IT Strategy Brief

ISSUE 12 | VOL 3 | December 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

What the Uber hack can mean for you

Just a few days before Thanksgiving, Uber CEO Dara Khosrowshahi announced that the globally-spanning personal transportation service had been the victim of a serious data breach. The attack occurred over a year ago in October 2016 under the previous CEO's watch, though the company was not made fully aware of the incident until the following month. Details are still coming out, but it appears that two perpetrators somehow accessed a third-party cloud server and acquired the information of 600,000 Uber drivers and 57 million customers.

Khosrowshahi's predecessor evidently decided to give into the demands of the hackers, and paid them US $100,000 with the promise that they would delete all of the data they had stolen. Khosrowshahi learned of the past breach some time before revealing it to the public, however, he claims he opted to investigate further and take steps to address it before making an announcement. Despite this assurance, the CEO was found to have already informed a potential investor about the attack before alerting everyone else, including authorities.

Uber has taken several steps to rectify the situation and regain the public's trust, including terminating two employees (Chief Security Officer Joe Sullivan and lawyer Craig Clark) who were involved in the initial response to the breach. Additionally, they have notified regulatory agencies of the breach, brought on cybersecurity expert consultants, and have offered increased protection and monitoring efforts for the drivers targeted and their hacked accounts. They have also offered numerous apologies for the behavior of the company immediately after the incident, though not all find this sufficient. U.S. lawmakers from both sides of the aisle have called on Uber to provide more details about the breach and the company's management of it.

Continued on page 2...

What our clients are saying: C. Abbonizio Contractors, Inc.

"SWK Technologies services have been very prompt and they always have a solution. A few months back a tornado came through the area and our server went down because we had lost electricity. Within an hour of calling SWK someone was at our office with a smile and cupcakes to get us back up and running."

Maureen Cleary
C. Abbonizio Contractors, 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:

Beverly Federman
Chowns Fabrication and Rigging

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

You could win a $25 Gift Card!

What the Uber hack can mean for you

Continued from page 1...

Both Democrats and Republicans have sent letters to Uber condemning the initial response and demanding more detailed answers. There is a very real possibility that the company may have violated multiple state and federal laws by paying the hackers, requesting the hackers destroy the evidence, electing not to inform the public or regulators, and informing investors before anyone else.

Uber has experienced a similar situation before in 2014, when they experienced a previous breach through a cloud server on Github.com and failed to alert either the drivers affected or the authorities for almost six months. They were forced to pay a $20,000 fine for their negligence.

Though Uber is still giving assurances they have the situation under control and that the data has not been leaked, there are several reports which may indicate otherwise. The Guardian reported that several users received bills for rides in several Russian cities that they never took, while the Independent claims that customers of UberEATS all of sudden found similar charges on their accounts from the same areas.

People across Australia, the Philippines, the United Kingdom, the U.S., and many other countries have had their information exposed by the massive breach. A Cyber Intelligence firm, RepKnight, claims that they have previously found thousands of Uber employee emails posted on the dark web, and that these have been open for sale to hackers looking to make phishing attacks on the company's software. Uber has become a tempting target for cybercriminals – they have access to personal and financial information of people across the world, they have proven to have relatively weak security for their size, and they have a history of not being forthcoming with authorities.

Between this incident or one of the many other recent data breaches where you may have to worry about your information being leaked into the dark web, as a business there is something else you should take away from this tale: protect customer data. No one wants to find out that the company with their credit card information was hacked. Attacks are made every day against organizations of all sizes, from small businesses to government institutions. Some cybercriminals might be relative amateurs, but others are longtime experts with refined techniques. Experiencing an attempted or successful hack is no longer a matter of if, but of when.

Not all of these breaches can be prevented with a technical security measure- sometimes the answer is as simple as being educated. Phishing attempts are a major cause of networks being compromised. SWK Network Services is here to not only manage your network, but can also provide training for employees to detect phishing attempts. We also have the ability to run scans of the dark web to see if you or your company has compromised credentials out there. If you are interested in learning more just give us a call.

