HC3: White Paper

October 23, 2023 TLP:CLEAR Report: 202310231700

QR Code-Based Phishing (Quishing) as a Threat to the Health Sector

Executive Summary

Phishing – the use of phony e-mails to deliver malicious code – has historically been a successful means for cyberattackers to compromsie victim organizations and launch full-fledged, multi-staged cyberattacks. Phishing attacks are frequently utilized as the first stage of an attack – the infection vector – and this is especially true for the health sector. A cyberattack that begins with phishing often ends with ransomware and/or a major healthcare data breach. Quick response (QR) codes were designed to quickly read and transmit legitimate data, but have become increasingly abused as part of phishing attacks, called "quishing". In this paper, we provide a brief overview of QR codes, phishing attacks, and the application of both of these to cyberattacks on the health sector. We conclude this analysis with recommended defense and mitigation actions to reduce the likeliness and effectiveness of phishing attacks, including those augmented by the use of QR codes.

QR Codes

A quick response code, or QR code, is a machine-readable image in the form of a matrix that transmits information when scanned by an informaiton system. QR codes connect the digital and physical world, and are frequently used by commercial tracking, advertising and convenience-oriented applications, and are compatible with and often utilized with modern smartphones. The term "quick response" refers to the purpose of a QR code to be scanned in order to access data, and this process happens very quickly. Legitimate QR codes are frequently sent via e-mail and as such, are also abused by those who use e-mail as part of cyberattacks, in the form of a phishing attack.

Phishing and the Health Sector

Phishing is a form of social engineering that is often used as the infection vector (initial step) in a multi-stage cyberattack. It utilizes an e-mail disguised to look authentic in order to provoke the victim to interact with it, and deliver malware to the victim's system and continue the cyberattack. Phishing e-mails include one of two means by which they drop malware, either by inducing the victim to open an attachment in the e-mail, or clicking on a link in the e-mail. Once that occurs, the malware is delivered and the cyberattack continues. Some of the most common cyberattacks targeting both the public and private health sectors are ransomware attacks, data breaches (and combinations of ransomware and data breaches), intellectual property theft (especially medical research), and other forms of digital disruption, extortion and data exfiltration. These attacks often begin with a successful phishing attack. (See **Figure 1**.) Phishing has been an increasingly successful tactic for initiating cyberattacks. In 2022, the FBI's Internet Crime Complaint Center (IC3) found that phishing attacks were the number one reported cyber crime, with over 300,00 complaints reported. These attacks are also very impactful. According to a 2021 survey conducted by the Ponemon Institute and Proofpoint, the cost of phishing attacks quadrupled from 2015 to 2021. The same research found that the average cost of a successful phishing attack in 2021 was $14.8 million. Phishing is a common tactic for hackers to use against the health sector because it often leads to data breaches, and the stolen health data has the potential to be lucrative for the attackers. The 2021, the Healthcare Information and Management Systems Society found that the most common attack impacting healthcare organizations was phishing, comprising almost half of all attacks.

HC3: White Paper

October 23, 2023 TLP:CLEAR Report: 202310231700

Figure 1: Phishing as Initial Access *(Source: Proofpoint)*

QR Codes and Phishing

QR codes are often inserted into e-mails for legitimate purposes. They can serve to replace traditional hyperlinks and be especially useful when the end user is utilizing a smartphone. However, they are often abused as a part of cyberattacks, especially phishing, which is sometimes referred to as quishing. The most common way QR codes are used for malicious purposes is to simply e-mail the user a QR code in a way presented as useful, but actually points the user towards a malicious site or initiates the download of malware. Fundamentally, quishing is very similar to phishing in the abuse of links to trick the victim into interacting with them. The ability to track a user into scanning a QR code is often based on false context; an e-mail containing text and graphics falsely creating the impression that it is something the user would be interested in. For example, **Figure 2** (below) is an example of a quishing e-mail designed to get the user's attention by purporting to be related to employee benefits, while **Figure 3** (below) is disguised as a security-themed e-mail alert, concerned with multi-factor authentication.

