

CYBERSECURITY

Presented by the National Auctioneers Association | April 2018

iSeries
Because it's about you.

NAA
Auctioneer

Table of Contents

3

Introduction

4

Is your flashlight app safe to use?

5

mCrime: Mobile cybercrime

8

Is your app putting your customers at fraud risk?

10

Hacked!

13

Are you following data protection laws?

Don't "Ware" out

Dear iSeries Reader,

Remember when it was hard enough trying to keep straight the difference between hardware and software for your computer? Now, anyone with a computer, let alone a company and its networks, has to battle spyware, ransomware, malware, etc.

Anytime, it is nearly impossible to go a full day without hearing about some new form of a cyber-attack, which makes sense when we consider the sheer number of attacks that now take place daily. (The Federal Bureau of Investigation pegs that number somewhere around 4,000 per day.) That number alone is enough to "ware" out a person or company. Still, none of that speaks to the equally tiresome long, complicated discussions a business owner and his or her team must have in identifying data protection needs and potential services; or, getting bombarded with 30 daily "Do this now!" security tips and automatic updates that never seem to end.

In any case, while it is common to hear some of the largest companies in the world being affected by data breaches or misused information, the rapidly growing trend is for cybercrime to target small and mid-sized companies – including in the auction industry. For auction professionals, many of whom fit that small-to-mid-sized

category, it means taking heart and not giving up against SPAM emails and potential buyer/seller data breaches. That's the easy part, however. The harder part is understanding your risk comfort level and then developing and executing a cybersecurity plan

(You want to do this. Google will mark any HTTP site "not secure" beginning in July 2018!)

Buyers and sellers trust that you will keep their data secure. We see the public fallout for companies that have not done

The FBI estimates that there are around 4,000 cyberattacks each day.

that suits your risk tolerance.

There are many products and services that will assist your goal of keeping your data safe, and we talk about some of those on a broad level in this newest NAA iSeries whitepaper. This paper's focus is to discuss some of the kinds of threats that exist, allow you to consider which ones might pose more potential risks to your business than others, and provide some ideas for how you can increase your security.

Some tweaks are simple – updating apps on your mobile device and controlling how much data you expose to those apps, for example. Others, like having your company website use HTTPS encryption, instead of HTTP, might require some professional help.

so, and this is not an issue that will fade away. Data protection is paramount.

Let this paper serve as a springboard into your company's cybersecurity conversation ... and action. That's our hope and goal with this latest installment from iSeries ... *because it's about you!*

Sincerely,

Your iSeries Team

Is your flashlight app safe to use?

You just had a flat tire along a dark country road. Luckily, you downloaded a flashlight app into your cellphone and now can put it to use.

But that flashlight, handy as it is, may be just one of many doors you unwittingly opened to let spies take up residence inside your phone.

"Most free flashlight apps are creepware," says Gary S. Miliefsky, CEO of SnoopWall, a company that specializes in cybersecurity.

Creepware is malware that spies on you and your online behavior, and could pass along information to others.

For example, Goldenshores Technologies, the company behind the popular "Brightest Flashlight Free" app for Android phones, agreed in 2013 to settle the Federal Trade Commission's charges that the software secretly supplied cellphone locations to advertising networks and other third parties.

The problem doesn't begin and end with flashlight apps, though. Many seemingly innocuous apps that people carry around with them on their mobile devices have the capability to eavesdrop on their activities.

"Consumers trust first and verify never," Miliefsky says. "As a result, most of their smartphones are infected with malware that they trust in the form of some kind of useful app or game."

Miliefsky offers these tips for ousting those spies inside the phone:

- **First, assume you've already been compromised.** It's nice to think all is probably well, but most likely it's not. Somewhere in the phone the spies are at work and it's time to take the privacy behaviors and privacy policies of these apps more seriously.
- **Verify the behavior and privacy risks for apps before installing them.** Do some research and ask the question: "Why does this app need GPS, microphone, webcam, contacts, etc.?" Most apps don't need these ports unless they want to invade your privacy, Miliefsky says. Find an alternative before installing risky apps.
- **Do a smartphone version of spring cleaning.** Delete all the apps you don't use that often. Replace the apps that take advantage of too many of your privacy settings, such as GPS, phone and text-message logs, with similar apps that don't.
- **Turn off WiFi, Bluetooth, Near Field Communication and GPS except when you need them.** That way, Miliefsky says, if you are at a local coffee shop or in a shopping mall, no one can spy using nearby (proximity) hacking attack. They also can't track where you were and where you are going on GPS.
- **Check to see if your email has put a tracer on you and your phone.** "If you use a Google email account and have an Android phone, you'd be surprised that even with your GPS off, it's tracking your every move," Miliefsky says. You need to go into the phone's settings to turn off that tracking feature, he says. In your Android phone, go to "settings," then "location." Select "Google location reporting" and set "location history" to off.

mCrime: Mobile cybercrime

Cybercrime goes mobile thanks to insecure mobile banking, mCommerce, and mWallet apps.

By Mark Laich

Millions of consumers no longer visit a bank to deposit checks or conduct financial transactions. Instead they rely on the convenience of using their mobile devices to send money, view account balances and bank online.

The same is true for how they spend their money – the shift from brick and mortar to e-commerce to m-commerce is already well underway. Think about it – how many times do you use your smartphone to research a product or purchase one?

Maybe you're going out to dinner tonight and you've already filled your Apple Pay, Google Wallet or other wallet technology with all of your credit-card information. Ever wonder if you could be pickpocketed wirelessly? Could an app you trust already be stealing your personally identifiable information (PII)? Sadly, the answer is yes.

Many financial institutions and retailers have launched mobile apps in the past 18 months to respond to demands from their customers who want the convenience of 24-hour, anytime/anywhere banking and shopping. Mobile banking apps help build customer loyalty, and mobile-banking transactions are significantly cheaper for banks compared with transactions that require employee interaction.

Mobile-retail apps capture consumers' buying impulse at the moment they occur, and allow for easy comparison shopping – the potential for finding an item cheaper is a quick tap away. Because more and more banks and retailers are making the investment to develop a mobile app,

having one has gone from being a competitive differentiator to a "must have" to compete for consumers' business.

And once a bank has made that investment, there is a concerted effort to encourage customers to use their mobile-banking platform. The same holds true for retail. Amazon and others will do anything to get you to shop online from your smartphone or your tablet.

But the growth of mobile banking and retail apps also means that more people are at risk for identity theft and the hacking of sensitive personal and transaction data by cyber criminals who plan to commit fraud. These apps are used on devices

that often aren't safeguarded from security holes. Most people have between 30 and 75 apps on their mobile device, and of course, when apps are installed on a device, users must grant multiple permissions for

The average person has 30 to 75 apps on their mobile device, leaving them open to a multitude of security vulnerabilities.

accessing a device's location, SMS capabilities, Wi-Fi, Bluetooth, camera and other device resources.

Some of these resources are used for the apps to do their intended task, but often apps demand resources that can open up a device to security vulnerabilities. Unfortunately, when consumers install an app on their mobile devices, few of them read all the permissions the app requests to make sure it isn't asking to use device resources that might be suspicious.

This issue is highlighted by a report from Gartner Inc., the technology research company, which concluded 75 percent of apps in the major app

stores fail basic security tests. Gartner defines this as an app using mobile-device resources that have nothing to do with the intended function of the app. Rather they can be used to eavesdrop on other apps that are running concurrently to collect data about the consumer. The rationale is that the collected information can be used for data analytics to help with targeted mobile advertising.

covertly on the mobile device. Monitoring software can access most mobile device activity and resources, thereby stealing consumer data just like the malware downloaded from an app store.

Most consumers are unaware of these types of threats, and even when they are aware, they don't take actions to protect their security and privacy until it is too late. On the other hand, financial



According to data from the Department of Justice and Privacyrights.org, more than 1 billion PII records have been compromised, resulting in identity fraud totaling \$24.7 billion in losses.

However, this has given cyber criminals a rather large attack vector to commit ID Fraud by using malware that looks like trustworthy apps to steal PII and financial transaction data from mobile banking apps, or to steal your credit-card information from your retail apps that reside on the same mobile device. This type of malware disguised as “trusted” apps has hundreds of millions of downloads from the major app stores.

Worse yet, this new form of malware is undetected by anti-virus and able to circumvent encryption, biometrics, tokenization, sandboxes and authentication. The result is that using mobile-banking apps to conduct transactions is similar to using an ATM to withdraw cash in a dangerous area with criminals lurking around, or handing your credit card to a stranger, in public, who is using the old-fashioned carbon copy credit card imprinter to take your order.

Another popular technique for cyber criminals is spear-phishing attacks – which take the form of email and text messages that appear to be from an official source or someone you know, usually garnered via a social-networking site. These messages can then install monitoring software

institutions carry the liability associated with the fraud that results from data stolen from mobile banking and retail apps. In a U.S. landscape where almost 1 billion PII records have been compromised and there is identity fraud totaling \$24.7 billion in losses – according to statistics from Privacyrights.org and the Department of Justice – greater safeguards are needed to protect consumers’ financial data.

At the same time, it is important not to intrude or detract from consumers’ mobile banking or retail experiences. Financial institutions and retailers can’t solely depend on consumer awareness and training, nor can they make it complicated for consumers to protect themselves.

For better or worse, the modern-day consumer has become enamored with using their mobile devices for apps such as social networks, location-based services, and games on the same device on which they want to do mobile banking and mobile commerce, thereby compromising their security and privacy. What financial institutions and retailers need is new, innovative security technologies that deliver an optimal balance between protecting consumer data and being




un-intrusive to consumers' total mobile-device experience.

In this way, their mobile banking and mCommerce apps can operate in a safe and trusted environment even when multiple applications are running concurrently. By working with companies that specialize in these types of new security technologies designed to thwart zero-day threats and malicious eavesdropping apps, financial institutions and retailers will not only protect themselves from liabilities, they will also be successful at convincing more of their customers to use mobile banking and mobile commerce, thereby increasing the ROI of their mobile-app investment and their operating efficiency.

Finally, as we look forward to what many believe will be the continued rapid adoption of mWallets, you must understand that they are inherently insecure because they operate on already infected devices. It's time to take a completely radical, proactive approach to securing consumers' data as the financial, transaction-based world shifts onto our smartphones and tablets.

This era marks the beginning of a new wave of enablement, opportunity and mCrime. Where there is mobile banking, mCommerce and mWallet there will be mCrime. Assume it comes in the apps as innocent as that flashlight app you recently installed, because if you don't, you'll be left in the dark missing your identity and your wallet.



Mobile malware could create revenues for malware authors touching in the billion-dollar range by 2020.
– McAfee Mobile Threat Report Q1, 2018

Is your app putting your customers at fraud risk?

New forms of malware make bank and retail apps vulnerable.

Mobile apps are becoming big business for businesses, including auction companies.

Many bank customers now check their account balances or transfer funds through an app on their cell phones. Savvy retail shoppers can use a favorite store's apps to learn about discounts, access coupons and find daily deals.

"The apps for financial institutions and retailers are getting greater use and that can be wonderful for business," says Gary Miliefsky, CEO of SnoopWall.

But as with so many things in the cyber world, caveats are connected. Even as companies provide additional services through those apps, they may be putting their customers at risk for fraud.

"Most companies don't realize just how vulnerable their apps are and what the potential is for leaking their customers' personal information," Miliefsky says. "And when that happens, it's bad for business."



69% of organizations don't believe their antivirus can stop the threats they're seeing. - Ponemon Institute, The 2017 State of Endpoint Security Risk Report



Since 2015, daily ransomware attacks have increased 300 percent. – Federal Bureau of Investigation, How to Protect Your Networks from Ransomware

He suggests a few reasons why most companies need better protection for their mobile apps, including new forms of mobile malware are being widely deployed in the major app stores and can eavesdrop on a customer through a company's app.

"These new forms of malware are undetected by anti-virus engines and are able to circumvent encryption, authentication and tokenization," Miliefsky says. "That makes it easy for cyber criminals to exploit the personal information of a company's customers and commit fraud."

PCI Data Security Standard

The PCI Data Security Standard requires merchants to protect credit-card holder data. Likewise, mobile-commerce providers must protect any payment card information, whether it is printed, processed, transmitted or stored, Miliefsky says. "Even though a customer has the breach on their mobile device, the retailer is responsible because it was their app that allowed the eavesdropping."

A breach of credit-card information potentially could result in fines for the retailer, Miliefsky says.

The FDIC's view

The FDIC requires banks that are providing an ATM-like online or mobile-banking experience to protect access to the confidential records of the consumer, the consumer's bank account information, user name and password credentials, and bill payment and check-deposit services. Just like with retailers, it doesn't matter that the breach happened on the customer's mobile device, Miliefsky says. The bank's app caused the problem because it allowed the eavesdropping, so "the risk and the responsibility is the bank's not the consumer's, he says. And, as in the case with retailers, banks could face fines for a breach.

"Businesses have become great at creating useful apps that their customers eventually feel they can't live without," Miliefsky says. "But the failure to secure that app is going to come back to haunt the business over the long haul."

Hacked!

Small businesses are a prime target for hackers and spam email campaigns. Here's how to better protect your inbox ... and your business.

By James Myers

Online threats are on a lot of peoples' minds, even small business owners.

Sure, the headlines are about the big companies, like Home Depot and Target, when they get hit, but small businesses often have less security than big corporations. This makes them a prime target for hackers.

So, it isn't surprising, or shouldn't be, that cybercriminals are increasingly preying on businesses through what is called a business email compromise, or BEC, because it has become a "highly lucrative threat vector for attackers," according to Cisco's 2017 Midyear Cybersecurity Report.

The report cites the Internet Crime Complaint Center, which says that between October 2013 and December 2016, \$5.3 billion was stolen through BEC. Furthermore, ransomware attacks took around \$1 billion in 2016 alone.

The report says there has been an overall increase in spam volume, which is defined as irrelevant or inappropriate messages, since mid-2016. However, these emails include "macro-laden malicious documents" that can work around some defense strategies.

Adam Jones is president and CEO of Firefly Technology, a Kansas City-based IT company that handles those duties for the National Auctioneers Association. He chimed in to offer some advice on how Auctioneers can protect their companies from online attacks.

Cybersecurity: Built-in SPAM filters aren't enough

First and foremost, Jones recommended that Auctioneers stop relying on built-in spam filtering with their hosted email products. He said companies of any size need to subscribe to a third-party spam service that sits between the internet and the mail host. Some examples include AppRiver, SecureTide, Barracuda and Mimecast.

While Jones holds that opinion, there are other options that don't require subscribing to a specific spam prevention service. One example is "G Suite" – originally launched by Google in 2006. The affordable suite provides email, video conferencing, online storage, and file sharing. A recent security update to the suite provided "features to block (ph)ishy activity, updated mobile device management controls and more."

Regardless which tool you choose, say a spam email does manage its way into your inbox. Let's explore several scenarios.

What about emails that ask the user to click on something?

"First check the actual email address that the email shows as coming from," Jones advised. "This sometimes requires clicking on the name at the top of the message, but it should reveal the full address."

Jones also said while there are spam emails that either masquerade or have come from the actual purported sender (e.g. in a hack scenario), many times, they simply masquerade the name. If the

email address does not match that which you would expect, it can (and should) be disregarded.

Also, if there is a link in an email, right click on it and copy the link. Then paste the link into a web browser, but before pressing enter, check out the link. For example, if someone said they're sending a link to a Google Apps file, make sure the address that you've copied and pasted says ".google.com." If the address is something different, it is an indication that the link is not safe because it will ask for personal information or download something that will infect your system.

"As a general rule," Jones said, "if you are not expecting something from someone with an attachment, attachments should be viewed skeptically. If you are suspicious of an attachment, having a relationship with a knowledgeable IT firm can come in handy as they can be used as a verification resource."

Jones said his company utilizes air-gapped computers that they can open attachments on, which tests for validity without putting their network of computers at risk.

1 in 131 emails contains a malware. - Symantec, Internet Security Threat Report April 2017

But what if the user has clicked on something in an email that they immediately realize could be bad news?

Jones said the first step is to shut down the computer. Then, immediately go to another computer and change the password to that email account.

"Then, engage IT support to ascertain the severity of what might have happened," Jones said. "They will determine if the computer is safe to continue using, or if it should be wiped, cleaned, etc."

Another precaution to take is to ensure that the mail server is set to reject emails that do not match someone's Sender Policy Framework, or SPF, record. Jones said this is a system that exists to tell email systems where legitimate email from the domain name should be coming from.

There is also the risk of becoming an unwitting spam sender. Nobody willingly does this, and there are ways to ensure it doesn't happen at your company.

Cybersecurity: Two-factor authentication

Jones recommends enabling two-factor authentication, or 2FA. Popular hosts like Google Suite and Office 365 support this. Basically, 2FA is a way to take steps beyond a password to gain access to your account. Once you enter your password, you get a verification message, which will come over via text to your phone or through an app on your mobile device.

"This is essential in today's climate," Jones said. To take it a step further, Jones recommends setting up DKIM (DomainKeys Identified Mail) verification. This is to prevent email spoofing and allows the receiver to verify that the email came from the right domain

"This is a more modern version of verification system and can be enacted with the help of your IT vendor and/or software vendors," he said.

Also, Jones said to be sure your organization has a proper SPF record set dictating the servers that might send email@yourdomain.com. An SPF record is a type of Domain Name Service (DNS),

which is an email validation system that identifies the mail servers that are permitted to send mail.

"Once set," Jones began, "recipient servers that are properly set to reject email based on what is defined in your SPF record would not receive emails that come from sources outside of those deemed legitimate senders for your domain."

Sending out mass emails can also be a problem. Jones said if you're sending out emails that don't require recipients to know to whom the email was addressed, use BCC (blind carbon copy).

"This can help prevent a scenario in which a recipient of a mass email gets hacked," he said, "and the hacker uses that information to send out spoofed emails to that group purporting to be the original sender."

Finally, Jones said many people list their email addresses in plain text on their website. This makes it easy for spammer to "identify the corporate hierarchy and then attempt to spoof users into actions of many types, such as wire transfers, login information, etc." Instead of using plain text, Jones said you can replace symbols with actual words, such as replacing @ with "AT", or users can also safely post their email address as an image.

While those options may be suitable for some, others who want more control or even higher security may choose to go a different route. For instance, instead of publishing an email address, some auction companies have opted for a contact form. This option involves developing a form so that the email address does not appear in a site's source code. Instead, the email address can be generated by JavaScript.

Also, depending on the platform your company uses for its site, there may be plugins or other similar tools (on WordPress, for example) that can help you develop a security-friendly form.

The bottom line is to find a solution that does not expose your company's contact information to spammers.

*Ransom attacks
took around \$1.6
billion in 2016 alone.*

Are you following data protection laws?

NAA members often hold buyer and seller data, but they aren't protecting it. That could mean huge problems.

By James Myers

Big data is a big deal, even for auction professionals. Business owners are capturing more data about their customers than ever, and they're making good use of it, but collecting that data comes with a lot of responsibility.

So, what are you doing to protect the data you have on your buyers and sellers? Furthermore, what are you doing to cover yourself should you become the victim of a cyber attack?

As cyber criminals become more evolved in their hacking methods, news of large corporations experiencing data breaches becomes more common. While the media focuses on breaches that occur at massive companies like Yahoo and Target, regardless of how large or small a company is, when a database is hacked, the company is liable for any personal information that gets into the wrong hands.

In most cases the company that was hacked is required by law to quickly notify any affected party that their information has been compromised. Failing to do this can result in big fines.

Larry Harb, a licensed Auctioneer and NAA member, is the founder and CEO of IT Risk Managers, Inc. He has spoken on the topic of risk management at NAA Conference & Show and also addresses the issue at state auctioneer association events. Harb estimates that up to 30 percent of auction

professionals, if they're being honest, would say they've lost personally identifiable information (PII) related to their buyers and sellers.

However, most are not aware that there are laws governing how to react to such a situation.

Smallbiztrends.com said that as of early 2017, 43 percent of cyberattacks targeted small businesses. Sixty percent of small companies go out of business within six months of a cyber-attack (U.S. National Cyber Security Alliance).

"This is the biggest exposure that Auctioneers don't realize they have," Harb said. "It could totally sink your company. They are oblivious to it because they've never thought about it or they haven't been educated on it."

It doesn't take a master hacker to get an auction professional in trouble – they can do it themselves by simply losing the data – on a laptop that is stolen out of a car or office, or mistakenly left behind and picked up by a stranger. For instance, Harb continues, an Auctioneer working at a fairground might register bidders and sellers on a laptop, perhaps by scanning driver's licenses. The auction company is now responsible for that information. Should that computer be stolen, the auction company would be in a sticky situation, particularly if they didn't encrypt the data.



Auctioneers need to protect themselves with database insurance, which provides them coverage against the loss of client, vendor and employee personal and private information.

"What are they doing to protect it?" Harb asked of the collected data. "Encryption is huge. If the Auctioneer encrypted all their data on their laptop or other electronic devices, they probably would not have to notify."

Many auction professionals use third parties to handle their credit card transactions.

For example, an Auctioneer doing an online auction would only know the last four digits of a buyer credit card account number. Should that third-party credit card transaction fall victim to a cyber criminal and that data get into the wrong hands, the law says the Auctioneer is the person who has the relationship with the buyer and is therefore responsible for notifying them that their personal information has been stolen.

"Most people don't pay attention to PCI DSS (Payment Card Industry Data Security Standard) compliance coverage," Harb

said, adding that this is also a big risk for Auctioneers. "Our policies cover fines and penalties for PCI compliance."

While every Auctioneer should do anything they can to protect their data, they should also be willing to protect themselves and transfer the risk via insurance.

Most Auctioneers have liability, or "slip and fall," insurance coverage, which protects them should someone be injured at auction or if auction items are stolen. However, most liability policies don't cover cyber issues.

Harb cites a landmark decision in a federal court in Arizona, which found that data is not tangible – it's virtual. Traditional insurance policies exclude virtual losses from being covered. The trigger in traditional insurance to cover clients is a physical act.

For instance, if a tree falls on your house, or a driver runs into the side of your car – your insur-

ance will kick in. In the virtual world, even though there can be financial losses resulting in the data being stolen, there is no physical trigger.

"Let's say you're an auction house and I acquire all the names of your buyers and sellers," Harb said. "At the end of the day, when I take that information, have you lost anything? According to the courts, the answer is no, but with this information, I can cause your company financial harm. Therefore, in order to cover your loss, you need a separate set of policies."

Harb said this is why Auctioneers need to protect themselves with database insurance, which provides them coverage against the loss of client, vendor and employee personal and private information.

"Every business that has a computer that's using the Internet has the exposure (to hacking)," Harb said.



LET **ISERIES** HELP YOU FIND YOUR NEXT **GREAT IDEA**



ABOUT **iSERIES**

As an auction professional, you know firsthand the importance of helping your client meet their goals. Now, it's your turn! With webinars and white papers covering general and industry-specific topics, iSeries is there to help you develop your business and hone your auction craft. Best of all - the program is free and convenient to all NAA members!

iSERIES ARCHIVES

From business planning and Facebook marketing to prospecting clients and doing appraisals, we've made the complete iSeries archives available on demand to NAA members.

www.auctioneers.org/iSeries



§ August 2, 2017

How to Get People to Pay for Your Services **BA**

§ October 4, 2017

Maximize Your Non-Sale Revenue **PCA**

§ November 1, 2017

Profiling & Targeting Customers, Part I (White Paper) **MM**

§ December 6, 2017

Your Online Auctions Are Terrible **MM**

§ February 7, 2018

Profiling & Targeting Customers, Part II **MM**

§ March 14, 2018

Building Your Commercial Real Estate Business **RE**

§ April 4, 2018

Personal & Cyber Security (White Paper) **MM**

§ June 6, 2018

How to Get Hired **CO**

support@auctioneers.org