Evolution of Sophisticated Phishing Tactics: The QR Code Phenomenon

Executive Summary

Since late 2024, Unit 42 researchers have observed attackers using several new tactics in phishing documents containing QR codes. One tactic involves attackers concealing the final phishing destination using legitimate websites' redirection mechanisms. Another tactic involves attackers adopting Cloudflare Turnstile for user verification, enabling them to evade security crawlers and convincingly redirect targets to a login page. We found that some of these phishing sites are specifically targeting the credentials of particular victims, suggesting pre-attack reconnaissance.

In traditional phishing attacks, attackers use obvious links or buttons in phishing documents. Attackers have begun embedding phishing URLs into QR codes, a technique known as QR code phishing or quishing. This strategy entices recipients to scan the codes with their smartphones, which can lead them to unknowingly access phishing sites and expose their credentials to theft.

Our telemetry shows these phishing attacks have been widespread across the U.S. and Europe. The attacks are also impacting various industries, including the medical, automotive, education, energy and financial sectors.

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Cloud-delivered security services for the Next-Generation Firewall including Advanced WildFire, Advanced URL Filtering and Advanced DNS Security

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics	**Phishing**, **Social Engineering**, **Credential Harvesting**

QR Code Phishing

A QR code is a machine-readable, scannable image capable of storing various types of information. It can contain numbers, text or a URL. To interact with these images, people use their smart devices' camera applications to interpret the code. The camera app typically assists in opening URLs in a browser or dialing a phone number if the QR code contains such information.

Figures 1 and 2 show that these QR code phishing attacks are spoofed to look like electronic signature documents generated through Docusign or Adobe Acrobat Sign. These are not legitimate documents generated by either service. Embedding phishing URLs within QR codes makes it more difficult for traditional scanning engines to extract the actual URL from phishing documents.

You have received a document to review and sign today

Review Now

Please use your smartphone camera to scan the Qr code below for quick access to your document for review

completed. Please Docusign - [redacted] documents

Do Not Share This Email
This email contains a secure link to Docusign. Please do not share this email link, or access code with others

About Docusign
Sign documents electronically in just minutes. it's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go - or even across the globe - DocuSign provides a professional trusted solution for Digital Transaction Management

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

Figure 1. A QR code phishing email spoofing a notification prompting the recipient to sign a fake DocuSign document.

ADOBE ACROBAT SIGN

company logo

All parties finished
QUOTE Agreement

Please use your smartphone camera to scan the QR code below for quick access to your document for review

Pending Quote approval.....

Attached is the final agreement between:

- |⊔•|⊔ [redacted]
- |⊔•|⊔ [redacted]

Read it with Acrobat Reader. You can also open it online to review its activity history.

Figure 2. A QR code in a PDF impersonating Adobe Acrobat Sign.

These phishing documents instruct potential victims to use their smartphones to scan the QR code, consequently raising the likelihood of them directly accessing the phishing URL on their personal devices. Personal devices often have weaker security controls than corporate devices, and accessing the URL on a personal device could bypass corporate security measures like email gateways and web filters.

Microsoft

[redacted] and Payroll Update for 2025

To:	[redacted]
Date:	Monday January 2025
From:	[redacted]
Remarks:	We value your contribution to the team, and in recognition of your hard work, dedication, and outstanding performance, we are pleased to inform you that you will receive a raise starting on your next paycheck.

Please scan the barcode and sign where necessary:

Please review the attached document, sign where needed (pages 4-5), and initial all pages before the next payment run. We appreciate your support and look forward to continuing this journey together. Kindly scan the QR code and follow the instructions.

Thank you for taking the time to provide your input.

Sincerely,

Figure 3. Phishing attempt impersonating company payroll update.

It is common for attackers to theme phishing documents around topics that would entice people to access the material without exercising due caution, such as payroll or HR announcements (Figure 3). To lower users' guard, attackers often include company logos, HR email addresses or dates in the document to make the phishing content closely resemble official documents. While these tactics are not new, we are observing more sophisticated tricks in current phishing campaigns.

