HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-11

PUBLIC WARNED AGAINST ‘QUISHING,’ THE LATEST CRIMINAL ACTIVITY ONLINE

1. Background

Quick Response (QR) Codes can be seen almost everywhere, physically and virtually, for a multitude of uses. The use of QR codes has been proven useful since the start of the COVID-19 pandemic. As the government requires businesses and services to shift to electronic payment and online processing due to health-related restrictions. However, scammers now use QR codes to launch cyber-attacks amid an increasing use for online payment transactions and many other purposes. By linking to a scam website via QR codes, they can bypass traditional defenses such as secure email gateways (SEGs) that scan for malicious links and attachments. This kind of cyber-attack refers to QR Phishing or “Quishing” wherein attackers utilize the QR codes for malicious purposes, such as intercepting personal information through links embedded in the QR Code.

2. What are QR Codes?

A QR code is a type of barcode that can be read easily by a digital device and which stores information as a series of pixels in a square-shaped grid. QR codes are frequently used to track information about products in a supply chain and, because many smartphones have built-in QR readers, they are frequently used in marketing and advertising campaigns. More recently, they have played a key role in helping to trace coronavirus exposure and slow the spread of the virus.

The development team behind the QR code wanted to make the code easy to scan so that operatives did not waste time getting it at the right angle. They also wanted it to have a distinctive design to make it easy to identify. This led them to choose the iconic square shape that is still used today.

QR codes are used in numerous contexts such as:

a. QR Codes in Sales and Marketing

Many advertisers use QR codes in their campaigns because it provides a faster and more intuitive way to direct people to websites than by entering URLs manually.

They can also be used to link directly to product pages online. For instance, if you were searching for the exact dress a model was wearing in a poster, a QR code could directly take you to the web page where you could purchase it.

b. QR Codes for Coronavirus Tracing

The coronavirus pandemic has supercharged the use of QR codes. For example, visitors to hospitality venues such as bars and restaurants are invited to scan a QR code upon arrival using a COVID-19 tracing app. This is to help trace and stop the spread of the virus. If someone tests positive for COVID-19 at that venue, other visitors to the location are alerted by an app, thanks to the data accumulated from QR code scans.

c. QR Codes on Product Packaging

You may also find QR codes on the packaging for some of your favorite products. These QR codes can reveal information about the product, such as nutritional information or special offers you can use next time you make a purchase.

d. QR Codes in Industry

QR codes were initially invented to help track parts in vehicle manufacturing, and they are still used throughout the manufacturing industry. You'll also find QR codes used by other businesses that need to keep a close eye on products and supplies, such as the construction, engineering, and retail industries.

e. QR Codes in Logistics

Logistics services around the world also use them. Because they can contain a large amount of information, they are often relied upon to track parcels. For example, major online stores have moved entirely to QR codes for tracking their shipments.

f. QR Codes in Education

QR codes are also used in schools and colleges to help engage students. They have appeared everywhere, from the classroom to the library, for tasks such as helping students find the books they are searching for.

3. Are QR Codes Safe?

Attackers can embed malicious URLs containing custom malware into a QR code, which could then exfiltrate data from a mobile device when scanned. It is also possible to embed a malicious URL into a QR code that directs to a phishing site, where unsuspecting users could disclose personal or financial information.

Because humans cannot read QR codes, it is easy for attackers to alter a QR code to point to an alternative resource without being detected. While many people are aware that QR codes can open a URL, they may be less aware of the other actions that QR codes can initiate on a user's device. Aside from opening a website, these actions can include adding contacts or composing emails. This element of surprise can make QR code security threats especially problematic.

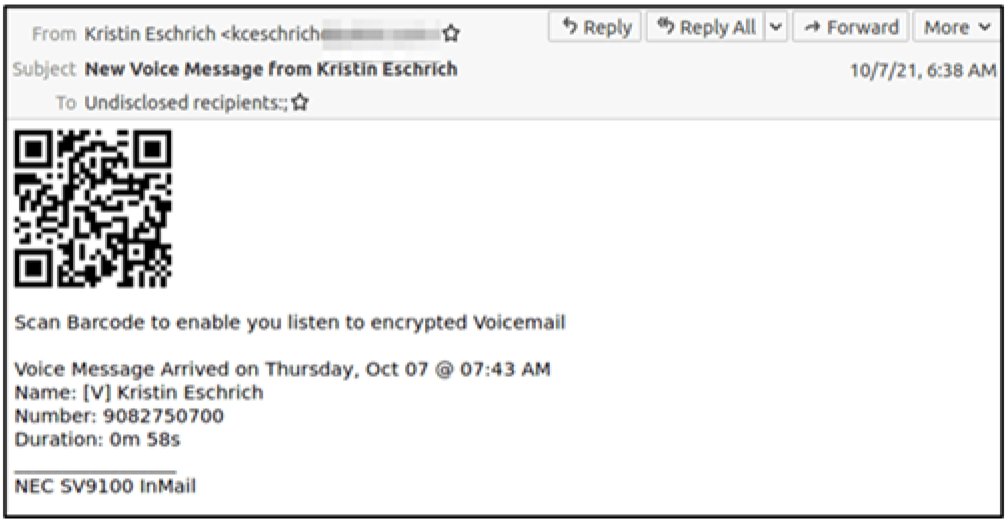
A typical attack involves placing malicious QR codes in public, sometimes covering up legitimate QR codes. Unsuspecting users who scan the code are taken to a malicious web page which could host an exploit kit, leading to device compromise or a spoofed login page to steal user credentials. Some websites do drive-by downloads, so simply visiting the site can initiate a malicious software download.

Mobile devices, in general, tend to be less secure than computers or laptops. Since QR codes are used on mobile devices, this increases the potential risks.

4. How Does Quishing Work?

Quishing scams first need the QR code itself to be delivered to the victims (usually via email). A common tactic is to invite people to access a message, which may indicate that they won a certain prize from a certain raffle, via a QR code. The victim then uses their camera to access the QR code and opens up their browser, which takes them to a phishing website.

At this point, a site pop-up might ask the victim for their login credentials that can be harvested and used to launch further attacks. New Scam QR codes can be made quickly, meaning it's unlikely they'll be reused, recognized and caught by a SEG's blocklist. They're zero-day attacks that need intelligent email security in order to be detected and caught.



From Kristin Eschrich <kceschrich[redacted]

Subject **New Voice Message from Kristin Eschrich**

To Undisclosed recipients:;

10/7/21, 6:38 AM

Scan Barcode to enable you listen to encrypted Voicemail

Voice Message Arrived on Thursday, Oct 07 @ 07:43 AM
Name: [V] Kristin Eschrich
Number: 9082750700
Duration: 0m 58s

NEC SV9100 InMail

5. Social Engineering Signs to Watch Out For:

While the method of attack differs, there are certain things to watch out for when it comes to **Phishing, Smishing, Vishing, and Quishing**. These scams can be sophisticated, so vigilance is required to detect the most advanced threats:

a. Urgency

A scammer usually wants something done immediately, as the longer you have to think, the more you may question whether it's a legitimate request. They want you to take action fast, whether that's following a link, downloading something, or sharing personal information.

b. Plausibility

Modern attacks will often be based on real-life mundane scenarios. If the scam request is close to something an employee does every day, they're more likely to miss the signs of phishing and do it in autopilot. They might also try to align with current events. For example, lots of scams have arisen in relation to Covid-19 and vaccinations.

c. Familiarity

There's been a marked rise in impersonation scams, where the attack is at least partially tailored to an individual – often claiming to be from an authority figure, such as a CEO, or a trusted source like your bank or a government department.

d. Confidentiality

The action required is specific to you and needs to be done by you alone, as getting someone else involved increases the chances of the scam being spotted.

6. Recommendations

There’s no telling where and when you might come across a malicious QR code. That’s why it is essential to use a QR Scanner you know you can trust and not download a random one from the app store or online.

Furthermore, to protect against Quishing, all personnel must be reminded of the following:

a. Users must only scan QR codes that come from a trusted or known source.

b. Before clicking a link that appeared upon scanning the QR code, check the destination first. If it seems dubious, it is best not to continue.

c. Watch out for advertising materials that have been tampered with.

d. Be careful about redirected web pages that will require your log-in credentials. Ensure that these web pages are legitimate.

e. Be mindful against people that are asking users for their PIN (personal identification number), security code or OTPs (one-time passwords).

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization’s overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://inqm.news/xxoc*
- *https://mb.com.ph/2022/07/29/quishing-is-latest-cyber-fraud-pldt/*
- *https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan*