PHISHING, SMISHING, VISHING AND NOW QUISHING?

The Cyber Actor's Next Attack Vector

Written By: *Mark D. Solomon, CCCI*
International President, IAFCI
Date of Publish: *12/11/2023*

International Association of Financial Crimes Investigators

In September of 2023, Detective Alec Campbell of the Charlotte Mecklenburg Police Department and Financial Crimes Unit began receiving complaints about fraudsters placing foreign objects on parking meters. I immediately began to think fraudsters were placing skimming devices on the meters as we have seen in the past. However, this "Device" was much more primitive, but equally effective. The device had no electronics, battery source, and was installed in seconds. The device he explained was a "QR code" sticker. I hate to give criminals any credit, but both the simplicity and effectiveness needs to be recognized. We will discuss in more detail going forward.

Thanks to fraudsters over the past 20+ years, The Webster Dictionary has had to be updated to include special definitions to explain various frauds and cyber related crimes.

The terms "Phishing," "Smishing," and "Vishing" have become familiar words when describing the tactics of fraudsters that try and lure you into giving away your PII, account information, or install malicious malware onto your electronic devices. Well, it is time to add another definition and attack vector to the definitions of fraud;" *Quishing.*" I know it is not an officially approved word because spellcheck does not recognize it multiple times in this article. Mr. Webster and Microsoft, can you please update, I already have enough typos to deal with!

The use of QR codes, or Quick Response Codes, started in 1994. Everyone has at least seen and/or used a QR code to get to an Internet site without having to google or type in a URL address. Just fixate your cellular phone's camera on the QR code, the link appears, click it, and off you go to the intended website. But are you truly at your destination? Cellphone users beware!

They are in convenience stores, restaurants, retail businesses, posted on bulletin boards, placed on business cards, websites, ATMs, and even gas pumps. Pull up to your drive-thru window and you see a sloppily placed QR sticker for a business or a job opportunity. QR codes were created to make it easier for customers to access a website. Its unintended consequence has also made it easier for fraudsters to target victims and obtain account information, PII info, or install malicious viruses, malware, or ransomware onto your cellular devices.

But before we look at this new attack vector, let us review the evolution of this fraud by starting with Phishing, Smishing and Vishing.

PHISHING ATTACKS

Fraudsters send unsuspecting victims an email and request that you provide your personal identifying information (Name, DOB, SSN) or account information, usernames, passwords, and provide your answers to security questions or the one-time passcode (OTP) you just received. The actors may pose as a representative of your financial or retail institutions, someone you do business with or even a family member. They may request information because there is a problem with your account, or they need to update your information, you won a free vacation, or the "International lottery." Your winnings will be delivered shortly, right after you pay taxes, custom fees, or a processing fee up front. Or your account will be restored once you verify your information and account info and password or PIN. The various phishing scams are endless, but the goal is all the same. To give away your financial DNA, steal your money, or infect your electronic devices with malware and viruses.

Emails were first introduced to society in 1977. Yet, the term "Phishing" was not officially used until a decade later.[1]

Often, fraudsters will use phishing emails to redirect you to a website where you provide PII, account information, or have you click on a link or attachment that can hack your electronic devices. The ability to spoof both emails and websites (create a similarly looking email or URL link) is not a complicated or time-consuming task for fraudsters. Just change a letter, number or symbol of the email or URL and you have set your "Phishing" hook in the water to catch yourself a victim. You just need them to take a bite of the bait. Making a fake website look like the real one is easy. Just search for the logo for the real business and download it, or take a screenshot of the businesses' Internet page, with a little cropping, you got your fictitious site to look just like the real one.

And if the actors are very savvy, they may also be able to hijack your legitimate email or website and it is now completely in the hands of the criminal.

Statistics do not lie. Phishing is a very prevalent and effective tool to steal your information and disrupt and infect your computers.