Phishing URL Redirection

Analysis of the URLs extracted from the QR codes in these campaigns reveals that attackers typically avoid including URLs that directly point to the phishing domain. Instead, they often use URL redirection mechanisms or exploit open redirects on legitimate websites, as shown in Table 1. By using URL redirection, attackers can surreptitiously redirect users to malicious websites while masking the true destination of the phishing link.

Full URL Extracted From QR code	Redirect to Phishing URL
`hxxp://{legit_domain}/ViewSwitcher/SwitchView?mobile=False&returnUrl=hxxps://ebjv[.]com[.]au/filesharer`	`hxxps://ebjv[.]com[.]au/filesharer`
`hxxps://{legit_domain}/redirect/head/?u=hxxps://docuusign[.]statementquo[.]com/ey8YO?e={user_email}`	`hxxps://docuusign[.]statementquo[.]com/ey8YO?e={user_email}`

Table 1. Examples of phishing URLs that exploit legitimate websites for URL redirection.

This method of URL redirection for phishing has been prevalent for years. Therefore, many people are taught to carefully examine the full URL to avoid clicking on phishing links. However, when the URL is accessed via a QR code, people can only view the domain name through their smart device’s camera application, making suspicious URLs more likely to appear legitimate.

Figure 4 shows that phishing URLs extracted from QR codes abuse Google redirects.

```
https://www.google.com.mt//url?q=
%7BSOME%20RANDOM%20MIXED%20TEXT_RANDOM_MIX(24,'lowercase%7Cuppercase')%7D_
%7BSOME%20RANDOM%20MIXED%20TEXT_RANDOM_MIX(24,'lowercase%7Cuppercase')%7D_
%7BSOME%20RANDOM%20MIXED%20TEXT_RANDOM_MIX(24,'lowercase%7Cuppercase')%7D&
sa=t&url=amp/s/web-ofisi.com.tr/yeni/T6epXbk4ck8zZNXyS5wyRzTbm43LOM1gR49
#[redacted]
```

random texts

phishing URL destination

user email

Figure 4. Phishing URL that abuses Google redirects.

These redirects enable legitimate websites to seamlessly redirect users to external pages while maintaining the original source. Attackers have taken advantage of this functionality to create more convincing phishing URLs.

To further deceive targets, attackers include random or meaningless text in the Google redirect URL, effectively obscuring the destination phishing URL. This poses a challenge for people attempting to verify the redirect destination on their smart devices when scanning QR codes.

Google states that, if you report only an open redirector, they won't file a bug unless its impact goes beyond phishing. When we contacted them regarding this post, they added the following clarification:

> *Open redirectors take you from a Google URL to another website chosen by whoever constructed the link. Some members of the security community argue that these redirectors aid phishing, because users may be inclined to trust the mouse hover tooltip on a link and then fail to examine the address bar once the navigation takes place.*
>
> *Our take on this is that tooltips are not a reliable security indicator, and can be tampered with in many ways. For this reason, we invest in technologies to detect and alert users about phishing and abuse instead. More generally, we hold that a small number of properly monitored redirectors offers fairly clear benefits and poses very little practical risk.*

Phishing Operations

Based on our investigation of recent QR code phishing attacks, we can summarize typical phishing operations into three key steps:

- Redirection
- Human verification
- Credential harvesting

Redirection entails directing the target to a phishing site upon scanning the QR code. By exploiting open redirects, attackers can use multiple redirects to ultimately guide their target to the destination phishing site.

Using multiple redirects obfuscates the attack, increasing the complexity for security crawlers. It also conceals the infrastructure of the phishing site, providing attackers with better detection evasion.

With human verification, attackers exploit legitimate websites' need to authenticate users as a way to defend against automated attacks such as web scraping and distributed denial-of-service (DDoS) attacks. Legitimate websites commonly use human verification mechanisms such as Captcha Verification Questions to validate that visitors are humans and not bots.