Shiny gadget of the month:
HP Sprocket Photo Printer

If you or someone you know loves to take pictures with their phone, then the HP Sprocket Photo Printer could be exactly what you are looking for. People love their phones and love taking picture with them to share electronically, but sometimes it is more fun to have an actual print, especially on the go with friends or at events. HP has created a tiny pocket-sized printer you can take with you and allows you to print photos directly from your phone.

The Sprocket is 3 by 4.5 inches, so it can fit in your pocket or purse and has a rechargeable battery. It uses Bluetooth to connect with your iOS or Android smartphone or tablet so that you can print directly from your device using a social media account or directly from your device's photo albums.

One of the coolest features is that not only that it is super portable, but that it doesn't even use ink. Instead it uses special paper named Zink paper which has heat activated dye crystals in it to create the colors. The one limitation is that it only supports 2x3 wallet-sized sheets, but they do have a peel off sticky back that could be fun.

Overall, this could be a fun device, especially for something like a party or event where people can connect to the printer with their own devices to print off photos. Since they can be a photo or a sticker that adds to the fun factor, and at places like a wedding or even just a get together with friends and family it could be a big hit.

While the Sprocket won't outshine a dedicated photo printer it definitely has its own unique uses for its fun and portability. At $130 it could be a fun gadget to give as a gift this Holiday season.

A recent update for Apple's latest macOS left a huge security bug

Apple first announced the successor to macOS Sierra, High Sierra, in June 2017 and released it to the Mac App Store the following September. Since then, they have applied three updates to the desktop operating system, the last of which created a serious vulnerability. It enables anyone with physical access to a Mac running High Sierra to be able to log in and enter without a password as long as they sign in as a Guest with the username "root." They would then be able to obtain administrator privileges on the machine.

There are a couple ways to use this trick, but they all show up on both the current version of High Sierra and the new beta. Apple released another update (https://support.apple.com/en-us/HT208315) the day after that ostensibly fixes the issue. Previously, the only suggested workaround was creating a new root password or changing the existing one to ensure no one else could get around the administrator authentication. Removing guest accounts entirely also works as a more direct way to prevent unwanted access.

This loophole was apparently caused by a logic error within the system that prevented proper credential validation. The bug was first brought to Apple's – and everyone else's – attention publicly on Twitter by software developer, Lemi Orhan Ergin, shortly after the update was launched. The public and speedy revelation of the glitch likely enabled the tech giant to address it quickly. Though their operating systems are often known for having better than average security, some still have holes that can be exploited.

Apple's security division announced a bounty system for reporting bugs in 2016 with payouts up to $200,000, though VICE's Motherboard reported that this constitutes a fraction of what white hat hackers are normally offered. Certain firms will pay as much as $1.5 million to obtain zero-day exploits and resell them legally on the grey market. The good news is that errors such as the High Sierra login bug are not really common, but Mac users should still take steps to protect themselves, and consider speaking to a professional for a second opinion.

Gift Card Trivia!

This month's question is:

When did the Uber hack occur? *(Hint: The answer is in this newsletter.)*

a. March 2017
b. October 2016
c. October 2017
d. January 2017

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

Microsoft to begin testing a new feature that could become quite handy

If you have ever used a computer before you have undoubtedly worked on something that required multiple sources. For instance, if you had an Excel spreadsheet open, along with a Word doc so that you could create PowerPoint deck. In this example you would have three different windows would have to be open and you would be clicking between them all.

Microsoft

The new vision Microsoft has is that instead of having different windows they would all be confined to the same window and use tabs, much like how a web browser functions. You might think that this is just a minor upgrade in convenience, but the real power that I see in it come from the ability to save a project you are working on along with ALL of the tabs. I know personally this would be fantastic as I consistently have a ton of windows and tabs up at all times in order to not forget about what goes with what. The ability to save a project and all its associated tabs so that if I close it out I can get all of it back from one location.

Microsoft is calling this functionality and groupings “Sets”. Right now it is still in development, but will be going out to select individuals for testing soon. Sets will also work with OneDrive so that you can save and close in one place, then open again somewhere else. They are also working on mobile device support too, so you can start a Set on your mobile device then open it up on a PC or vice versa.

These Sets could become very helpful with the organization of work. While we are all so used to doing things a certain way now, it is likely we will not know how we ever used to do things the “old” way once Sets become available to the general public.