LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Happy Holiday Season!

During the rush of the holiday season, we often find ourselves with many extra items on our to-do lists. Whether those items are related to work, family, faith, or friends, I hope you find the time necessary to complete your tasks *and* have ample time to enjoy all the wonders of the holidays.

For those of you receiving or gifting smart devices, the feature on page 3 is a great reminder on how to keep our personal information safe from fraudsters.

On behalf of the LACFE, I wish you all a safe and happy holiday season filled with joy!

IN THIS ISSUE

Fraud Talk Podcast

Diversity, Equity and Inclusion in the Anti-Fraud Field

Earlier this year, the ACFE hosted a webinar titled, "A Conversation About Diversity, Equity and Inclusion in the Anti-Fraud Field," which is free and available to view for all ACFE members. In this month's episode of Fraud Talk, you'll hear an excerpt where the four panelists share who should be involved in this discussion and why. They also share how anti-fraud professionals can make belonging an integral part of workplace culture.

https://www.podbean.com/ew/pb-t7782-f1ce73

UPCOMING EVENTS

LOCAL:

Michigan Association of Certified Public Accountants
Webcast – MICPA Winter Bonus Program *Free to MICPA Members*
December 15, 2020
8:00 am – 12:50 pm
Learn more: https://store.micpa.org/Product/Details?productId=33311

Michigan Association of Certified Public Accountants
Webcast – Financial Accounting & Reporting Standards: Annual Update & Review of GAAP, Tax & Cash Special Purpose Frameworks, & AICPA's Preparation, Comp, Review & Audit Standards by Walter Haig
January 6 – January 7, 2021 (early registration ends December 8th)
Learn more: https://store.micpa.org/Product/Details?productId=35359

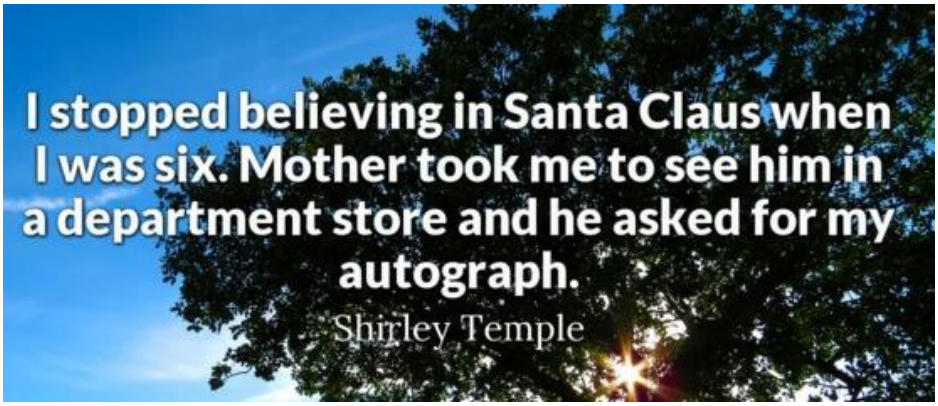
Michigan Association of Certified Public Accountants
Webcast – Hot Topics in the Financial and Reporting Standards: Topics That All CPAs Should Have a Basic Understanding Of! by Walter J. Haig
January 8, 2021 (early registration ends December 10th)
Learn more: https://store.micpa.org/Product/Details?productId=35350

NATIONAL:

ACFE
Virtual – Investigating Conflicts of Interest
December 10 – December 11, 2020
Learn more: https://www.acfe.com/events.aspx?evtid=a3Y1Q000002kXNGUA2

ACFE
Virtual – Bribery and Corruption
January 6 – January 7, 2021 (early registration ends December 7th)
Learn more: https://www.acfe.com/events.aspx?evtid=a3Y1Q000002kgAjUAI

If you have an event that you would like posted in our newsletter or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com



Are Home Devices Really Spying On Us?

By James I. Marasco | Managing Partner

https://stonebridgebp.com/library/uncategorized/are-home-devices-really-spying-on-us/

With the holiday season over, many of you may have purchased or received a smart device. Almost seven out of ten of American households reported owning a smart product. A smart product/device for the purpose of this article is a device that can connect to the Internet using Wi-Fi or Bluetooth—such as a smart speaker, TV, doorbell, lock system, and even pet cameras/treat dispensers. Sales of smart devices increased by 25% in 2018 and are expected to have double-digit growth over the next 4 years. The growing popularity amongst consumers has also opened a door of opportunity for manufacturers and hackers to gain access to your personal lives.