Attackers often integrate human verification within the multiple redirects they employ. We have observed a trend of recent QR code phishing attacks incorporating Cloudflare Turnstile as a means of human verification, as shown in Figure 5.

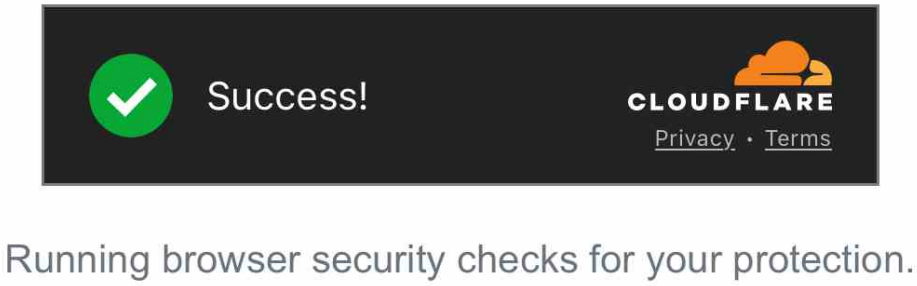

Figure 5. Human verification during attackers' multiple redirects, using a tool designed not to mandate direct human interaction to proceed.

Cloudflare Turnstile offers a free subscription. The key benefit of this human verification technique to attackers is that it does not mandate direct human interaction to proceed.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product is flawed or malicious.

We also found that attackers set up redirects to legitimate login pages or Google 404 error pages when human verification mechanisms block access. This helps avoid detection of phishing infrastructure when security crawlers try to access these pages.

The final step is credential harvesting, where attackers collect credentials or sensitive information provided by victims on fake login pages. These fake login pages are often designed to mimic legitimate service providers, such as Microsoft 365, or may display the victim’s company logo.

In QR code phishing, the phishing URL often incorporates the user's account or email address. Consequently, when targets encounter the fake login page, they may see their account or email address is already populated as shown in Figures 6 and 7. This eliminates the need for them to re-enter this information. As a result, the target may only be prompted to input their passwords, creating an illusion of familiarity and legitimacy to further deceive them into divulging their credentials.

UNIT 42
BY PALO ALTO NETWORKS

Sharepoint

Verify Your Identity

You've received a secure link to:

Shared file.

To receive and download this PDF file, please enter specific professional email **jac*****@**[redacted] credentials that this document was sent to.

Verify

© 2024 Microsoft Share Point Privacy & Cookies

Microsoft

Figure 6. Fake Sharepoint page with pre-populated user email.

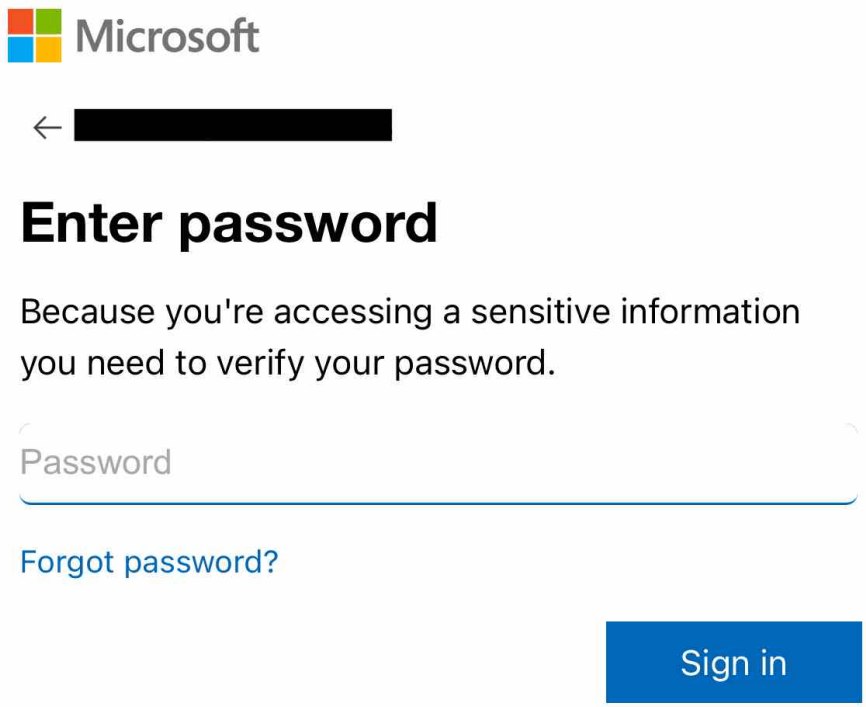

Figure 7. Fake Microsoft 365 login page with pre-populated user account information.

It is surprising and concerning that attackers can selectively harvest credentials based on a targeted list of victim names. The fact that fake login pages reject arbitrary credentials and display error messages (as shown in Figure 8) suggests a sophisticated level of targeting and customization in these phishing attacks. Attackers using such tactics are likely focused on specific individuals or organizations, and they'll tailor their efforts to maximize the success rate of credential harvesting.

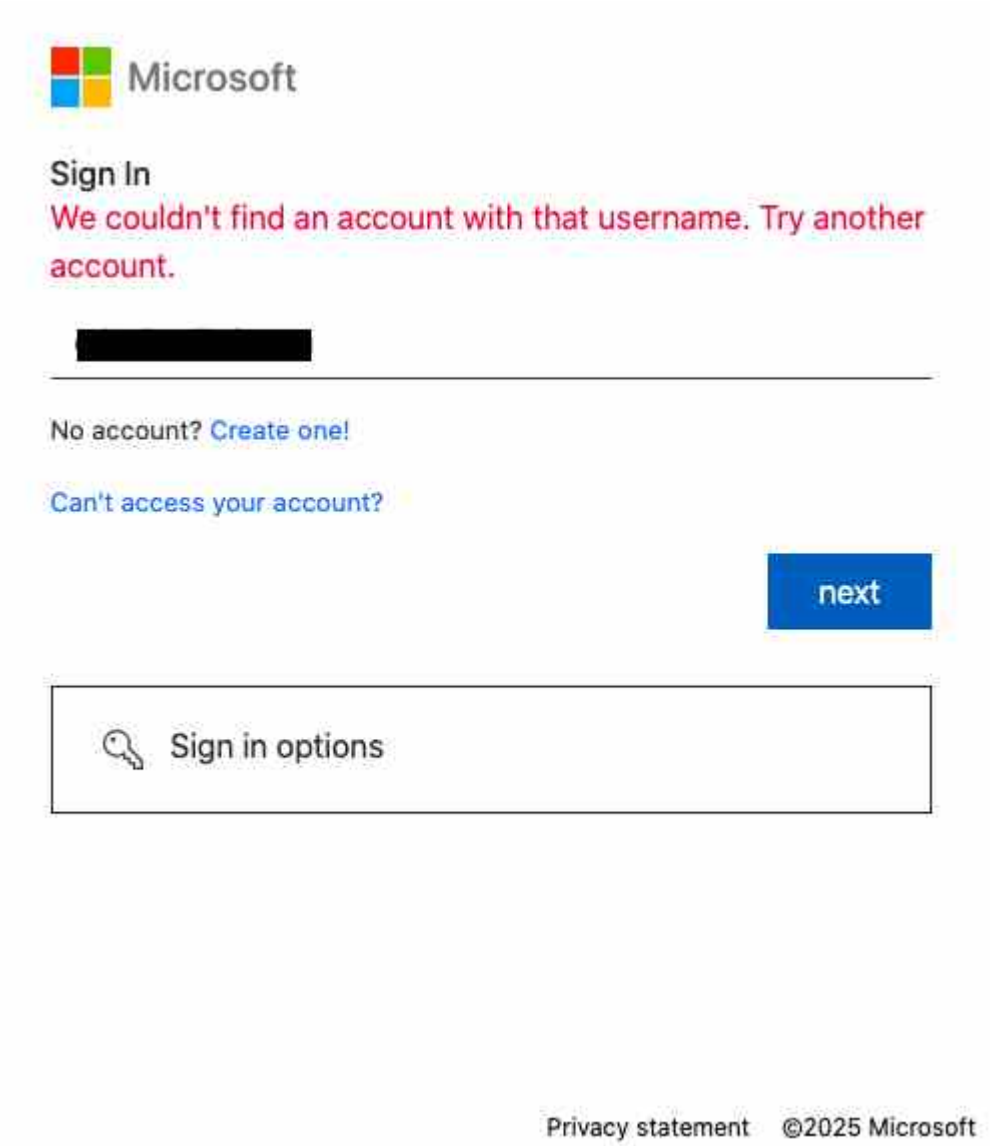

Figure 8. Error message to reject arbitrary credentials.

Conclusion

Phishing attacks and social engineering tactics remain significant threats to users, and it is evident that these tactics have evolved over time.

Our research highlights several key observations of attacker's activities:

- Using QR codes in phishing documents to disguise malicious URLs
- Exploitating open redirects to complicate attack analysis

- Incorporating human verification within redirects

These evolving tactics challenge both security detection mechanisms and user awareness. Attackers' increasing use of QR codes in phishing highlights the need for improved security awareness training and technical solutions that can detect and block these threats.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the IoCs shared in this research.
- Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

PDFs:

- b6130b45131035bec8d9b0304e934f2db0ee092ccaa709c3c2e8dd93770527bb
- e2cdd7eb0ea24c22d1e3dfea557a5a47dfdcd7c6b00b05bd5d099e0c8633ac25
- fa38f31ed09774cfd2627bff376c27c44611b842b96f3215b0a491805d525a40
- 0209e93d568da3cd33f7af9e8733dd6eb56b3957b19622126f5115f36c2433dd
- 6963820a6dadba2779a4b3999c5fde88faf8cf2dfa55d032b307217d9a80b77c
- a4d40396bc437933a7f097e3ba997c91c82a5f516a719f6181ca4d51fa85a7aa
- 1c3be2037b2a7b36311ef8fbcaa416ecb250dc20f5881570e8373e6e7f8237b1
- 8ea80304722e4285987b66dd8c74853b8a1474f585d7e24dc7616be4265d0d82
- cbc5c6edb34ca898ca55f166ec64b23b057f9d8e8859c6fe9c9065bb42991f5b
- 46897a4edb500df17e32ccee8a3134e3a15db387dd0492d8e110200d8cb57b60
- 3f2a3cc1216bfc6d1aa6d1b75150350da86a3a8c9c5b014c4b5f7ca62935c88c
- e682612a533382ddc188f547b37d93fd3f2de8ac7d5fd5f76eb92a22849109aa
- 6a0c8d59d5d0b2bd44d81a3f3e20bcd6c515ca6bd30c3bf090bccc4049276276
- 6472293c24554bf52772a9f8543fe7ae973f1d5b4795ccc14940beeddcba118e
- 9fe76bad7fa4f45ef49e720dde442f31f4c1847c7322ec09c09c5dd851f4de38
- 56d3e1daddd87a2454084a4687d6c245b3a3b2f2010d705d2b1983c0e87a5509
- 1bd8cace9e338eacdd9e41b55c594404483e1a1860d1946f612ecd21a6a7e5e5
- 3d66c093763eef0aa1b7c31242516d8d56e8fbe178f0915063045a6f85e61399
- 389ba4f794b66abe4fde0ede57450abb63ba1a3cd43940925762f206b03e1bea
- 0e03f873f1fb44e2d9f8ba29c80158f23735bb2ef819feb99f5623e933d752e9
- 0d0d4cd198de3a8b5af74fbebfc4c657609570157f8f961499433d0d5f748e7c
- 8c744eadec25b92de4ada45cdbc5e4c3507195127b2ed2f8450a7435b50b1f25
- 1737819220920abfa1d2201c0986df84b6570cbbc8d1aa96245151ed95c5992d
- b39855bd43bf45aff70da6fbd918789b17ff58d9c6764cc40db9aec4ecb79cc0
- de158906c855857d435635ebfd1ac97a6715b0a890f536aafcf55c601585f751
- 07fec0a55956f66f20888e21f72a01c043b1c02a141c07988a6313099526c796
- 891abde147f30c6dfd791f7f2f7cb081f5474f4f1392f670ed55a6d6cd3f14a2
- bdcfe5bf6eba8f59248739e1634bc43d50f5c55efbb7412c3b41e94f1a313771
- 5a5134dfed0d47d23073547ace40ff63be0b3138d835d6d5b0a5c5c3e1aa3d8e
- 2f38a598fd49256691c707198c546ab84ddeafedbe72c60a9d03364263820d25