According to a report from the FBI's Internet Crime Complaint Center (IC3), it received 800,944 reports of phishing, with losses exceeding $10.3 billion in 2022.[2]

In 2022, Trend Micro™ Cloud App Security discovered 40 million high-risk email threats, in addition to those detected by built-in Microsoft 365 and Google Workspace security.[3]

---

[1] https://www.mail.com/blog/posts/fiftieth-anniversary-of-email/20/#:~:text=The%20first%20email%20was%20sent,is%20also%20credited%20to%20Tomlinson

[2] https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

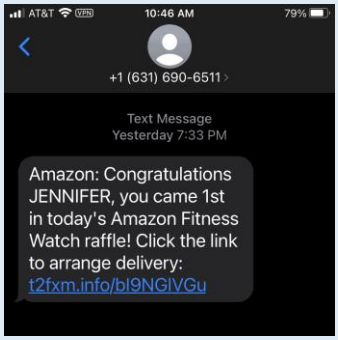
[3] https://www.trendmicro.com/en_vn/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html

What I like to call "Phishing 2.0" took Phishing to a whole new level. It went from just stealing PII or account information, to something more dangerous to the user or to a business. Insert a malicious code into the equation, such as malware or a virus, and now you can infect that computer and others on the network. Click on a link or download an attachment, and now the malicious actors can do more damage from network intrusions, denial or disruption of services (DDOS), or even turn your electronic device from a working computer into a paperweight by installing ransomware on your computer or business' network. And good luck trying to decrypt the ransomware malware. Unless you have the decryption key, your computer is a useless piece of metal that you might as well drop it off at your local transfer station.

Again, the statistics do not lie:

- Phishing scams account for 36% of all data breaches, according to Verizon's 2022 Data Breach Report.[4]
- Trend-Micro detected and blocked 4.3 million malicious files in 2022. This represents a 29% rise when compared to 2021. The number of unknown malware threats also spiked to 3.8 million, indicating a substantial 46% surge. Nevertheless, it is important to mention that the number of known malware files to 505,838, representing a 32% decline.[5]
- According to a report by security company Egress, 92% of organizations have fallen victim to phishing attacks in 2022. This accounts for the 29% increase in phishing incidents from 2021, where we detected and blocked a total of over 21 million attacks.[6]
-

SMISHING ATTACKS



Well, it took some time, but 15 years later and in 1992, the first text message was sent from one phone to another. And the fraudsters were ready to quickly adapt to the latest technology as well. Known as SMS texting (Short Message Service), this way of communication, without having to place a call or sending an email, quickly became a popular feature for cellular phone users to immediately communicate with another person or business without sending an email or dialing a phone number. The fraudsters saw this modern technology as another tool to entice victims into giving their personal identifying information and financial DNA. So instead of sending you an email, targeted victims receive a similar request for information via text. [7]

Additionally, smishing made it easier for fraudsters to send out mass text messages and set thousands of "Smishing hooks" within seconds. Instead of having to make individual calls to potential victims, SMS texting allows hundreds and thousands of SMS messages to go out within seconds. Blast out 10K text

---

[4]https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwjC25Khy8iCAxWJjcgKHSWADu8YABAAGgJxdQ&ase=2&gclid=EAIaIQobChMIwtuSocvIggMViY3ICh0lgA7vEAAYASAAEgIQB_D_BwE&ohost=www.google.com&cid=CAASJuRoKGRHsKjtFr2BvvnqQTJQMr-oxvvagKh3XS2kTaHymeHC6Nkp&sig=AOD64_2xySBnVdYx9Nm-40kfueuwLZBkBw&q&nis=4&adurl&ved=2ahUKEwicroqhy8iCAxWoMlkFHeqeDpEQ0Qx6BAgLEAE

[5] https://www.trendmicro.com/en_vn/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html

[6] https://www.computerweekly.com/news/365532100/Nine-in-10-enterprises-fell-victim-to-successful-phishing-in2022#:~:text=Email%20security%20company%20Egress%20finds,email%20gateway%20(SEG)%20technologies.

[7] - https://www.vodafone.com/news/technology/25-anniversary-text-message#:~:text=Neil%20had%20been%20working%20as,message%20on%203%20December%201992.

message in second and see how many "smishes" are in the pond that are willing to take a bite. So, what if I only get 100 to respond, go to a link, provide PII or click on an attachment or link that will infect your cellular phone. That is a surprisingly good haul for a smishing actor.

