

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 18, 2024



Security Challenges Rise as QR Code and AI-Generated Phishing Proliferate

Threat actors are increasingly using QR codes in phishing attacks, particularly adversary-in-the-middle (AitM) attacks, to capture two- and multi-factor authentication (2/MFA) credentials.

Threat actors' use of generative AI (GenAI) models to create credible phishing messages without grammar and syntax mistakes is almost certainly increasing.

Threat actors debuted the use of Amazon's notification service, AWS SNS, to automate smishing attacks, and weaponized VAST tags, a standardized format for delivering video ads, to deliver malicious content through video players.

Executive Summary

Between Q4 2023 and Q1 2024, threat actors increasingly used quick-response (QR) codes in phishing emails primarily targeting executives, abused Amazon Web Services (AWS) Simple Notification Service (SNS) to automate the delivery of malicious SMS texts, and weaponized Video Ad Serving Templates (VAST) tags for malvertising purposes. Additionally, they increasingly used large language models (LLMs) to generate highly believable and tailored phishing messages and introduced a new attack method to bypass machine learning-powered email gateways.

These tactics, techniques, and procedures (TTPs) broaden threat actors' reach while increasing the chances of bypassing security solutions and evading detection. For example, generating QR codes can be done easily and quickly using one of many tools available, and users have familiarized themselves with the technology, as shown by the 433% [increase](#) in QR code scans between 2021 and 2023. Similarly, LLMs can allow threat actors to [generate](#) approximately 1,000 phishing emails that are nearly as [convincing](#) as their humanly-crafted counterparts in under two hours for as little as \$10. On a related note, researchers associated a [reported](#) 1,265% increase in phishing attacks with the release of tools such as ChatGPT.

Phishing can lead to several business risks for companies. As an attack vector popular among cybercriminals and state-sponsored groups, it can have diverse effects depending on the perpetrator's ultimate motive. Regardless, these will almost certainly always include financial costs associated with remediation efforts, which can [exceed](#) \$1 million in worst-case scenarios. As new techniques such as QR code phishing and the use of LLMs continue to supercharge phishing attacks and help threat actors bypass traditional security solutions, capture multi-factor authentication (MFA) tokens, and deceive users, it becomes more likely that companies will face substantial financial losses and other business risks.

Companies must therefore familiarize themselves with the latest phishing trends and adapt their security posture accordingly. Mitigating QR code phishing and AI-generated phishing emails, for example, requires new training for employees — for example, the use of gamification can help turn a typically mundane training topic such as phishing into an engaging and effective learning experience — and the implementation of security tools capable of detecting such threats. Additionally, stronger oversight over corporate and personal mobile devices can help block employees from being redirected to malicious resources after scanning QR codes, and machine learning-powered email gateways offer several advantages over their traditional counterparts.

Key Findings

- Threat actors are increasingly using QR codes in phishing attacks, particularly adversary in-the-middle (AitM) attacks, to capture two- and multi-factor authentication (2/MFA) credentials, with a 248% increase in the number of references to the technique on sources such as security vendors, mainstream media, and government reports between Q3 2023 and Q4 2023.
- Several factors almost certainly drive this increase, including the added layer of obfuscation QR codes offer and the fact that victims need to scan them using mobile phones, which often fall outside the security umbrella of organizations.
- QR code phishing has become so prevalent that popular phishing-as-a-service (PhaaS) platforms, such as Tycoon 2FA and Greatness, have recently incorporated QR codes into their offerings.
- Based on data from Abnormal Security, executives received 42 times more QR code attacks than other employees in the second half of 2023, almost certainly due to their privileged and broader access to companies' resources and applications.
- Threat actors' use of generative AI (GenAI) models to generate phishing messages is almost certainly increasing; security company SlashNext recently correlated a 1,265% increase in phishing attacks between Q4 2022 and 2023 with the release of LLMs, such as ChatGPT.
- LLMs have so far mostly allowed threat actors to craft credible messages devoid of grammar and syntax mistakes, rather than facilitating the development of entirely novel techniques.
- Threat actors also debuted a new method for bypassing machine learning tools embedded in advanced email security solutions, dubbed "Conversation Overflow", in credential-stealing phishing operations.
- Threat actors debuted two additional novel techniques between Q3 2023 and Q1 2024, both designed to broaden the scale of phishing operations and lower the chances of detection. The first involves the use of Amazon's notification service, AWS SNS, to automate smishing attacks, and the second weaponizes VAST tags, a standardized format for delivering video ads, to deliver malicious content through video players.

