IT Strategy Brief

ISSUE 3 | VOL 5 | March 2019

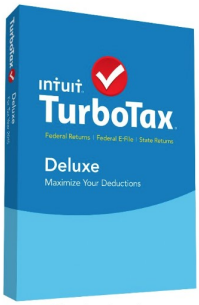
INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:

Hackers Target TurboTax Users to Gain Tax Return Data



Software developer Intuit recently released a letter to TurboTax users warning them that they may have been victims of a cybercrime attack. At least one account was found to have been breached possibly using credential stuffing methods that leveraged leaked username and password combinations. Intuit alerted their users that the unauthorized access may have allowed the malicious actors to obtain past or current tax return information. The developer provided measures for those affected to reactivate their accounts, which were shut down to prevent further access by hackers.

Tax Season is Phishing Season

Tax return season is a favorite period of cybercriminals to launch phishing campaigns for several reasons, but chief among them is the high volume of financial data being exchanged. Potential victims are either sending information out or expecting email notifications or checks in return. Some are rushing to do last minute audits and looking for quick, easy or free ways to download tax preparation applications such as TurboTax.

This makes it easier for hackers to hijack these processes at any one of many stages and gain access to sensitive data. Capitalizing on the fast pace and desperation of the season, cybercriminals wait for their victim's guard to be let down and then send out a phishing communication disguised as a trusted source. This can take the form of an email from the IRS asking for e-Service account information or from a software provider such as Intuit featuring an update for their application.

Tax Preparation Professionals Targeted Too

Casual users of tax software are not the only potential victims targeted by hackers and tax preparation professionals were a prime objective of cybercriminals in previous tax seasons. Tax preparers can be a lucrative avenue to exploit as they give access to the data of multiple victims through a single channel. Hackers that successfully phish a preparer or preparation agency can siphon the information of their clients at their leisure.

As many of these professionals use their own versions of tax software on their work machines, scammers can use the methods outlined previously to break into these databases just as they would a personal one. That means that breaches such as the most recent suffered by TurboTax can generate an eventual windfall of personal data if the right account is hit. In addition to fraudulent tax returns, hackers can leverage this information for increased credential stuffing attacks in the future.

Protect Your Network Against Phishing During Tax Season

Phishing is a human error-reliant method of obtaining tax information that remains one of the most popular cyber scam techniques. Defending against the inevitable phishing attack is a matter of educating and training users to spot the signs of an attempt.

Sign up for our Phishing Defender solution for access to resources and employee training that will give you the tools needed to fight against data breaches.

What our clients are saying: Parts Life, Inc.

"Help is always available at SWK Technologies when you need it. Their staff is friendly and courteous. They get back to you promptly and stay on top of your issue. It's a pleasure working with a company that cares."

Meredee Parsons
Parts Life, Inc.

PARTS LIFE, INC.

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Justin Jones
Chelsea Textiles

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

You could win a $25 Gift Card!

Cybersecurity-Informed Employees Save Costs

Employees can help as much as hurt an organization's network security, says South African cybersecurity expert Charl Ueckermann. The CEO of Johannesburg-based AVeS Cyber Security told Independent Media that while internal personnel are seen as a business's biggest threat, they are also the greatest resource for maintaining IT security when properly informed. "Educating employees on cyber threats and how to use IT resources and the internet securely can help lower security risks, as well as the costs associated with managing those risks."

Employee ignorance of cybersecurity best practices often represents one of the biggest gaps that can exist in your network defense. However, as experts like Ueckermann point out, everyone within an organization can become its best defender if armed with the right knowledge and training to be able to identify and respond to cyber risks. These informed personnel consequently avoid data breaches and malware infections, which cuts costs from downtime, privacy regulation enforcement, and all the other expenses of a cyber attack.

Learn How to Combat the Cybersecurity Risks for Everyone
Successful network security requires building your business culture around the right ways to defend against an attack. Committing to awareness training and teaching your employees techniques for preventing intrusion will enable your business to avoid incurring the significant costs of a breach.