Today, cellular phones and texting allow users to have the ability to communicate instantly, conduct transactions, download information and yes, give away your PII, account info and infect and destroy your cellular phones. Just take a walk through Grand Central Station and see how many are on their phones, just texting away. Smishing, just like Phishing, is designed to steal info, trick you into financial transactions and infect your cellular phones.

VISHING ATTACKS

Vishing is the use of phone calls and voice messages, using the technique of "social engineering" to lure you into giving your PII, sensitive information, (bank information, passwords) and other info they may need to access your accounts or open new ones with your information. With modern technology of "spoofing" (fraudsters use applications to have your true phone number show up on the caller ID screen) can trick financial and retail institutions, co-workers and friends to believe you are making the call. SIM Swapping (actors disable your phone and have the SIM card to your existing phone cloned and placed into another phone), can also be used to make your banks, co-workers and friends believe it is a call from you.

Voiceover apps can be used to change the fraudster's voice into any voice you believe the victim would want to hear to convince you into fall victim to the scheme. Voice cloning is also another up-and-coming tactic where technology can convert the voice of another into a facsimile AI generated voice that sounds almost identical to yourself, a family member, friend, co-worker, celebrity, or even a politician. The FTC addressed this issue in May of 2023 when Sen. Mike Braun, R-Ind., the top Republican on the Senate Special Committee on Aging, spearheaded a bipartisan letter to the Federal Trade Commission (FTC) about AI-drive scams against the elderly. The letter was unanimously signed by every member of the committee and they are making inquiries as to how AI-powered technology can be used to replicate people's voices.[8]

Just like Phishing and Smishing, Vishing can be a dangerous attack method for the cyber actor and the consequences of Vishing attacks are truly scary.

- Vishing attacks are resurgent and shockingly on the rise by 550% in 2022.[9]

- According to the True Caller Insights 2022 US Spam & Scam Report, 68.4 million US citizens lost money to phone scams. This figure indicates a 23% increase in American losses to phone fraud in 2021 (59.4 million), 26% of Americans (about 56 million) reported falling victim to phone scams in 2020.[10]

[8] https://www.foxnews.com/politics/ai-voice-clone-scams-hitting-elderly-americans-senators-warn
[9] https://techreport.com/statistics/vishing-statistics/#:~:text=FAQs-,Key%20Vishing%20Statistics,the%20highest%20awareness%20of%20vishing.
[10] https://techreport.com/statistics/vishing-statistics/

- 1 out of 3 Americans have fallen victim to a scam at least once (33% of America's population).[11]

- Approximately $39.5 Billion in 2022 and $29.8 Billion in 2021 were lost to Vishing in the United States of America.[12]

WELCOME TO THE NEW WORLD OF QUISHING

I would love to say I was aware of this new attack vector, but it shows the importance of education, networking and intelligence sharing, which are the core goals of the mission statement for the International Association of Financial Crimes Investigators (IAFCI). Thanks to Detective Campbell, we can all benefit from the information he shared with the IAFCI.

As the complaints began to come in about counterfeit QR Codes being placed on parking meters, Det. Campbell seized one of the stickers and learned that counterfeit QR codes were created and placed on both parking meters and kiosks in 2 different States. The customers were being redirected to a payment processing site that the actors created and controlled and were able to get victims to turn over their full card number, expiration date and security code (CVV) of their debit/credit card.

Once learning about this new attack vector, and as a seasoned investigator, I immediately accessed a "top-secret" intelligence sharing website to validate the authenticity of this type of attack. After "Googling Quishing," I realized that this attack vector is gaining the interest of fraudsters in the United States and globally. Yet little is published about how to identify and prevent being scammed. More importantly, there was even less as to how to investigate Quishing. So, let us start with the basics and then get more into the weeds.