Threat Analysis

Traditional phishing techniques, such as using archive files (ZIP, RAR, and so on), disk image files (ISO), HTML attachments, and Windows Installer (MSI) files to deliver malware, remained prevalent in Q4 2023 and Q1 2024. However, threat actors also introduced novel methods to enhance their campaigns, such as distributing malicious QR codes and VAST tags, as well as using legitimate services such as AWS SNS to automate the delivery of malicious SMS texts. Additionally, recent evidence highlighted threat actors' increasing use of GenAI models to craft phishing messages and seek novel ways to bypass email security solutions powered by machine learning.

These new developments are each explored in more detail below, with corresponding mitigations provided in the **Mitigations** section of this report.

QR Code Phishing Takes Center Stage

QR code phishing, also known as “quishing”, is a technique in which threat actors use manipulated or fake QR codes for malicious purposes, such as redirecting victims to malicious websites and login portals, downloading harmful content to steal sensitive information, and soliciting money transfers.

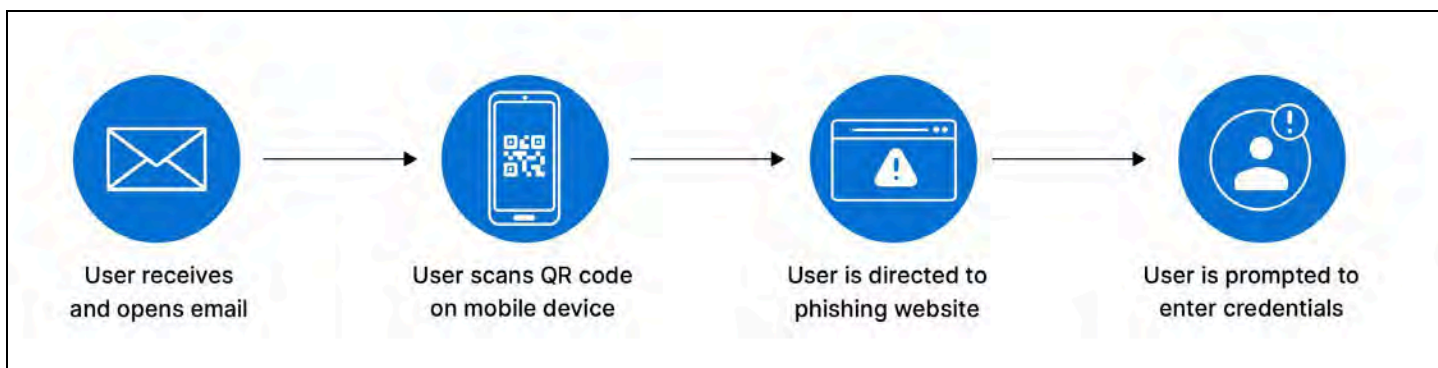


Figure 1: Example of a typical QR code phishing attack (Source: Recorded Future)

Malicious actors have actively exploited QR codes for phishing purposes for years, particularly since the COVID-19 [pandemic](#), during which QR codes were widely adopted as a contactless interaction method [1, 2, 3, 4, 5, 6]. However, evidence from several security vendors highlighted a marked uptick in QR code phishing in the latter half of 2023.

ReliaQuest [reported](#) a 51% increase in QR code phishing attacks in September 2023, when compared to the cumulative figure for January through August 2023, and the Hoxhunt Challenge (a cybersecurity study) [reported](#) that 22% of all phishing attacks within its purview in the first weeks of October 2023 used QR codes to deliver malicious payloads. Additionally, we observed an approximately 248% increase in references to QR code phishing and “quishing” on high-fidelity reporting sources (including government, mainstream media, and security vendor outlets) in Q3 2023 and Q1 2024 (**Figure 2**). While not every reference necessarily corresponds to a unique QR code phishing incident, the substantial

increase in mentions across high-fidelity sources strongly suggests a growing adoption of this technique by threat actors.