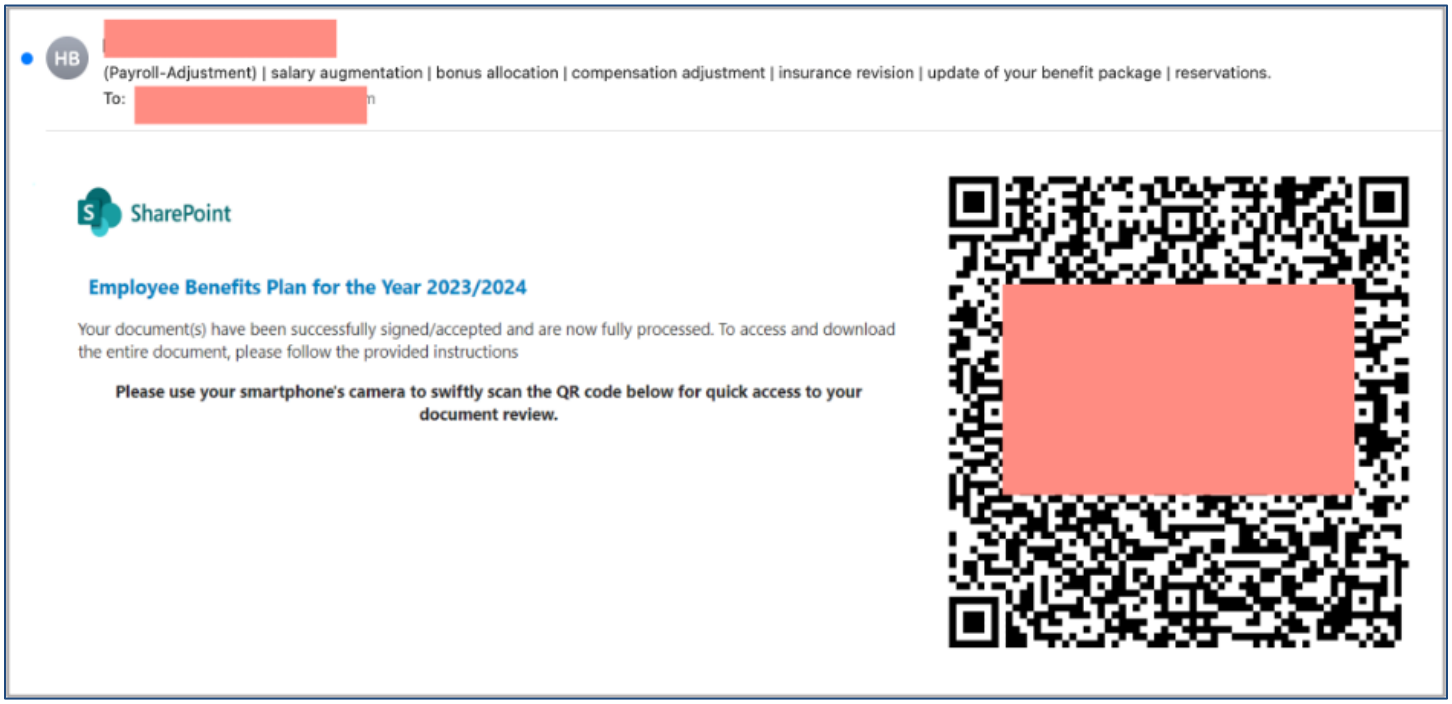

Figure 2: A quishing example pretending to be an employee benefit plan. *(Source: Barracuda)*

HC3: White Paper

October 23, 2023 TLP:CLEAR Report: 202310231700

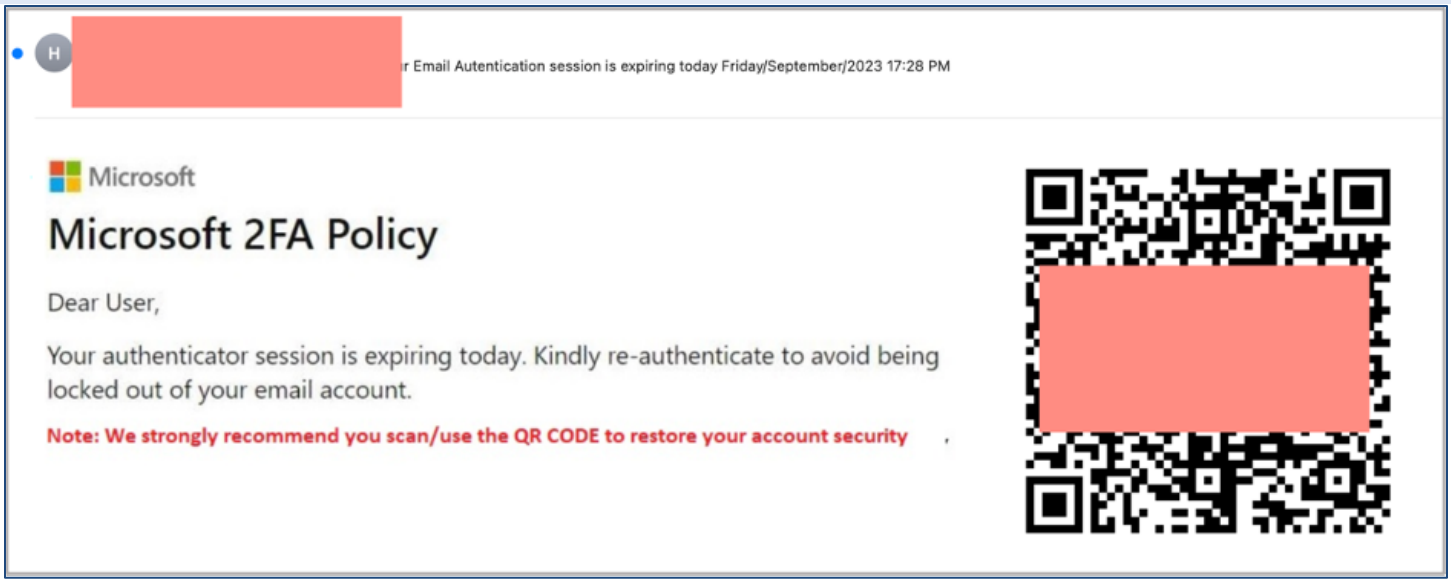

Figure 3: A quishing example pretending to be a multi-factor authentication security alert. *(Source: Barracuda)*