Smart Device Capabilities

Years ago, baby monitors were found to be transmitting conversations through neighbors radio frequencies, causing quite a stir. This pales in comparison to the creation and evolution of smart devices which have grown rapidly in the past few years. Not only are there smart speakers and TVs, it seems like there is a smart device version of everything— a doorbell, refrigerator, light bulb, door lock, thermostat, and even a smart treat dispenser for your furry best friend. As easy as it is for the consumer to remotely unlock their door, turn up their thermostat or spy on their pet, manufacturers and hackers can gain the same opportunity.

Hacking Vulnerabilities

The greatest threat you face with your smart devices is getting hacked. Because smart devices are typically installed somewhere in the home, they don't face the same threat as a smartphone—being lost or stolen. However, if they're hacked, the perpetrator can download the app that corresponds to the device and gain complete access to your private information. With some of these devices, that means the hacker will be able to unlock doors, access security cameras, control lights, and in some cases, even use the microphone to speak to you or your family. Imagine they gain control of your refrigerator and raise the temperature such that all your food spoils or they gain access to your home thermostat and turn it off while you are out of town and freeze your pipes.

In late 2019, over 3,000 Ring Doorbell users were urged to change their passwords and use two-factor authentication following reports that claimed Ring login information may have been exposed online. Gaining access to someone's login information allows hackers to have the ability to view the live camera feed and recording, as well as personal information like phone numbers and addresses. Hackers are able to get this information through a method called "credential stuffing"—this is done by taking usernames and passwords from other data breaches to gain access to your account.

With the world being as digital as it is, almost everything we do requires a username and password. That being said, it would be nearly impossible to keep track of all of them if you made every one of them different. For convenience, many people choose to use the same username and password for a multitude of devices and/or websites. This is exactly what hackers are counting on. If a hacker gets a hold of your username and password for one of your smart devices, they may gain access to your other ones sharing similar login credentials.

Another threat is ransomware. This is a type of malware where a hacker locks your system and demands that a user pay a price to regain control of compromised devices. Municipalities all over the U.S. have fallen victim to this type of attack. For example, in 2018, Atlanta spent several million dollars recovering from a ransomware attack, while Albany, NY spent hundreds of thousands in 2019. Unfortunately, individuals are also falling victim to these type of attacks from hackers as well. As we allow more Internet-connected devices into our homes, our risk increases.

Manufacturer Recordings

Every time a consumer pushes a request through a smart device either through an application or voice command, it is recorded in a server and pinged back to the device to execute the command. All of these commands are being recorded by the manufacturer or service provider. In the privacy settings, some allow you to disable certain features, but most default settings allow for the recording and retention of this data. For example, if you have a Google or Amazon smart hub, you can actually review archives of everything it has listened to or captured through your voice commands. Simply, go into your account, select the device and

review. Hopefully, the information it captured was triggered by the "wake" command and not random listening!

Safeguarding Your Smart Devices

One of the best ways to safeguard your confidential information and privacy with your smart devices is to have different usernames and passwords for each of them, not just the smart ones. According to consumerreports.org, 52% of Internet users reuse or modify the same passwords—that makes it easy for hackers to gain access to your smart devices. Other vital precautions include:

- **Set up a password manager** – A password manager can generate very strong and random passwords for your accounts. Not only that, but it will store them securely and remember them for you. Many of these applications are even free to download!
- **Enable automatic updates** – By regularly updating your devices when a new software is available, you limit the ability for hackers to use a company's known vulnerability as a hole to break in.
- **Set up two-factor authentication** – If the device allows for it, this extra layer of security allows the application to send you a one-time code via email, text message or even a phone call that you input with your username and password. With this feature, if someone attempts to gain access to your device's account, they won't be able to without the one-time code.
- **Do your due diligence** – Be sure to read the terms of service, review the features, and read the manual of the device. Since these documents are typically very long, you can try finding one online and searching for words such as "camera," "microphone" and "privacy". Since this information is being collected and retained by the manufacturers who sell you these products, buy from a trusted source and not the cheapest option available.
- **Turn off device when not in use** – If a device isn't being used, turn it off. If a feature is not used, be sure to disable it in the settings. For example, if you are not using the camera function on your Smart TV, go into the settings and disable the function. If this is not available in the settings or you are still concerned about features like the camera, you can put a piece of black tape over the camera.
- **Pay attention to where you place your smart hubs** – Be mindful of where you place devices that are always on and waiting for a specific wake up call, like an Amazon Alexa or Google Home. They

should not be placed close to first floor windows and entrances as someone could access them from outside your home.