QUISHING DEFINED

According to techtarget.com, Quishing, also known as QR code phishing, involves tricking someone into scanning a QR code using a mobile phone. The QR code then takes the user to a fraudulent website that might download malware or ask for sensitive information.[13]

Research revealed the notion of Quishing was first discussed in 2021 when tech experts began talking about this attack vector. In 2021, tech experts began sounding an alarm about the potential of Quishing attacks.

Shortly thereafter, an article appeared in the Washington Post discussing the dangers of QR codes and whether they were tracking people or collecting data. However, the article also brought out the important

---

[11] https://techreport.com/statistics/vishing-statistics/
[12] https://techreport.com/statistics/vishing-statistics/
[13] - https://www.techtarget.com/searchsecurity/feature/Quishing-on-the-rise-How-to-prevent-QR-code-phishing#:~:text=Quishing%2C%20also%20known%20as%20QR,or%20ask%20for%20sensitive%20information

fact that, like Phishing, fraudsters can use QR codes to trick consumers into providing their PII or account information.[14]

From 2021 until mid-2023, the threat of Quishing has gone unnoticed. I could only locate a handful of articles discussing Quishing and extraordinarily little dedicated to educating the public or financial crimes investigators on how to investigate.

QUISHING; METHODS OF DEPLOYMENT

In July 2023, Microsoft authored an article about the threat of "Quishing" and provided some various tactics in which Quishing attacks can be used as well as valuable tips on how to avoid becoming a victim of Quishing. First, let us look at the deployment methods being used by these actors.

1. Phishing & Pop-up Scams with QR Code Redirection:

In combination with a Phishing scam or Pop-up scam, the victim is enticed to access the QR code, not knowing it is bringing you to the criminal's site or is capturing your account information. The intro of a Phishing scheme containing a QR code may make the victim believe that this is not a scam when it is.

2. QR Code Payment Scams

Scammers can place malicious QR codes in public places, gas pumps, parking meters, ATM machines, or at restaurants to pay with your phone. Create a QR code sticker and place it over an existing one and you can steal a considerable amount of account or PII information. Create a fictitious website and ask for PII info or your credit card number, expiration date and security code and you have got all you need to hit the jackpot. Open a merchant account and link it with the fictitious website and QR code and you can save a step or two to get the victim's money into your possession.

3. QR Code Package Scams

Bad actors can slap a sticker on unsolicited packages, mailings, or slip them inside the envelope or package. Make the reason to point your cellular phone at that QR code, such as a big discount, additional free offer, or confirm that you received the package and the fraudsters have successfully lured you into the "Quish".

4. QR Code Cryptocurrency & Investment Scams

QR codes can be used to entice crypto currency buyers as well as those looking to invest their hard-earned savings. It might be an offer to receive additional free crypto currency or be purchased at a discounted price. The problem with falling for a crypto-currency QR code scheme is the fact that the transaction is what we call a "Push" transaction. Once you send that currency, there is little recourse to get it back and no one will be refunding you the currency event though it was a fraudulent transaction. You pushed it and it is not coming back.

[14] https://www.washingtonpost.com/technology/2021/10/07/are-qr-codes-safe/

QR codes can also be used to lure victims in the beginning or final stages of an investment scheme. Received the investment pitch that is too good to be true? If you are in on this guaranteed investment, you will just need scan the QR code we sent you and provide your account information.

5. QR Code Donation Scams

Actors can post and display a QR code that is linked to a worthy cause or charity. The fraudster is praying upon the victim's kindness to help others. These types of donation scams historically started with a knock on the door, or an email. Today, they have metastasized to an 8.5 x11 piece of paper posted in a public area that contains a QR code bringing you to that fictitious website for you to send your charitable funds to a fraudster.[15]

6. Malicious Injection to Your Cellular Device

If the first 5 attack options have not scared you enough, cyber attackers can use QR codes to inject malicious malware, ransomware and other information directly into your cellular device. Scan that QR code and click on the URL and it can land you onto a page in which it automatically installs malware onto your phone (AKA Drive-by Downloads). You do not even have to click anything once you arrive at the malicious website.[16]

Kaspersky also warns QR code users that actors can also add contacts to your phone and compose emails from your own email address. By doing so, the cyber actor has many options to reach out to your contacts and perpetrate further fraud.[17]

THE LURE OF QUISHING FOR THE CYBER ACTOR

So why would QR attacks be appealing to cyber actors? There are several reasons that we will examine in this article.

MINIMAL EFFORT TO CREATE MALICIOUS QR CODES & REDIRECTION TO FRAUDULENT WEBSITES

QR codes are so easy to create on the Internet. First, if the actor is looking to obtain victims' PII or account information, they will have to create a website that appears to be a legitimate website. There are endless sites that can be used to create a legitimate looking website. And if you are smart, you can pay for the opening of the fraudulent website with a victim's credit, debit, or account information.

If fraudsters do not wish to create a new fraudulent E-commerce site, there are other options. Create a spoofed website (website created to look like the true website of a bona fide business). Just change one letter of the URL, steal some of the logos from the bona fide business and you have your landing page for your victim. In that spoofed website, the actor may solicit you for your PII

[15] https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/five-common-qr-code-scams).
[16] https://usa.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan
[17] https://usa.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan

info, account info or simply ask you to click on a link that installs malicious malware onto your cellular phone.

The creation of a QR code can be done on multiple websites and there is no oversite as to what is being embedded into the QR code. Within 60 seconds, you can have a professionally looking malicious QR code and even put in your own business logo or that of a legitimate business to lend credibility of the QR code. Just type in "Create QR Code" into your search engine and you have multiple free options to create your code in just minutes. You can personalize the QR code, from design, color, and size.

Easy Deployment & Lack of Deployment Detection

Once you have your website and QR code, the fraudster needs to deploy the QR code to the public. Well, as stated before, QR codes can be seen everywhere you go:

- Bulletin boards at work, schools, and grocery stores
- Restaurants that put QR codes on menus or tabletop holders, or menus
- Parking meters, soda machines, ticket machines, transportation hubs
- Phishing & Smishing emails and text messages with a QR code attached.
- Drive thru lanes at fast food or financial institutions
- Gas pumps, and ATMs
- Storefront windows
- Pop up advertisements

If the fraudster is into ATM, POS, and Gas Pump Skimming, it usually takes place where there are cameras that are capturing you from different angles. The reward may be large, but sometimes, so are the risks. QR code actors can go into a diner and put a sticker over the original QR code. Or, put a sticker on the drive-up window when the employee has their back turned. Parking meters, bulletin boards or any public space can be utilized to install your low-tech device. The lifespan of your device is not limited to recording space, powering of the device, or space to store data. And how long will it take for victims or law enforcement to make the connection between your stolen PII or account information and that QR sticker you honed your cellular phone upon? Probably a long time!

And if you scan the QR code and provide your information, and it does not pay your bill at the restaurant or parking meter. How many will realize that you have just been a victim of Quishing?

Customers and employees will just suspect that the QR code failed or malfunctioned.

AVOIDING QUISHING & TIPS FOR THE PUBLIC AND BUSINESSES

As always, the International Association of Financial Crimes Investigators (IAFCI) has the dual mission of educating our 7,000+ investigators around the globe on the latest crime trends and tactics being used by the criminal element. The IAFCI is also committed to educating the public, our financial institutions and retail businesses. First, let us look at some vital information to protect the consumer and our financial and retail industry.[18]