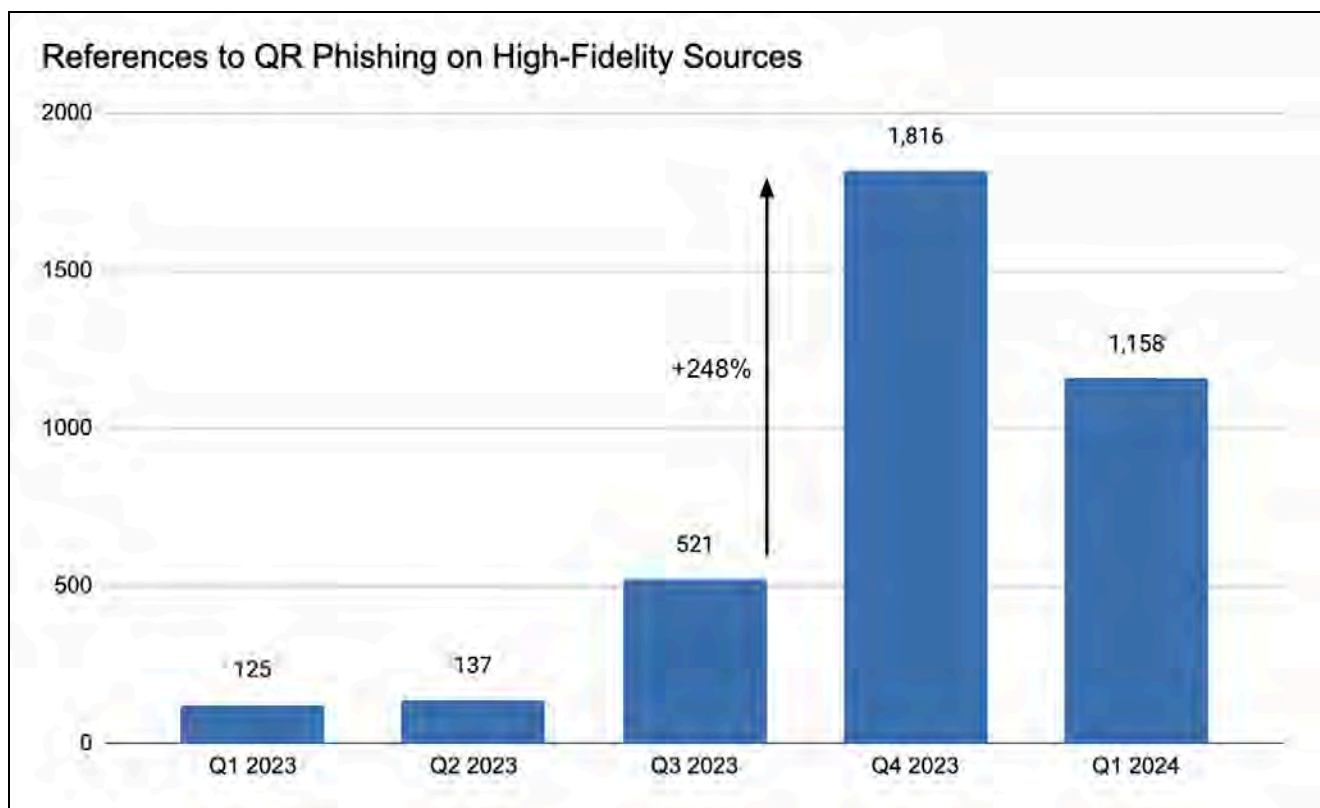


Figure 2: References to QR phishing spiked in Q4 2023 and continued in Q1 2024 (Source: Recorded Future)

The use of QR codes has become so popular in the threat landscape that PhaaS platforms offered on dark web forums and messaging platforms have started integrating them into their offerings. One recent example of this trend is Tycoon 2FA, a PhaaS active since at least August 2023 that is capable of stealing victims' credentials and 2/MFA codes through adversary-in-the-middle (AitM) attacks. As [reported](#) by Sekoia, Tycoon 2FA mostly uses URLs and QR codes embedded in email attachments or bodies to redirect victims to phishing pages. Another example is Greatness, a PhaaS platform available since mid-2022 that was [created](#) by a user going by the moniker "fisherstell". In January 2024, Trustwave [reported](#) that the latest version of Greatness supported QR code generation to store phishing URLs.

