Ukraine but quickly spread from there. Huge companies, such as Rosneft, the largest oil production company in Russia all the way to one of the largest pharmaceutical companies in the world, Merck, right here in New Jersey were hit.



This is another instance of hackers using the NSA's EternalBlue exploit that took advantage of Windows PC's just like WannaCry did the other month where you don't need to be the person to open the phishing email to get infected, just someone on your network. Perhaps even scarier is that ransomware attacks like this don't even need to be carried out by computer experts. There are forms of ransomware for sale out on the dark web as a do-it-yourself kit, where creators take a cut of the ransom.

GoldenEye spread to billion-dollar companies with big wallets, but recent reports may have found ulterior motives...

Continued on page 3...

What our clients are saying: Procacci Development Company

"You guys are absolutely the best. I would recommend the services of your organization and staff to anyone who needed excellent IT Services."

Michele Mertz
Procacci Development Company

PDC Procacci Development Company

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Neo Galicia
BCA Watson Rice LLP

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 **August 7th** to get your name in the hat.

You could win a $25 Gift Card!

How good is your web browser's security?

Recently, an unprecedented strain of ransomware known as "WannaCry" infected hundreds of thousands of computers across the globe. This horrible campaign has forced small businesses to revisit the security of their IT infrastructure. It's a complicated endeavor, but reevaluating your web browsers is a quick and easy place to start.

Microsoft Internet Explorer (IE)/Edge
Despite their nearly identical logos, Edge and IE are actually different browsers with vastly different security strategies. Microsoft's legacy browser, IE, isn't even fully supported anymore. The most recent version still gets occasional updates, but experts don't expect that to last for long. If any website or services claims to require IE to run, consider that a possible red flag.

Windows 10's default browser, Edge, is a different story. This browser uses a technology called *virtualization* to create safe spaces to open and test links before granting a website's programming code full access to a computer and user. Edge is based on the same software as IE, and the majority of its security improvements come from scrapping the browser's customizability. If you're okay with a fairly inflexible browsing experience, Edge is a good option.

Apple Safari
Safari is to Macintosh computers what IE is to Windows machines. Safari comes pre-installed on OS X and it has a long history of battling malware. Its security programming has been bested a number of times, but usually in research settings. The commonly held belief is that Safari just doesn't have enough users to make it a profitable target. Apple has a history of responding quickly to malware, but we don't recommend leaving anything to chance.

Mozilla Firefox
One of the earlier third-party web browsers to gain popularity was Firefox. Unfortunately, it just can't keep up with the competition. In just one example, all the data from browser plugins is stored in the same location, which means a compromised add-on could easily gain access to the data stored in a password manager.

One of the reasons that Firefox continues to stick around is its commitment to privacy. All the other browsers on this list profit from analyzing (and sometimes selling) your browsing habits, while Firefox has cornered the market on privacy. Security and privacy should never be confused, but if the latter is more important to you and you aren't installing third-party plugins, Mozilla is an OK option.

Google Chrome
Chrome is used by almost two-thirds of all internet users, and for good reason. Like Edge, Chrome also uses virtualization to create a quarantined space between the internet and your computer. Additionally, Google issues routine security updates to its browser more frequently than any of the others on this list. There is near unanimous consent among experts that Chrome is the safest of all web browsers.

Privacy however, is a whole other ball game. Pretty much every action you take using the Chrome browser is tracked, stored and analyzed. That's not to say that your email isn't encrypted or your saved passwords aren't safe, it just means you have much less control over your internet identity.

Shiny gadget of the month: ORWL : The ultimate secure PC

It seems like every day there is a new threat and a more advanced way that hackers are infiltrating computers. Sometimes it may seem like you are defenseless (at least if you are not being protected by a managed service provider), but now it seems like the tech may have gotten out in front of the hackers with the ORWL PC that is set to ship in August.

The ORWL, which raised over 400% of its goal comes loaded with a number of features to keep your data safe, one of which is a "self-destruct" function that will wipe data if someone tries to physically tamper with the machine. The device itself is actually pretty compact only about the size of your palm and comes with a unique key fob that uses NFC to communicate with the PC. Should you move more than 10 meters away the PC locks itself and shuts down all of the ports so that it is locked down completely. It has a bunch of tamper-monitoring sensors too, like motion/shock detection as well as temperature. If it senses there is tampering with the case to gain physical access it can wipe the encryption key for its hard drive so your data doesn't fall into the wrong hands. It also uses a secure boot, secure firmware upgrade, and a password is needed along with the key fob to turn it back on.

The thing that really makes the ORWL a unique product is the previously mentioned security measures for physical hacking. Software based attacks are a little easier to prevent or recover from, as we have mentioned in previous months the physical hacking is the hardest to prevent. While this PC is more of a niche product it will be interesting to see in the future if some of these physical prevention safety measures are implemented on more mainstream machines.

The ORWL being so unique and niche is also represented in its specs and price, starting around $1700. You can read more on the specs and details on their site http://bit.ly/orwlpc .

GoldenEye Attack: Was it just ransomware, or something more?

Continued from Page 1...

The ransomware GoldenEye hit fast and hard globally. A few of the big name companies that were hit are worth billions, which leads to question the $300 per computer ransom. According to CNET the whole thing may have been a smoke screen and the goal was not to actually collect the ransom, but to in fact destroy the data.

The ransomware displays a message for $300 worth of Bitcoin, but the email associated with this was shut down by the email provider. So even if someone paid they won't be getting the decryption code and their data is lost. The GoldenEye ransomware also take extra steps when it does the file encryption to not only get crucial files, but the entire hard drive and forces the PC to restart after. It even goes as far as deleting the computer's event logs to attempt to completely cover its tracks.

The exact purpose is still speculation, but one thing can be certain, ransomware is here to stay and it appears to be getting worse with each attack. However, you can still take measures to protect yourself. Education of employees for spotting phishing attempts can make all the difference as well as keeping your systems up to date.

How to Protect Yourself

If your servers and workstations are covered under a SWK Network Service plan you are likely fine. However, if you are not covered by a Network Service plan we recommend ensuring that your systems have been patched to protect your network from Petya. Consumers who have up-to-date software are more likely to be protected.

Gift Card Trivia!

This month's question is:

What happened to the email that you used to send in the ransom for the GoldenEye attack? *(Hint: The answer is in this newsletter.)*

a. Nothing
b. It sent you the encryption key
c. It sent you a virus
d. It was shut down

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **August 7th**, 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
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.swktech.com

SWK TECHNOLOGIES

SWK at the New Jersey Land Title Association Conference

Last month the NWS team attended the New Jersey Land Title Association (NJLTA) conference at The Sagemore Resort on Lake George and had a great time meeting the attendees there and hearing about all the first-hand issues that they were encountering. Cyber security, email phishing and ransomware in the title industry were surely the hot topics! Since title companies handle large transactions all the time it makes them a prime target for phishing attempts to have funds transferred to hacker's accounts.

Protecting your business is important to us and after hearing about so many personal experiences with phishing threats and exploits, we wanted to make sure everyone is educated on phishing and that there is actually a service to help train employees. If you had not read about it before in our newsletter you can contact us to find out more information on Phishing Defender. Education and vigilance are our best defense against phishing and ransomware and that's what Phishing Defender is about!!