1. Awareness & Education: Knowing about the types of frauds that affect consumers, financial, and retail institutions is critical. The more we know, the less likely the fraudster will be able to successfully target you. Understand that there are many legitimate reasons and benefits of using QR codes. But, like any technology, it is neither good nor evil. It just depends upon whose hands it is in.
2. Inspect & Research Before You Point: QR codes have been created to get you to your destination quickly. But a well-informed consumer should not rush into scanning a QR code. Is another QR code underneath the visible QR code? Is the advertisement or posting with the QR code grammatically correct and it is in a place you would expect the QR advertisement to be? Would the location of the QR code be easily accessible to the criminal actor to post? QR codes are meant to shorten your time to get to a legitimate website. But if you are unsure, wouldn't it be better to google the company or charity and go to the known website instead? Remember, the quickest way to a destination may not always be the safest way.
3. Point But Do Not Redirect: Well, if you have followed the last step and there are no obvious red flags, you may wish to proceed to the next step over pointing your cellular phone at the QR code. Once you focus in on the QR code, it should bring up a URL link within the camera of your phone. Point #3 is "Not to rush to click". Take a deep breath and inspect the URL link. If it is a legitimate business or retailer or financial institution, the URL should look authentic to the true businesses' URL. Look for misspellings, changes of single letters, numbers, or characters. Remember, spoofing of a website and/or email can be done with just one change to the true URL.
4. Houston...We have landed...But Do not Step Foot Yet: If you have navigated your way to the website, again, do not rush into providing information or clicking on any links or buttons. Legitimate E-businesses, retailers, charities, and financial institutions will spend considerable time with professional marketing, graphic design and most importantly, security. If the quality of the site looks poor, it very well may be a spoofed or fraudulent website. Fraudsters are looking to spend as little as possible to create a site and know that time is ticking until the gig is up for that site. Thus, the fraudster will usually cut corners to minimize their time and resources to focus on the fraud. Additionally, look for that secure network logo at the bottom of the screen to make sure it is showing as a secure website. Additionally, make sure the URL starts with "https:" That last letter indicates that it is a secure website. It does not mean it is a not a fraudulent website or the site has not been hacked, but the risk is reduced.

[18] https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/five-common-qr-code-scams

5. Unsolicited QR Codes Beware: Just like any unsolicited phone call, email, text and now QR codes, we do not know the identity or intent of the sender. I have spent decades educating the public that you should not provide any personal identifying information or account information from any incoming email, phone call or text. Do not reply, hang up, or do not text back or click on any links. Same goes for QR codes that are received by you without request. The ultimate choice to scan a QR code rests with you. But the safest way to ensure who you are connecting with a business, financial institution or retailer is for you to make the first contact. If you receive a QR code from a company, retailer, or financial institution that you have a relationship with, you can also contact them on their known phone number or legitimate website. Never take the word of an incoming QR code when it comes to its authenticity. The average time between scanning a QR code and landing on a malicious site can take just seconds. Typing in the legitimate business, retailer or financial institution into a search engine may take another 30 seconds, but isn't that worth the wait? I'll leave that up to you to decide.
6. Too Good to Be True: Just like any sales pitch, offer or opportunity, if it sounds too good to be true, then it probably is not true! Same goes with QR codes. Unreasonable discounts, significant investment opportunities, and crypto currency deals should be sending off red flag signals to you. Again, the fraudster will pray upon good fortune and will rush you into making a decision. Again, the transfer of PII info or account information should always be done through a trusted and most secure method as possible.
7. If It Does Not Work...Tell Someone: If you use a QR code and you get a message that there is an error or the site is down after you provide your account or PII info, tell someone right away. If you are in a restaurant, tell the manager and educate him about Quishing. If a QR code on a Parking meter does not work, call the town or local police department. The sooner these fraudulent QR codes are detected, the quicker law enforcement and businesses can react.
8. Disable Automatic Scam: Some scanners on your cellular device can automatically scan QR codes. Make sure you disable that function on your phone to prevent your device from scanning malicious QR codes.
9. Download a QR Code Reader That Has Malware Detection: Remember, a cellphone is not just a cellphone anymore. It is a fully functioning computer that allows you to make calls. And we know that computers, no matter how secure, can be compromised. Thus, always use a reputable QR code scanner to read QR codes.
10. Is It Worth the Time: QR codes are an incredible luxury and speeds up the cellular phone user's time to get to a destination. But how much time are we truly losing and at what risk? When it comes to many different types of frauds and scams, fraudsters like to put the victim under duress (good or bad fortune) and usually want you to act quickly (limited time). In any technology, we are all drawn to instant access. The quicker and faster we get somewhere we believe it will save us valuable time and energy. But at what expense? Criminal cyber actors are counting on our desire for instant access and instant satisfaction. In this case, it may be safer to take the route of the tortoise rather than the hare. I am neither for, nor against QR codes. I am not telling you that every QR code that you come across contains malicious links, malware, or will lead you to a nefarious website. But using a more secure way to get to a website worth the time? Especially when you are providing sensitive account information or your PII? I will leave that answer for you to decide. I prefer the slow and steady wins the race.

IF YOU THINK YOU ARE A VICTIM OF QUISHING

If you suspect that you have been a victim of a Quishing scam, time is of the essence! Here are some quick reaction steps you can take to avoid further damage:

1. If you provided your account information, contact that financial/retail institution immediately and have the account closed. If you provided any passwords to security questions to the accounts, change them.
2. If you provided your PII information, file an identity theft report with your local police department as well as with the Federal Trade Commission (https://reportfraud.ftc.gov/#/). Provide the suspected location of the QR code that you scanned as well as the URL link from your history browser, but do not go onto the site to view it again.
3. Notify the credit bureaus and file an identity theft report and request a "Credit Freeze." This will prevent anyone from opening a new account with your PII information. However, you are going to still need to monitor your existing accounts for fraud. Depending on the PII information you provided, the fraudster may be able to access multiple accounts that are associated with you.
4. If you suspect that you downloaded malware onto your Android device, you have two options.
    a. Download a reputable malware scanning software onto your phone and conduct a full scan.
    b. Users can also use Google Play Protect to scan your apps for malware.
    c. For more information on who to scan for malware on Android phones, here is a great article: https://www.androidauthority.com/scan-android-viruses-3208378/
5. For iPhone users, and despite what you may have heard, there are no downloadable apps that will detect malware on your phone. Due to security restrictions on iOS, it is not possible for any app to scan the system or other apps for malware. Apple does not allow these applications. Malwarebytes for IOS Version 1, cannot scan your iPhone for malware. However, it can help protect your phone and help identify malicious websites, identify scam phone calls, and text messages. The download can also block advertisements on your iPhone. For more information, click on Malwarebytes article:
    - https://support.malwarebytes.com/hc/en-us/articles/360039022853-Scanning-for-malware-on-iOS-devices-v1
6. If you used your cellphone after a download of malware, you would need to change your password. However, you will want to run a scan for malware first on your Android phone. Once this is done, it is recommended that you change any passwords that you might have used to access any of your accounts. It is also recommended that you change the passcode to your phone as well. However, make sure the malware scan has been done first. If you are an iPhone user, it is still recommended that you change any passwords to sites that you logged into after accessing the QR code.
7. Ensure that you have multifactor authentication on your cell phone and any accounts you have accessed.

For more information, go to the following Microsoft article:

https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/five-common-qr-code-scams

This article has covered what Quishing is, how to identify and prevent a possible Quishing attack, and what you should do if you suspect you scanned a malicious QR code. The IAFCI is committed to protecting our global citizens as well as our retail, financial institutions and other industry partners.

**The IAFCI would like to personally thank Detective Alec Campbell of the Charlotte-Mecklenburg Police Department for bringing awareness to this crime!

ABOUT THE AUTHOR:

Mark Solomon, CCCI is the International President of *the International Association of Financial Crimes Investigators (IAFCI)*. Mark spent 26 years in law enforcement and most of his tenure as a fraud, financial and cybercrime investigator. Currently, Mark is a Vice President for a Financial Institution in the U.S. and works with a dedicated team to combat fraud by protecting its customers and clients and working with other public and private sector investigators. He is a Certified Cyber Crimes Investigator (CCCI) with the IAFCI.

He is also the co-host of the *"IAFCI Presents...The Protectors Podcast"* along with IAFCI International Chairman, Michael Carroll. He has spoken throughout the U.S. and Internationally on how to not only prevent and detect financially related crimes, but also helps educate those who are tasked with investigating and prosecuting these crimes that impact our citizens. He has received numerous awards during his time in law enforcement and private sector career and is passionate about the IAFCI and its mission. Mark joined the IAFCI in 2008 and has held various leadership positions within the organization before coming International President of the IAFCI.