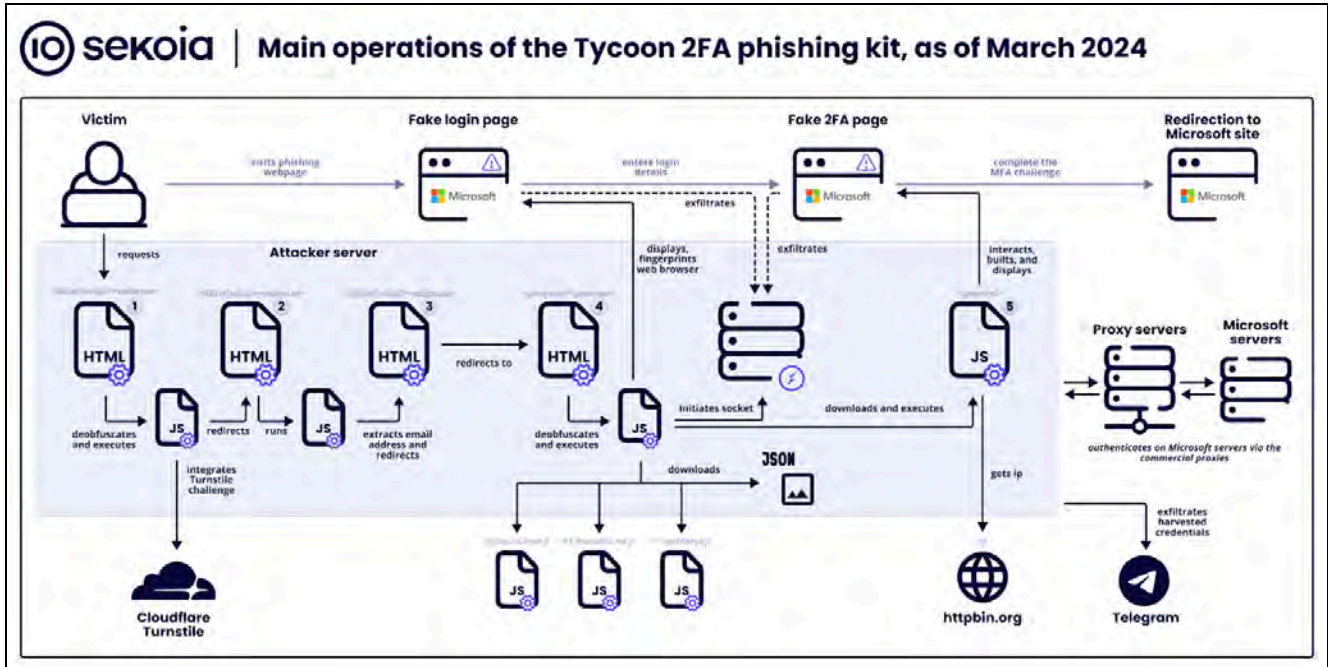


Figure 3: Overview of Tycoon 2FA infection chain (Source: Sekoia)

Although QR code phishing is often an opportunistic threat targeting a wide range of individuals and organizations, executives were disproportionately affected by these attacks. Data from Abnormal Security, for instance, [showed](#) that personnel in executive roles received 42 times more QR code attacks than other employees in the second half of 2023. This is not entirely surprising, as threat actors have long been targeting executives and high-level personnel with more or less tailored phishing messages, a technique called “whaling”, primarily due to those employees’ typically higher level of access to company resources. Abnormal Security also [reported](#) that a significant portion of malicious QR codes, approximately 27%, were used in phishing attacks impersonating 2/MFA notifications, almost certainly to generate a sense of urgency and prompt victims to take immediate action.

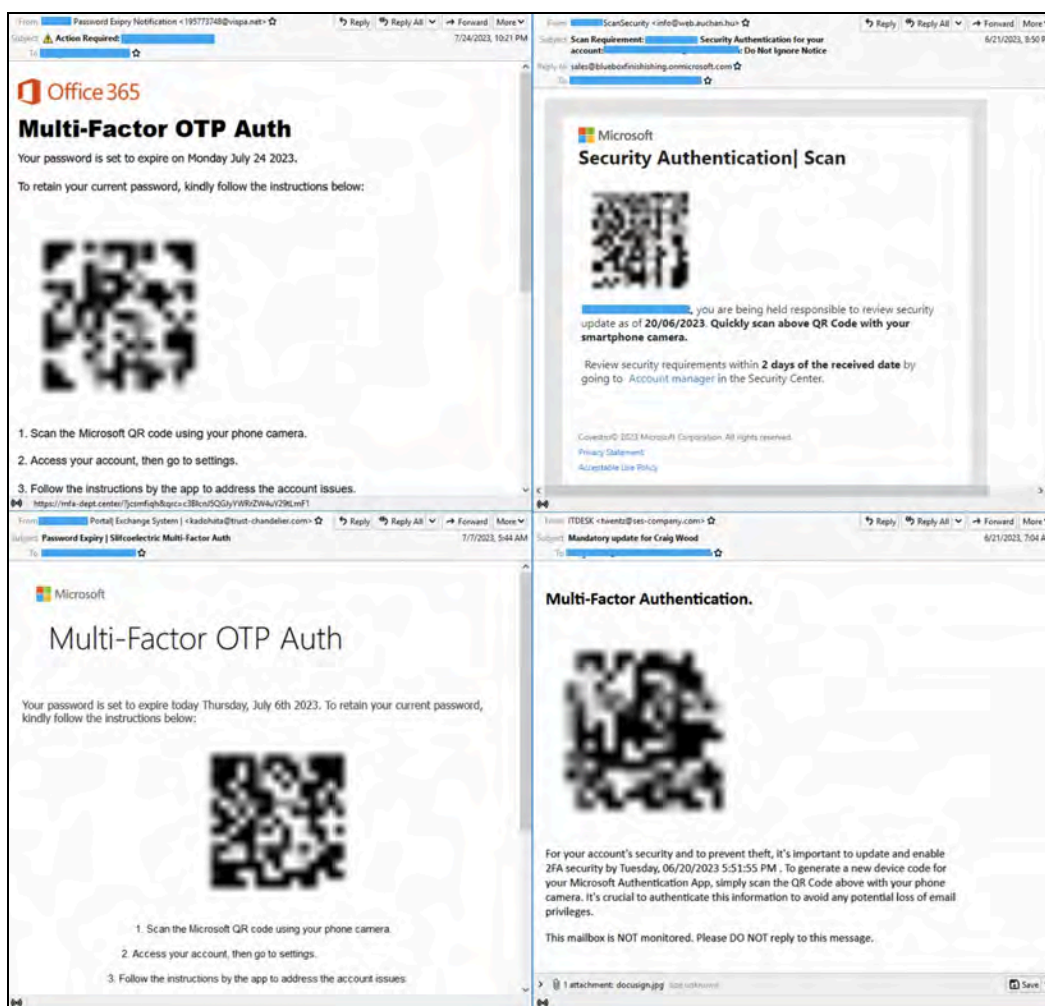


Figure 4: Examples of malicious QR codes impersonating MFA and security authentication notifications (Source: [Trustwave](#))

Although we do not believe that a single event in the broader security landscape triggered the observed uptick, several reasons almost certainly explain threat actors' increasing interest in using QR codes in phishing attacks. As previously mentioned, threat actors are capitalizing on the popularity of QR codes and taking advantage of users being used to encountering them in various contexts. Other, equally important, reasons almost certainly underpinning the observed trend include the following:

- Obfuscation:** QR codes add a layer of obfuscation that can help bypass traditional and static email security solutions and deceive users. Most defense software lacks the capability to scan QR codes. Their content is not readable by the human eye, meaning they have lower chances of raising immediate suspicion from recipients compared with URLs embedded within a phishing email's body and attachments.
- Exposure:** Scanning QR codes requires recipients to use their mobile devices, which can lack security software and fall outside the protection of the corporate environment. By using QR codes and pushing victims to use their mobile devices, threat actors can increase their chances

of avoiding security measures.

- **Versatility:** QR codes can encode various types of data, not just URLs, and can be used to trigger downloads, make phone calls, and initiate payments. In other words, they can provide threat actors with multiple avenues for social engineering attacks.
- **User Trust:** Surveys have shown that users generally perceive QR codes as safe, and lack awareness of their versatility and the many actions that can be triggered by scanning them [1, 2]. Threat actors can exploit this trust and lack of knowledge to their advantage.

Generative AI Likely Behind Spike in Phishing Attacks

In January 2024, the UK National Cyber Security Centre (NSCS) [assessed](#) that GenAI models such as ChatGPT provide capability uplift in social engineering to threat actors across the board, especially for less-skilled and opportunistic cybercriminals. Researchers and security experts have been [warning](#) for years about the risks associated with the dual-use nature of LLMs and their potential for facilitating phishing, especially since ChatGPT was publicly released in late November 2022 [1, 2, 3, 4]. On January 26, 2023, for example, Insikt Group [reported](#) observing threat actors on dark web and special-access forums sharing social engineering tutorials enabled by the use of ChatGPT only days after its launch. Additionally, threat actors were [observed](#) advertising malicious GenAI models on dark web and special-access forums throughout 2023, marketing them as being capable of bypassing ethical guardrails and generating phishing messages, among other functionalities. Examples include WormGPT, FraudGPT, WolfGPT, DarkBARD, DarkBERT, and DarkGPT.