Countermeasures and Mitigations

Preventing successful phishing attacks begins with defense in depth. The first layer of protection for any enterprise will likely be at its e-mail server, which will have a connection to the Internet. Ensuring that your mail server is configured to filter unwanted e-mails, or an additional platform is integrated into your information infrastructure, such as a spam gateway filter, will serve this purpose. These will not prevent all phishing e-mails, but they should strip away some unwanted traffic.

Second, awareness training for end users is imperative. They should be trained to detect a phishing e-mail and interact with all e-mail with a healthy degree of skepticism. Phishing e-mails will be designed to capture the attention of the victim, and there are any number of common themes in order to attempt to do this:

- The e-mail may reference an invoice (and contain an attachment).
- The e-mail may be requesting personal information.
- The e-mail may reference suspicious activity or login attempts on an account a user might have.
- The e-mail may reference a payment, especially a late payment, and provide a link to pay.
- The e-mail may offer a coupon or discount on products or services the user may be interested in.
- The e-mail may reference a government refund.

Other indicators of phishing attempts include a suspicious sender's address, generic greetings, spoofed links, improper grammar and spelling, and suspicious attachements. More details on these can be found on CISA's social engineering resource page.

Third, multi-factor authentication is highly recommended. This will protect against stolen credentials, which can be the initial purpose of a phishing attack. MFA will not prevent malware from being dropped on a victim system. The Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security, has created a guide on Implementing Phishing-Resistant MFA, which is highly recommended.

Fourth, security software should be in place. In addition to the previously-mentioned e-mail gateway

filtering, endpoint security software deployed to and frequently updated on every end user's system is highly recommended. This type of software may detect malware as it is being executed on a system, if a phishing e-mail is interacted with by a user.

Similarly, preventing QR code abuse and use in a cyberattack involves education and prevention. The same resources that can be used to prevent user access to known malicious sites, and can prevent downloading of malware with traditional phishing attempts, can also apply to quishing. The FBI recommends the following actions to prevent quishing:

- Do not scan a randomly found QR code.
- Be suspicious if, after scanning a QR code, the site asks for a password or login info.
- Do not scan QR codes received in emails or text messages, unless you know they are legitimate. Call the sender to confirm.
- Some scammers are physically pasting bogus codes over legitimate ones. If it looks as though a code has been tampered with, do not use it. The same caution applies to legitimate ads that you pick up or get in the mail.

Additional FBI guidance can be found here and here.

Resources

CISA phishing infographic:
https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

FBI Tech Tuesday: Building a Digital Defense Against QR Code Scams:
https://www.fbi.gov/contact-us/field-offices/elpaso/news/fbi-tech-tuesday-building-a-digital-defense-against-qr-code-scams

CISA: Avoiding Social Engineering and Phishing Attacks:
https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

References

Peeling off QR Code Phishing Onion: Revealing the Hidden Layers of Deceit
https://www.trellix.com/en-us/about/newsroom/stories/research/peeling-off-qr-code-phishing-onion.html

Quishing: What you need to know about QR code email attacks
https://blog.barracuda.com/2023/10/05/quishing-what-you-need-to-know-about-QR-code-email-attacks

Ivanti: QR Code Survey Report
https://www.ivanti.com/resources/v/doc/ivi/2554/e3af63a9e95e

How attackers exploit QR codes and how to mitigate the risk
https://www.csoonline.com/article/569957/how-attackers-exploit-qr-codes-and-how-to-mitigate-the-risk.html

Cybersecurity Stop of the Month – QR Code Phishing
https://www.proofpoint.com/us/blog/email-and-cloud-threats/cybersecurity-stop-month-qr-code-phishing

Cybercriminals Tampering with QR Codes to Steal Victim Funds
https://www.ic3.gov/Media/Y2022/PSA220118

QR Code Phishing Campaigns
https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/qr-code-phishing-campaigns

Phishing Campaign Abuses QR Codes to Steal Credit Card Details
https://threatresearch.ext.hp.com/chinese-phishing-campaign-abuses-qr-codes-to-steal-credit-card-details/

QR Codes Are a Double-Edged Sword for Patient Care
https://healthtechmagazine.net/article/2023/08/qr-codes-are-double-edged-sword-patient-care

Scammers are emailing waves of unsolicited QR codes, aiming to steal Microsoft users' passwords
https://cyberscoop.com/qr-code-phishing-scam/

Phishing attacks use QR codes to steal banking credentials
https://www.bleepingcomputer.com/news/security/phishing-attacks-use-qr-codes-to-steal-banking-credentials/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback