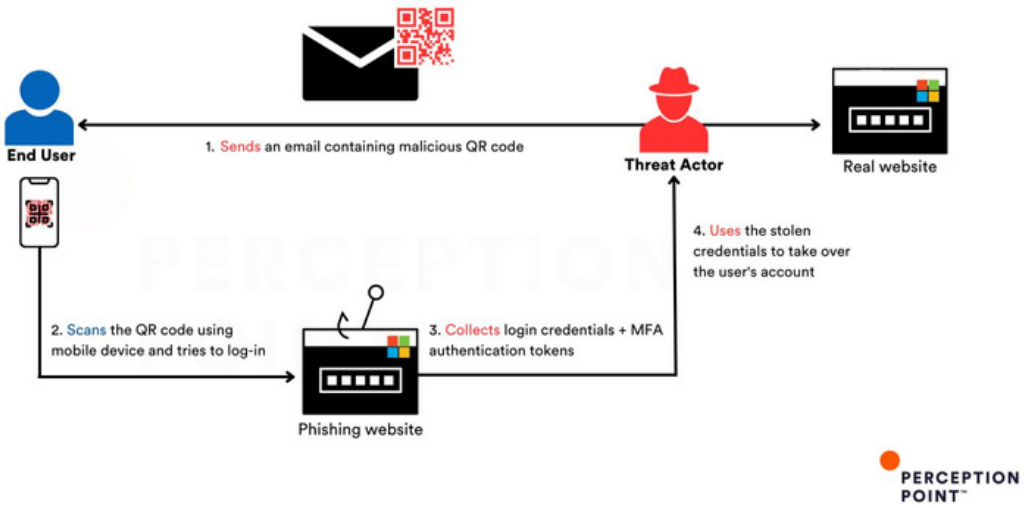
QR Code Red: Quishing Attacks and How to Prevent Them

Learn how cybercriminals exploit QR codes to deliver advanced phishing, or “quishing,” attacks and how Perception Point is stopping them.

Scan at Your Own Risk: QR Code as a Threat

QR codes that re-emerged into our lives during the COVID-19 pandemic have given rise to a new wave of advanced phishing attacks targeting thousands of organizations worldwide. These evasive threats also known as quishing (QR phishing), lure end users into scanning a QR code sent to them via email using their mobile device camera, redirecting them to malicious websites aiming to steal their login credentials, harvest financial information, or infect their devices with malware.



Quishing Kill Chain – What QR code phishing attacks look like

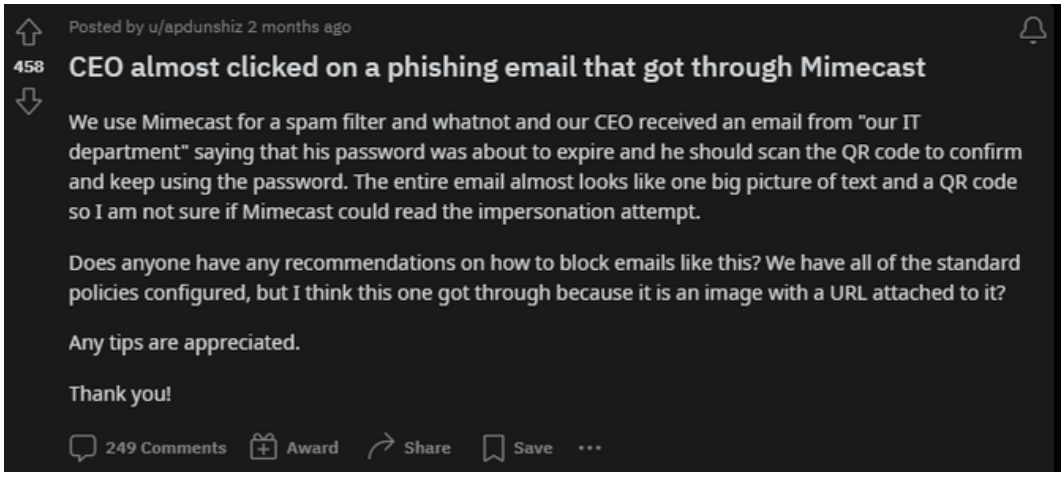
© 2023 Perception Point

The Quishing Quandary: Phishing Evolved

In 2019, receiving an email containing a QR code would have likely raised some eyebrows, appearing strange and suspicious to the recipient. Fast forward to the year 2023, and the situation has dramatically changed. The widespread adoption of QR codes for everything from viewing restaurant menus to online payments and public transport apps has conditioned many of us to respond almost instinctively. The sight of a QR code in an email or text message acts like a "Pavlovian cue," prompting us to unthinkingly reach for our phones, ready to scan.

This shift in human behavior was noticed by threat actors, who are now capitalizing on the "conditioned" trust in QR codes to launch increasingly sophisticated phishing attacks. Despite the fact that the core principles of phishing remain largely unchanged, quishing makes the threat more complex and much harder to detect. By hiding the malicious link behind a QR code, threat actors force the victims to move from a laptop or a desktop to their mobile devices, which in most cases have much weaker cyber defenses.

Quishing utilizes another psychological maneuver that greatly benefits the attackers and increases their success rates. Quishing moves the "playground" onto a mobile phone where the victims are primed for additional steps that involve their personal device. With the phone in their hands, the cognitive journey users must take for going through Multi-Factor Authentication (MFA) is significantly shorter, and the chances of the user inserting SMS verification codes, tapping a prompt on the screen or using biometric authentication (facial recognition or fingerprint scanning) are much higher.



The CEO almost fell victim to quishing attack – a tale from a /sysadmin sub-Reddit

© 2023 Perception Point

Undetectable? The Deceptive Simplicity of Malicious QR Codes in Emails

Quick Response (QR) codes are essentially a graphical representation of data, mostly used to encode URLs, the process of converting a link into a QR code takes seconds and can be easily done by anybody with online access (there are hundreds of free QR generators available).

When a malicious URL is hidden behind a QR code, the link becomes an image file, not a clickable element. Traditional email security systems like secure email gateways (SEGs) and even the most modern email security solutions scan for suspicious links in the email body of the message to prevent phishing attacks (relying on domain reputation and other indicators), but may overlook embedded URLs within images or file attachments. Most security solutions are unable to extract and dynamically scan links from QR codes.

Quishing campaigns present a unique challenge to defenders. By embedding the phishing link within a QR code, the threat is effectively concealed, rendering security measures ineffective and allowing malicious emails to slip through and reach the inbox of targeted end users.

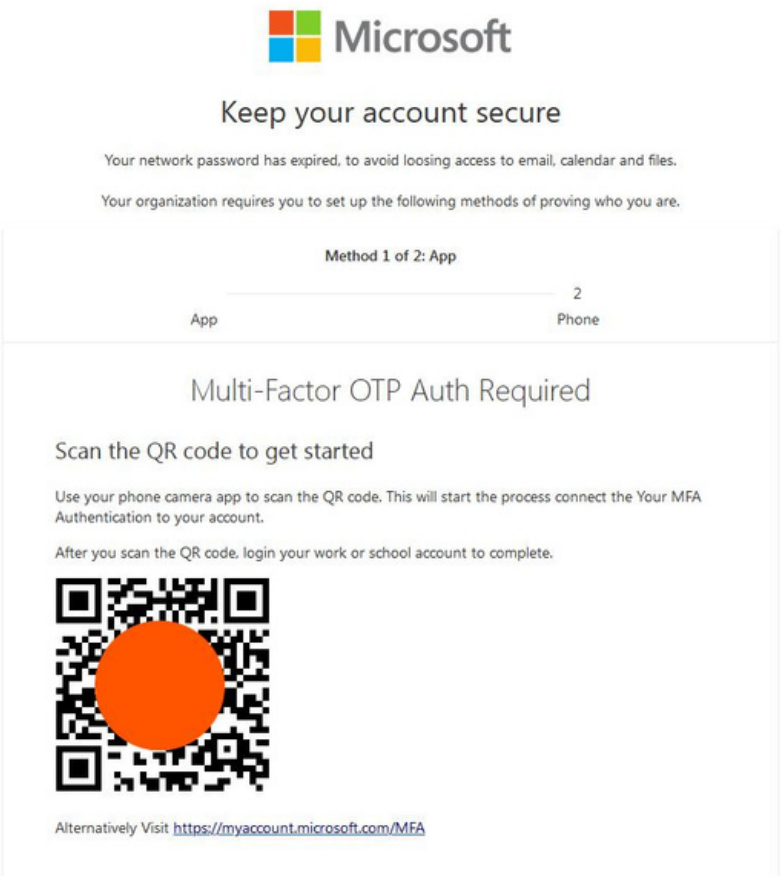
In addition to the technicalities involving the malicious URL delivery, threat actors often craft their QR codes, the look and feel of the email, and the associated phishing site to impersonate known and trusted brands. It is very common to see logos and domain names that mimic Microsoft or Google in quishing campaigns. Social engineering techniques also play a major role in quishing where cybercriminals employ scare tactics and incite urgency (“your password is about to expire”) to encourage the users to scan the QR code without questioning its legitimacy.

Quishing Impossible: a Look at Examples From the Wild

Perception Point’s security research team has observed a substantial increase in quishing campaigns over the last few months with 90% of the attacks targeting end users that operate within Microsoft 365 email environment. Let’s review 2 examples caught by Perception Point to better understand the modus operandi of threat actors that employ QR code attacks.

© 2023 Perception Point

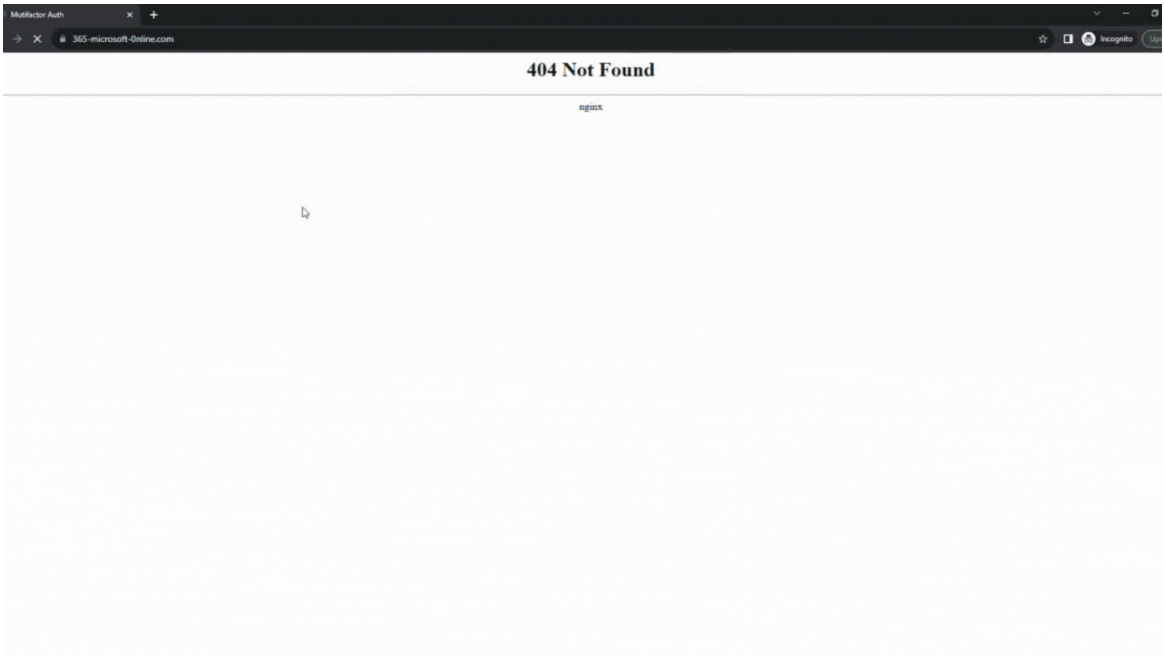
Quishing 1: QR Code Embedded Within the Email Body as an Image
Email subject: <COMPANY NAME>, Multi-Factor Auth
Sender display name: <COMPANY NAME> 2FA Security <noreply@COMPANY DOMAIN>



In this particular quishing campaign sent to multiple targets within many organizations, the threat actors impersonate Microsoft 365 and alert the end user about their "network password" that has expired. The message encourages the recipient to scan the QR code using their mobile camera for "connecting" MFA method to their Microsoft account. The sender's name and email subjects were altered to fit the target company.

The text, logos and the QR code are actually a single image and the email body contains no textual data at all.

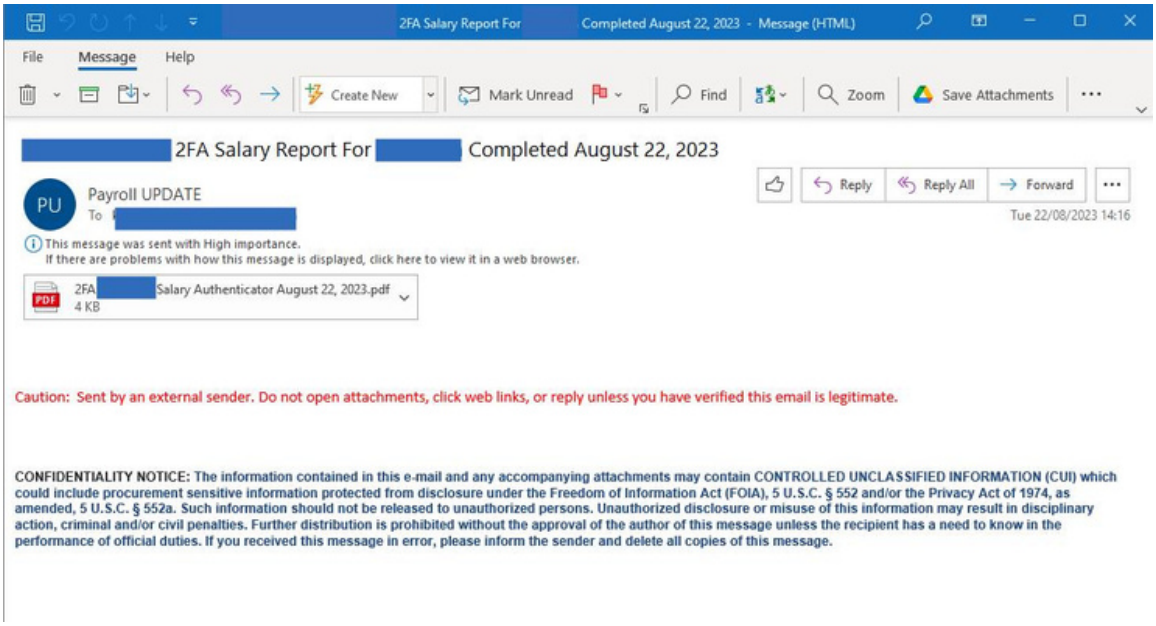
End users that would have fallen for the quishing scam and actually scan the code would have been presented with a Microsoft look-alike page that automatically redirects them to a fake login page aimed to steal their account credentials.



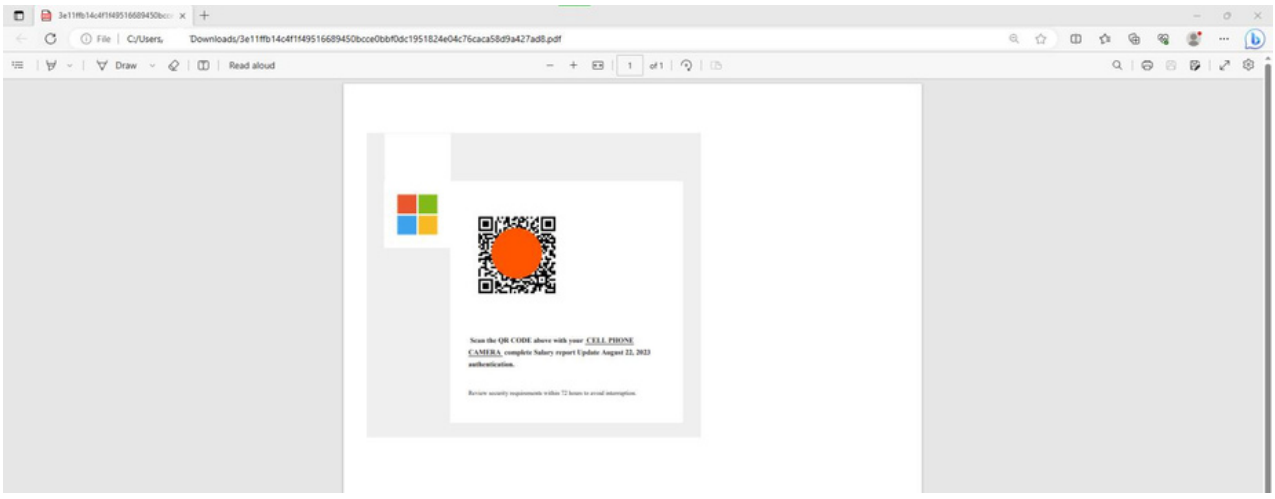
© 2023 Perception Point

Quishing 2: QR Code Inside a PDF attachment

- Email subject: <COMPANY NAME> 2FA Salary Report For <TARGET NAME> Completed August 22, 2023
- Sender display name: Payroll UPDATE
- File attachment name: 2FA <TARGET NAME> Salary Authenticator August 22, 2023.pdf



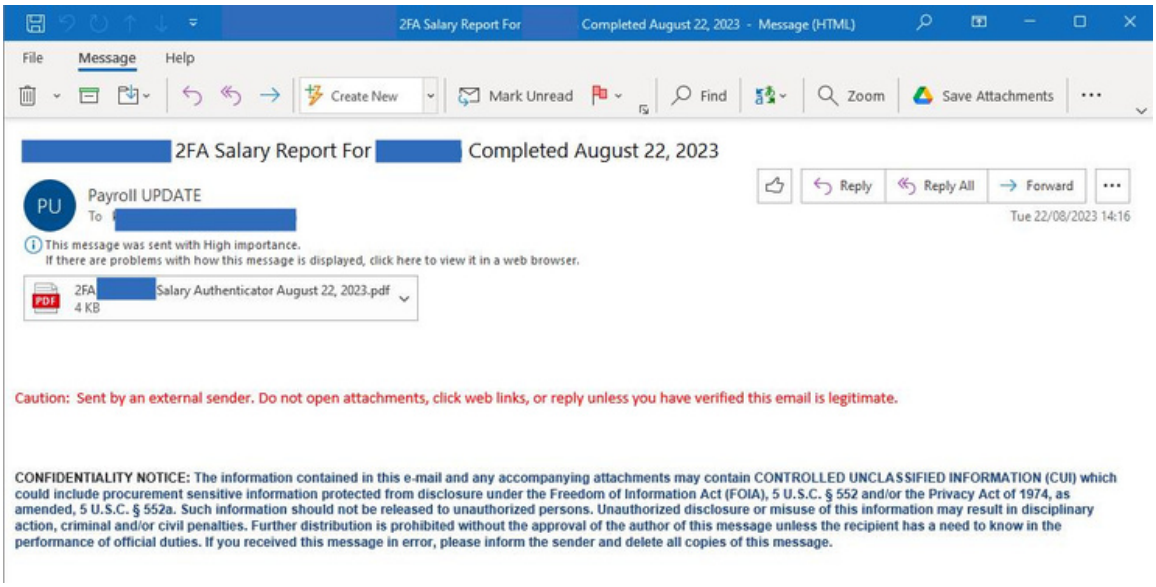
Here we have another quishing sample where the malicious QR code is hidden inside an attachment to the email – a PDF file. The social engineering behind this campaign revolves around the financial motivation of the targets. The email subject, sender's name and the PDF file attached all indicate a vague requirement to complete some sort of Two-Factor authentication (2FA) regarding the target's salary.



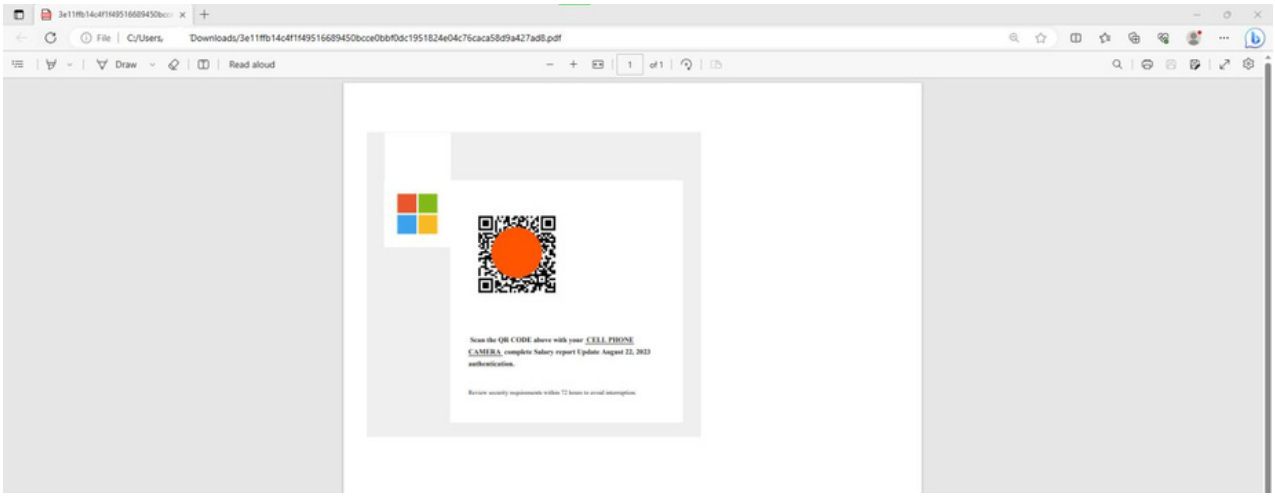
© 2023 Perception Point

Quishing 2: QR Code Inside a PDF attachment

- Email subject: <COMPANY NAME> 2FA Salary Report For <TARGET NAME> Completed August 22, 2023
- Sender display name: Payroll UPDATE
- File attachment name: 2FA <TARGET NAME> Salary Authenticator August 22, 2023.pdf



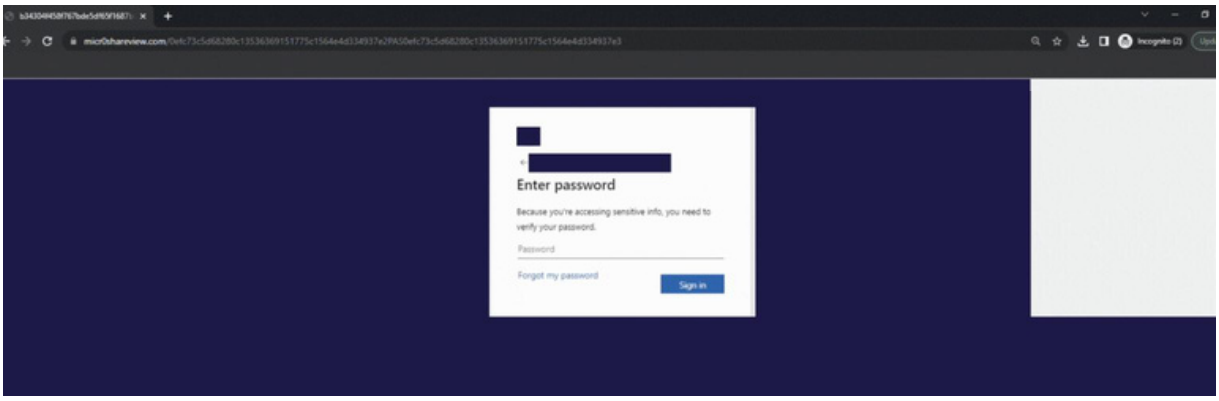
Here we have another quishing sample where the malicious QR code is hidden inside an attachment to the email – a PDF file. The social engineering behind this campaign revolves around the financial motivation of the targets. The email subject, sender's name and the PDF file attached all indicate a vague requirement to complete some sort of Two-Factor authentication (2FA) regarding the target's salary.



This is what the PDF looks like. We can see Microsoft logo, a QR code image and a short instruction to "scan the QR CODE above with your CELL PHONE CAMERA complete Salary report Update August 22, 2023 authentication."

© 2023 Perception Point

Upon scanning the QR code, the targets would have been redirected to a fake Microsoft login form automatically injected with their email address. To add another touch of personalization, the threat actors used the target's own company logos when designing the spoofed Microsoft form.



Preventing Quishing Starts with Actual Prevention

In the battle against quishing, many email security vendors tend to "beat around the bush," offering insights and best practices that, while valuable, do not directly address the core issue of quishing, and assume that malicious QRs reaching the user's inbox is inevitable. Common recommendations include security training for employees, Multi-Factor Authentication (MFA), and URL inspection. While these measures can enhance overall security, they can fall short in preventing the quishing attacks.

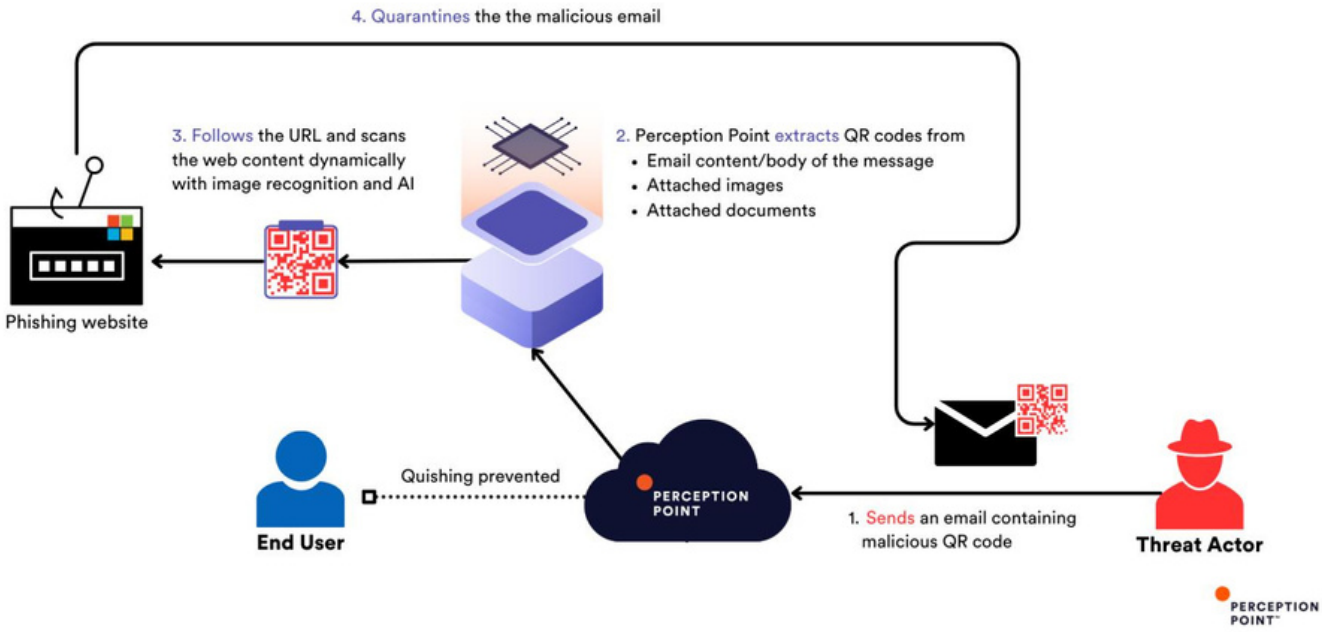
The Limitations of Conventional Solutions

- Security Training: Educating employees about the risks of quishing and how they can recognize potential threat indicators ("hey, don't scan QR codes from emails") is essential but not foolproof. Human error remains a significant risk factor, and even well-trained individuals can fall victim to QR code-based attacks.
- Multi-Factor Authentication: MFA adds an extra layer of security but may not prevent the initial compromise through a quishing attack. If the malicious QR code leads to a phishing site that captures MFA credentials, the added layer can be bypassed.
- URL Inspection and Sender Anomaly: Traditional URL filters do not extract URLs hidden within QR codes, especially if they are embedded in images. Detecting anomalies is a good method but what if the malicious QR code is sent from a perfectly legitimate source? (e.g external account takeover).

© 2023 Perception Point

A Definitive Solution to Quishing

At Perception Point we take a different, much simpler and more secure approach, focusing on actual prevention of quishing rather than mitigation or education. By actually scanning all QR codes and actually following the URLs within them, Perception Point uses image recognition and AI to detect and block quishing attacks at their source before they even get to the end users.



How Perception Point Prevents QR code Phishing Attacks

Using real-time image recognition models, QR codes are extracted from the body of the email or from attached images and documents (PDFs, Office files, etc.). A proprietary anti-evasion algorithm then follows the URLs to scan them dynamically for any phishing or malware delivery attempts.

Perception Point anti-phishing technology consists of a myriad of AI and ML detection models including:

- Two-Step Phishing: object detection model examines webpages to recognize clickable elements for further scanning (evasion: end users are first presented with a trusted page, clicking an element within it redirects them to the malicious payload).
- Login Forms Detection: Computer vision models detect input boxes and login forms, crosscheck them with the URL and identify anomalies and prevent credential theft.

© 2023 Perception Point

- Brand Recognition: Comparing email/URL/file screenshots/images/URL favicons to logos and visual assets of known brands to detect spoofing and phishing. The data is analyzed against known 'clean' images (e.g. official Microsoft logos) and known 'malicious' ones (impersonation attempts caught by Perception Point).
- Domain Lookalike and URL Lexical Analysis: S-GLocal algorithm incorporates heuristic biological algorithms and modifies them to identify domain lookalikes and impersonation attempts. ML model analyzes the URL structure to find similarities to malicious URLS and to predict whether or not the link is malicious.
- GenAI Decoder™: LLM-based model utilizes transformers to recognize the patterns in AI-generated text and detects malicious social engineering attempts in the email text.

By focusing on actual prevention and leveraging advanced technology, Perception Point is leading the way in protecting modern organizations from the hidden dangers of QR codes.

Contact us: info@perception-point.io
Visit us: perception-point.io
© 2023 Perception Point