A Balancing Act

It's become so convenient to walk into a room and commend Google, Alexa or Siri to turn on the lights, request the weather or call for takeout. But keep in mind, you are giving up a ton of personal privacy by allowing that information to loosely regulated manufacturers. Furthermore, hackers are finding their way into these same devices raising the stakes considerably. At what point, have we gone to far?

Reindeer Games

Cipher

This is a Ceaser cipher, where each letter of the alphabet has been replaced by a different letter.

Hint: Quote by the 2nd Leader

"Ehfdxvh srzhu fruuxswv, vrflhwb'v ghpdqgv iru prudo dxwkrulwb dqg fkdudfwhu lqfuhdvh dv wkh lpsruwdqfh ri wkh srvlwlrq lqfuhdvhv."

- Mrkq Dgdpv

A	B	C	D	E	F	G	H	I	J	K

L	M	N	O	P	Q	R	S	T	U	V

W	X	Y	Z

Holiday Word Search Challenge

Solve each clue to reveal the holiday-related words to find in the puzzle going across, down, and diagonal.

1. **December 25th holiday:** _ _ _ _ _ _ _ _
2. **Jolly man in red suit:** _ _ _ _ _ _ _ _ _ _
3. **Hung by the chimney:** _ _ _ _ _ _ _ _
4. **December holiday celebrating African-American heritage:** _ _ _ _ _ _
5. **Family customs passed down to next generation:** _ _ _ _ _ _ _ _ _ _
6. **Kwanzaa candle holder:** _ _ _ _ _ _
7. **Hung on a door at Christmas:** _ _ _ _ _ _
8. **Jewish Festival of Lights:** _ _ _ _ _ _ _ _
9. **Special Jewish candelabra:** _ _ _ _ _ _ _
10. **Red and white striped Christmas sweet:** _ _ _ _ _ _ _ _ _
11. **A wax light that is used as a ceremonial symbol of many holidays:** _ _ _ _ _ _
12. **Number of days of Hanukkah:** _ _ _ _ _
13. **Santa's vehicle:** _ _ _ _ _ _
14. **Kwanzaa feast:** _ _ _ _ _ _
15. **Gifts given on the last day of Kwanzaa:** _ _ _ _ _ _
16. **Christmas songs:** _ _ _ _ _ _
17. **Potato pancakes:** _ _ _ _ _ _
18. **They pull Santa's sleigh:** _ _ _ _ _ _ _ _

N	Z	R	D	C	C	J	Y	H	C	H	R	I	S	T	M	A	S
T	L	C	X	U	C	A	N	D	L	E	L	L	L	S	T	I	J
H	F	D	Z	N	N	O	Z	H	R	J	E	C	E	Q	R	G	R
V	O	G	R	C	L	U	A	C	E	W	M	N	R	J	A	Q	R
G	M	O	B	N	O	K	W	H	K	V	A	E	P	O	D	J	K
G	C	E	W	Q	K	O	A	N	R	C	E	W	X	K	I	I	A
S	A	F	N	U	C	G	D	E	Y	D	K	Q	S	V	T	L	R
B	T	S	N	O	O	Z	I	D	N	R	N	E	W	K	I	X	A
D	G	A	T	E	R	E	N	I	L	O	K	N	R	W	O	Q	M
O	H	N	R	O	K	A	E	F	S	T	T	T	E	A	N	L	U
N	G	T	R	H	C	R	H	L	A	K	N	H	A	N	S	F	W
W	Q	A	Q	Q	O	K	O	L	W	N	G	J	T	Z	G	G	G
S	R	C	B	X	I	R	I	H	K	I	C	F	H	A	W	I	P
R	M	L	W	A	A	F	F	N	E	I	W	Y	S	A	G	F	N
P	E	A	Y	C	T	X	P	L	G	I	N	X	T	R	X	T	F
O	Z	U	G	Q	G	U	S	O	D	S	G	A	C	R	D	S	U
S	G	S	V	Z	N	W	V	F	C	D	X	H	R	U	N	E	L
V	W	V	C	E	L	E	B	R	A	T	E	F	T	A	W	M	I

Bonus: Find 5 more holiday words hidden in the word search grid

SCHOLASTIC Find more printables for children at scholastic.com/parents/activities-and-printables

A Riddle:

My life is measured in hours.
I serve you by expiring.
I'm quick when I'm thin.
I'm slow when I'm fat.
The wind is my enemy.

The Clemson University Media Forensics Hub presents: Spot-the-Troll

The quiz where YOU examine images of real social media content and decide whether it's from a legitimate account or an internet troll.
https://spotthetroll.org/

Showtime's "Love Fraud" Explores the Dark Pull of Romance Scams

November 13, 2020
https://acfeinsights.squarespace.com/acfe-insights/showtime-love-fraud-explores-the-dark-pull-of-romance-scams

GUEST BLOGGER
Hallie Ayres
Contributing Writer

Showtime's recent four-part documentary series "Love Fraud" covers a familiar premise: a conman meets a slew of women on dating apps, woos them, convinces them to marry him and then wipes them of their savings and disappears. But directors Heidi Ewing and Rachel Grady have given this particular narrative a twist — instead of focusing on the conman himself, their documentary follows in real time as the victimized women band together to seek revenge.

The series opens by introducing the viewer to some of the women as they recount the deception methods used by Richard Scott Smith, a conman based in and around Kansas City, Missouri. The women detail the lies Smith told them to impress them — that he was about to win a lucrative lawsuit, that he was a pilot, that he was a successful entrepreneur. Then they detailed how he would swindle them out of money for cars and houses before running off with the rest of their savings. At one point in the series, a private investigator reads off the results of a background check into Smith. He had 10 different social security numbers, 43 different phone numbers and 58 different addresses.

The women also explain how they met through a blog started by one of Smith's victims who hoped to spread awareness about his romance scams. The blog, which still exists, grew into a forum for the women to track Smith's moves after he had scammed them in the hopes that they would eventually be able to bring him to justice.

With the help of a bounty hunter named Carla, who takes on the case pro bono because she genuinely wants to help find Smith, the women move forward with their plan to put Smith behind bars. Sabrina, a victim who estimates Smith swindled her out of nearly $100,000, says, "The best way to get over a guy is revenge."

As the show progresses, Ewing and Grady shine light on the state of romance scams today. In one elucidating scene, Carla explains Smith's strategy. "He did not run off with millions of dollars at all … He makes enough money to support his habits, like new trucks and new Harleys. He's a good conman, but he's not a big-dollar conman. He's a nickel-and-dime conman. He goes after middle-income women that have just enough money to make him look good. Meanwhile, he drains them of everything they've worked their whole life for, and it's not that much."

Carla notes that Smith isn't intent on going after one big scam to get rich. Rather, his track record suggests a certain addictive proclivity to the art of the scam and a desire to achieve his goals through legal means, i.e. marriage. Once Smith is able to convince a woman to marry him, their finances are shared, and the high-dollar purchases he made are left to the women to pay back, as is legal and customary with debts and shared accounts. As Grady mentions in an interview with Vox, "[Smith] wasn't some sort of genius, but he was good at reading people in terms of who was vulnerable, what their vulnerabilities were. I think that he was able to really get away with a lot doing that."

Ewing and Grady also make it clear the ways in which the legal system fails the women who come forward seeking justice. There was a warrant out for Smith's arrest since 2017, and reports of his domestic abuse and multiple marriages had been circulating in news outlets since then. Yet the women featured in the documentary series express the troubles they had seeking help from law enforcement.

In one scene, one of Smith's exes details an interaction with her local sheriff in which he said he wouldn't devote any time or resources to her case because Smith had disappeared out of his jurisdiction. In response to this, Carla reminds the victims, "Nobody is going to be active on the streets looking for him, except us." Throughout the production, the directors even had to hire private investigators to track down Smith since law enforcement had not shown any interest in the case.

Speaking to Vanity Fair, Ewing underscored Carla's usefulness in their search for Smith. "She was somebody who understood the law, could help track him and knew how he could be brought to justice legally." Ewing not only highlights Carla's expertise, but she also reiterates the importance of working with someone who is well-versed in rules and regulations when it comes to fraud and cons. The fact that the women did not find this when approaching law enforcement officials, and instead had to turn to a bounty hunter and private investigators, shows how prescient it is to fight fraud in a way that is expansive and empathetic.

The directors of “Love Fraud” see fraud fighting as an extremely crucial field, and they hope that the show encourages victims to come forward with their own stories of being targeted by romance scammers — and that victims receive fair treatment that does not reduce their experiences to a source of shame. Ewing also hopes that the series inspires a sense of caution in women who are dating, especially over the internet. “There are a lot of Richard Scott Smiths out there. Hopefully mothers will watch this with their daughters and say: Watch out for red flags. If it seems too good to be true, it probably is.”

QUOTE OF THE MONTH

"If you haven't got any charity in your heart, you have the worst kind of heart trouble.”

- Bob Hope