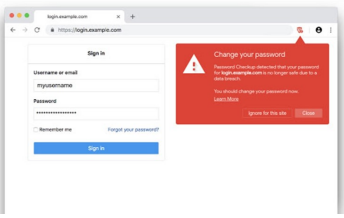
Visit the swknetworkservices.com website often to see what webinars we have to offer so you can learn more about the common cybersecurity risks and how you can combat them.

Chrome's latest extension Password Checkup will warn you if your passwords have been compromised

In today's age of cybersecurity there have been frequent hacks and data leaks you hear of in the news to the point where it has become regular. Odds are you may have even been one of the millions potentially affected. Google recently taken security measures a bit further to help chrome users manage their credentials. They released a new extension for the Chrome browser that allows you to get an alert if you enter a username / password combination that Google "knows to be unsafe." Google says it has a database of 4 billion credentials that have been compromised in various breaches that it runs your password against.

Should your credentials be affected you will get a prompt from a red dialog box to update your info.

Learn about unsafe accounts wherever you sign in



You may be wondering what exactly Google is doing with your data, but they promise to never report any information about your accounts, passwords, or device. They wrote a blog further detailing this information https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html . Aside from the alerts, another nice feature is that Password Checkup won't be a stickler about your passwords if you do need to change it (like telling you to use numbers and special characters). It just lets you change your password and will notify you of any that have been compromised.

In a digital world where you can never be too safe a tool like this could come in handy. If you wanted to take a look at the extension for yourself you can find it on their chrome web store.

Shiny gadget of the month: Wacaco Minipresso NS, Portable Espresso Machine

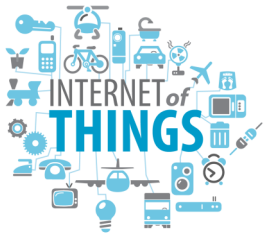
Have you ever had the craving for an espresso randomly throughout the course of your day? Maybe you hit that mid-day, post-lunch point where you just need something to give you some energy. The Wacaco Minipresso machine is the nifty little gadget for you then no matter where you are.

The portable espresso machine is small and light, making it easy to bring along wherever you are headed. It uses small quantities of water to inject into the coffee adapter, and after a few pushes the optimal pressure is reached and the espresso is extracted. It doesn't require anything like compressed air or electricity for operation so you can prepare your drink anywhere. It also uses little pods so it is convenient for transportation and getting the right measurements.

The only real drawback is that if you are out in the wilderness and need an espresso you will have to settle for a cold one since you would need to use hot water in the machine. However, if you just need the pick me up a cold espresso might just work fine.

It is a pretty neat little gadget, and it is even under $50, so maybe it is worth a shot if even just for the novelty of it. You can check out the Wacaco Minipresso on Amazon here.

The Network Security Challenge of IoT



The Internet of Technology (IoT) is the term used to describe the network of connected sensors and sensor-driven machines utilizing wireless technology such as Wi-Fi and RFID. Popular examples include smart home devices such as the Nest thermostat or the Amazon Echo speaker. However, Industrial IoT applications that deliver value to enterprise-level commercial processes are increasingly entering professional spaces – which creates a whole new reality for network security.

IIoT devices are by definition constantly connected to a network, which means they represent potential entryways for hackers looking to gain access to data deeper within the system. Machines existing in an IoT network are new endpoints that have to be continuously monitored and cybersecurity experts have portrayed these applications as an inevitable nightmare for IT security practices. The good news is that network security in the wake of IoT is possible - it will just require a whole new level of vigilance.

The Entire Network is a Threat
Often the hardest concept for unaware users to grasp is that IoT devices effectively create a security gap that can span your entire system. They potentially remove the need for social engineering attacks and luck as the primary means to breach a network as these connected machines act like lighthouses guiding hackers to ports of entry.

Attackers that have previously broken into consumer-level appliances have relied on the security of those devices correlating with their individual value, meaning that they were protected only as much as they were worth by themselves. These applications can longer be treated as one particular system to be monitored, but as a node existing unceasingly within the whole network.

Hijacked Devices
Common workplace security practices have still not caught up to the reality of every networked device being a danger. IoT raises that threat exponentially – now every machine is a vehicle that can be used to access its partners. This is how attackers have historically deployed botnet attacks such the one that affected networks across the US East Coast in 2016.

If utilized within an IIoT network, such an attack could cripple a business – or several. As cyber warfare becomes an increasingly viable option for resource-strapped nation states and terrorist groups, this will likely be tactic employed to attack American infrastructure through enterprise-level and mid-market manufacturers.

Distributed Security
Even while the IoT network act as an ocean in the digital space, the reality is that the physical side of each device still exists in one place, and that is often what throws off businesses using contemporary security practices. IT units have gotten used to monitoring devices from a centralized data silo, which is what creates the reactive methodology that has produced so many data breaches in the past.

This strategy will be next to impossible maintain in the age of IoT as each appliance becomes a network unto themselves. The distribution of networked functions will require a distribution of security and cyber intelligence tasks in turn.

Commit to Monitoring Your Network if You Deploy IoT
IoT is one of the biggest cybersecurity concerns in 2019, and that concern will only grow along with its IT footprint. Yet the benefits of IIoT mean that businesses can capture significant value from deploying connected devices to optimize operational processes. Do not be afraid to consider an investment in IoT, but be ready to commit resources to keeping your network secure if you leverage this technology.

Sign up for our Network Vulnerability Testing service to adopt a solution that will keep your IoT investment protected.

Gift Card Trivia!

This month's question is:

Tax season is a big target for hackers, what the main method used to gain access to individuals as well as professionals accounts? (Hint: The answer is in this newsletter.)

a. Brute Force Attacks
b. Phishing Emails
c. USB drives
d. Encryption

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **April 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
- 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 NETWORK SERVICES

SWK Technologies Recognized for Excellence in Managed IT Services

SWK Technologies Named to CRN's 2019 MSP500 Elite 150

EAST HANOVER, NJ, March 05, 2019 -- SWK Technologies, Inc. (SWK), has been named to the 2019 Managed Service Provider (MSP) 500 list in the Elite 150 category by CRN®, a brand of The Channel Company. This annual list recognizes North American solution providers who have cutting-edge approaches to delivering managed services. Their offerings help companies navigate the complex and ever-changing landscape of IT, improve operational efficiencies, and maximize their return on IT investments.

In today's fast-paced business environments, MSPs such as SWK Technologies play an important role in helping companies leverage new technologies without straining their budgets or losing focus on their core business. CRN's MSP 500 list shines a light on the most forward-thinking and innovative of these key organizations.

"Capable MSPs enable companies to take their cloud computing to the next level, streamline spending, effectively allocate limited resources and navigate the vast field of available technologies," said Bob Skelley, CEO of The Channel Company. "The companies on CRN's 2019 MSP 500 list stand out for their innovative services, excellence in adapting to customers' changing needs and demonstrated ability to help businesses get the most out of their IT investments."

"We're proud to be named to the CRN MSP500 Elite 150," said Mark Meller, CEO of SWK. "Our team, under the leadership of Bill Michael and others, continues to provide cutting edge products and services which help our customers navigate the challenges and complexities of today's cyber environment. Whether in cybersecurity, application hosting, business continuity, disaster recovery or helpdesk, the SWK team helps our customers protect their data and recognize value for their IT investment each and every day."

The MSP500 list is featured in the February 2019 issue of CRN and online at www.CRN.com/msp500.

About SWK Technologies:
SWK Technologies, Inc. (www.swktech.com) is an IT consulting company that develops and provides internationally distributed on-premises and cloud solutions, including Sage ERP, MAPADOC EDI, Time & Billing, Acumatica, NetSuite, Nectari, AccellosOne WMS, and other business software essentials. SWK's network services division provides comprehensive IT infrastructure management, security, back up, and business continuity services. SWK's parent company, SilverSun Technologies, Inc., is publicly traded (NASDAQ: SSNT).