- 3e8a9620823039b938b662d6285330baca7f3930e790faeaf4e4b95dd3c02427
- bc5e4ad38e324d742af28a2302bc6f59ec5f603f69b72bec7149b2cfbb50d980

Phishing **URLs:**

- hxxps://ebjv[.]com[.]au/filesharer
- hxxps://a1892279[.]nhubiubuniunuion[.]workers[.]dev
- hxxps://docuusign[.]statementquo[.]com/ey8YO?e=
- hxxps://fa8ea903[.]nhubiubuniunuion[.]workers[.]dev/
- hxxp://dhzyxo[.]promptexpression[.]com/?e=
- hxxps://docusignelectronic[.]courtappdirectory[.]com/6PkvL/?e=
- hxxps://storage[.]cloudcourtdoc[.]com/wsTtv?e=
- hxxps://fbl[.]5jbl2j[.]com/P6ThlTUUTfoKMgwqFKuQ/
- hxxps://docdxsiga[.]goodbreadtrucklng[.]com/gbkrV/
- hxxps://Docxxdoct[.]goodbreadtrucklng[.]com/U6bXM/
- hxxps://wtcg[.]rolixanorn[.]ru/n7cLGYDs/
- hxxps://dmcomunicacaovisual[.]com/m/?c3Y9bzM2NV8xX3NwJnJhbmQ9UjFKVU9YUT0mdWlkPVVTRVIwNjAxMjAyNVUwMzAxMDYzOQ==N0123N
- hxxps://advitya-heights[.]com/m/?c3Y9bzM2NV8xX25vbSZyYW5kPU9Ya3piRFU9JnVpZD1VU0VSMDYwMTIwMjVVMjUwMTA2NTA=N0123N
- hxxps://clases[.]pastorluiscastro[.]com/m/?c3Y9bzM2NV8xX25vbSZyYW5kPVVrcGhRMFE9JnVpZD1VU0VSMDYwMTIwMjVVMjUwMTA2NTA=N0123N
- hxxps://htbilisim[.]com/m/?c3Y9bzM2NV8xX3NwJnJhbmQ9V2tVNWFuWT0mdWlkPVVTRVIwNjAxMjAyNVUwMzAxMDYzOQ==N0123
- hxxps://www[.]magneticosrmn[.]com/m/?c3Y9bzM2NV8xX3NwJnJhbmQ9T0hwWFUxZz0mdWlkPVVTRVIwNjAxMjAyNVUwMzAxMDYzOQ==N0123N
- hxxps://vk[.]hrewatecea[.]ru/0Jrsf/
- hxxps://gracious-tranquility-production[.]up[.]railway[.]app/fa910c532fc9c990/eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9[.]eyJrZXkiOiJmYTkxMGM1MzJmYzljOTkwIiwiaWF0IjoxNzMzOTQ2NjQ0fQ[.]GDYykGf3tTA6K0GSiSvl01y_U0zveiKk9jmR_B3jTEw
- hxxps://web-ofisi[.]com[.]tr/yeni/T6epXbk4ck8zZNXyS5wyRzTbm43LOM1gR49#

Additional Resources

- Quishing – United States Postal Inspection Service
- Effective Phishing Campaign Targeting European Companies and Organizations - Unit 42, Palo Alto Networks
- Open redirectors – Google, Bug Hunters
- Cloudflare Turnstile - Cloudflare