Although Recorded Future did not observe wide-scale use of GenAI in phishing campaigns between Q4 2023 and Q1 2024, several security vendors argued that spikes in phishing activity observed throughout 2023 were partly due to threat actors' increasing adoption of LLMs. In November 2023, for example, SlashNext [reported](#) a 1,265% increase in phishing attacks between Q4 2022 and 2023, [attributing](#) the uptick to the public release of LLMs such as ChatGPT. Although we believe this correlation requires more data to indicate a causal link between GenAI and phishing volume, other vendors provided evidence of threat actors' use of LLMs for phishing purposes. In the latter half of 2023, Abnormal Security [reported](#) that 80% of 300 interviewed security stakeholders confirmed or strongly suspected that their organizations received AI-generated phishing emails, and [shared](#) five examples of phishing emails cybercriminals likely generated using LLMs. Furthermore, in February 2024, Microsoft and OpenAI reported that several state-sponsored groups used LLMs as part of their operations [1, 2]. These included the following:

- Charcoal Typhoon, a Chinese state-sponsored threat actor that overlaps with groups tracked as RedHotel, Aquatic Panda, ControlIX, and Bronze University, used LLMs for assistance with translations and communication, likely to establish connections with or manipulate targets.
- Emerald Sleet, a North Korean state-sponsored threat actor that overlaps with groups tracked as Kimsuky and Velvet Chollima, used LLMs to generate content likely for use in spearphishing

campaigns against organizations and individual experts on North Korea.

- Crimson Sandstorm, an Iranian state-sponsored threat actor that overlaps with groups tracked as Tortoiseshell, Imperial Kitten, and Yellow Liderc, interacted with LLMs to generate phishing emails, including messages that impersonated an international development agency and a pro-feminism website.

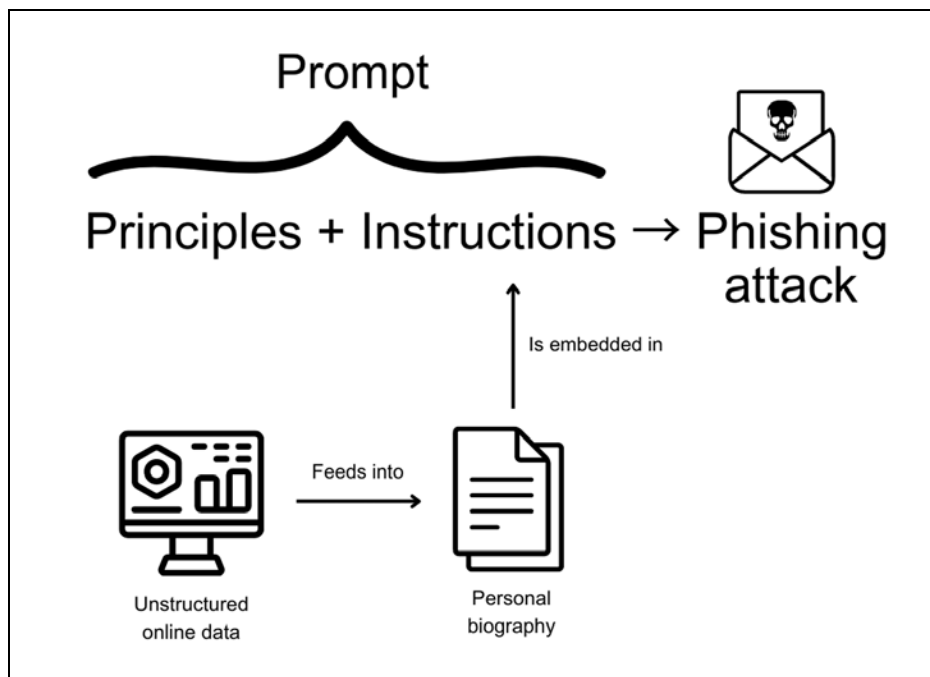


Figure 5: Example of the steps threat actors will typically follow when using LLMs to generate tailored phishing messages
(Source: [arXiv](#))

Threat actors' increasing interest in using LLMs for phishing almost certainly stems from the benefits such models can provide, such as the following prominent examples:

- **Improved and Customized Messages:** LLMs allow threat actors (particularly non-English speakers) to generate texts devoid of typos and other lexical and grammatical errors that would otherwise raise suspicion. They can also generate content that mimics legitimate communication styles and can be instructed to include information tailored to victims. In October 2023, IBM [reported](#) that phishing emails generated using LLMs proved almost as effective as emails written by a team of experienced social engineers in tricking recipients during a red team exercise.
- **Automation and Scalability:** LLMs can enable threat actors to automate the creation of phishing content, producing a variety of messages tailored to different recipients. Academic researchers, for instance, recently [observed](#) that threat actors were able to generate 1,000 phishing emails for approximately \$10 in under two hours by using Claude, an LLM that the US-based AI company Anthropic [released](#) publicly in March 2023. Similarly, IBM researchers [reported](#) that

they were able to generate convincing phishing emails using GenAI in just five minutes, while it typically takes them sixteen hours to do so manually.

Despite the advantages, LLM-generated phishing messages still rely on victims performing an action, such as interacting with a malicious link or attachment. LLMs have so far largely enhanced threat actors' existing capabilities, rather than allowing them to experiment with entirely novel phishing attack vectors. That said, academic research recently highlighted how GenAI models can become both the enablers and targets of new phishing techniques. This was the case with Morris II, a proof-of-concept (PoC) zero-click worm designed by researchers from the Technion Israel Institute of Technology, Intuit, and Cornell Tech, presented in a whitepaper [published](#) on March 4, 2024. Morris II, which takes its name from the 1988 [Morris worm](#), is capable of targeting GenAI email assistants and propagating across such agents without the need for user interaction. It does this by embedding prompts in phishing emails designed to instruct a target AI assistant to fetch malicious data that corrupts its internal database. The malicious prompts effectively jailbreak the AI assistant and instruct it to share the same instructions with other hosts using similar GenAI technologies, allowing for Morris II to propagate.

Although Morris II remains a PoC rather than an attack vector observed in the wild, the phishing landscape is adjusting in other ways to organizations' increased adoption of machine learning (ML) in email solutions. In mid-March 2024, SlashNext [reported](#) observing phishing attacks that employed a new technique it dubbed "Conversation Overflow" to bypass ML-powered email security controls in order to target executives with malicious login pages. According to SlashNext, in a Conversation Overflow attack, phishing emails are split into two sections: an upper part readily visible to recipients and urging them to take action and a lower, partly hidden part filled with seemingly benign text. The text in the lower part, which is separated from the top by a significant amount of blank space, mimics normal, harmless communication, and exploits ML systems' reliance on identifying deviations from known and standard behaviors, effectively bypassing security filters. The Conversation Overflow attack technique demonstrates how AI and ML solutions also introduce new security considerations and challenges that threat actors are already taking advantage of. It also shows that attackers do not necessarily need to rely on LLMs themselves to pose a threat to organizations, such as by using such tools to craft convincing phishing messages.

Threat Actors Use AWS SNS and VAST Tags to Scale Up Operations

In addition to the uptick in QR code phishing and threat actors' increased use of GenAI to craft malicious messages, threat actors debuted two new techniques to scale up and broaden their operations in Q4 2023 and Q1 2024. The first entailed using Amazon Web Services (AWS) Simple Notification Service (SNS) to send malicious SMS Messages in bulk (smishing).

According to SentinelLabs, which first [reported](#) on the malicious script on February 15, 2024, the SNS Sender script marked the first case of AWS SNS being used for phishing purposes. Previous tools like AlienFox were observed [using](#) business-to-customer (B2C) communications platforms such as Twilio for smishing.

SNS Sender requires access to an AWS account in which SNS is already provisioned, configured, and enabled, in order to function correctly. This requirement, however, is somewhat easily met, as users can remove default restrictions to AWS accounts enforced through a feature called [SMS sandbox](#) by spending \$1 and providing a viable use case to AWS support. Other parameters SNS Sender accepts include phone numbers to target, the message content, and a sender ID. Notably, the inclusion of a sender ID contrasts with SNS Sender's targeting of US citizens through messages impersonating the United States Postal Service (USPS). As also stated on the AWS official documentation [page](#), support for sender IDs varies by country, and carriers in the US do not support sender IDs at all. Based on this evidence, we suspect that the threat actor behind the script likely resides in a country where using a sender ID is commonplace, such as India.

According to SentinelLabs, a threat actor known by the moniker "ARDUINO_DAS" is responsible for creating SNS Sender. ARDUINO_DAS is well-known in the phishing kit landscape, having authored over 150 phishing kits, although they seemingly abandoned this moniker in 2023 after having been accused of defrauding buyers.

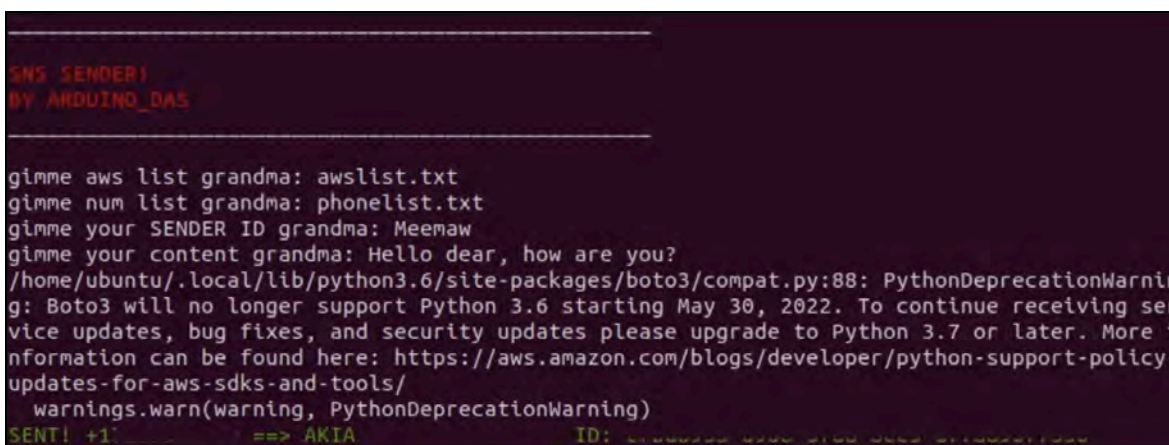
A screenshot of a terminal window with a dark background and light-colored text. The text shows a series of prompts and responses for a script named 'SNS SENDER'. The prompts are in red and the responses are in green. The script asks for AWS list, phone numbers, sender ID, and content. A Python deprecation warning is visible, and the final output shows 'SENT! +1' and 'ID: AKIA'.

Figure 6: SNS Sender inputs and outputs (Source: [SentinelLabs](#))

The second technique was introduced by Ghostcat, a financially motivated and likely China-based threat actor also known as ScamClub, which has been [active](#) since 2018. The group is known for undermining the reputation of Demand-Side-Platforms (DSPs), Supply-Side-Platforms (SSPs), and publishers, by abusing ad platforms to stage large malvertising campaigns. As [reported](#) by The Media Trust on February 5, 2024, in late 2023 and early 2024, Ghostcat ramped up their activity, shifting to using Video Ad Serving Templates (VAST) tags to deliver malicious links through video players and redirect victims to phishing pages. In doing so, Ghostcat was able to reach millions of consumers, while evading header- or wrapper-based malware-blocking scripts.

VAST is a set of standards [developed](#) by the Interactive Advertising Bureau (IAB) in 2008 to facilitate the consistent delivery and management of video ads across different media players and platforms. VAST [standardizes](#) the communication between video players and ad servers by using an eXtensible

Markup Language (XML) schema, enabling the efficient serving of video ads, tracking of viewer interactions, and collection of metrics across devices and platforms. This allows advertisers to deploy their video campaigns more reliably and measure their effectiveness with greater accuracy.

In one particular instance, The Media Trust [observed](#) Ghostcat embedding URLs within a VAST tag designed to execute a script hosted on *azureedge[.]net* that, while mostly containing video player code, triggered a POST request to the domain *trackmenow[.]life*. The request was laden with form data containing detailed fingerprinting information about victims' devices, such as screen dimensions, window properties, current URL, browser cookies, and timezone. This is information that allowed Ghostcat to gather information on potential targets and tailor their attacks accordingly. The response from *trackmenow[.]life* contained a redirect URL. Multiple obfuscated scripts then ensured victims were ultimately redirected to phishing pages, such as a fake McAfee virus alert hosted on *securitypatch[.]life*.

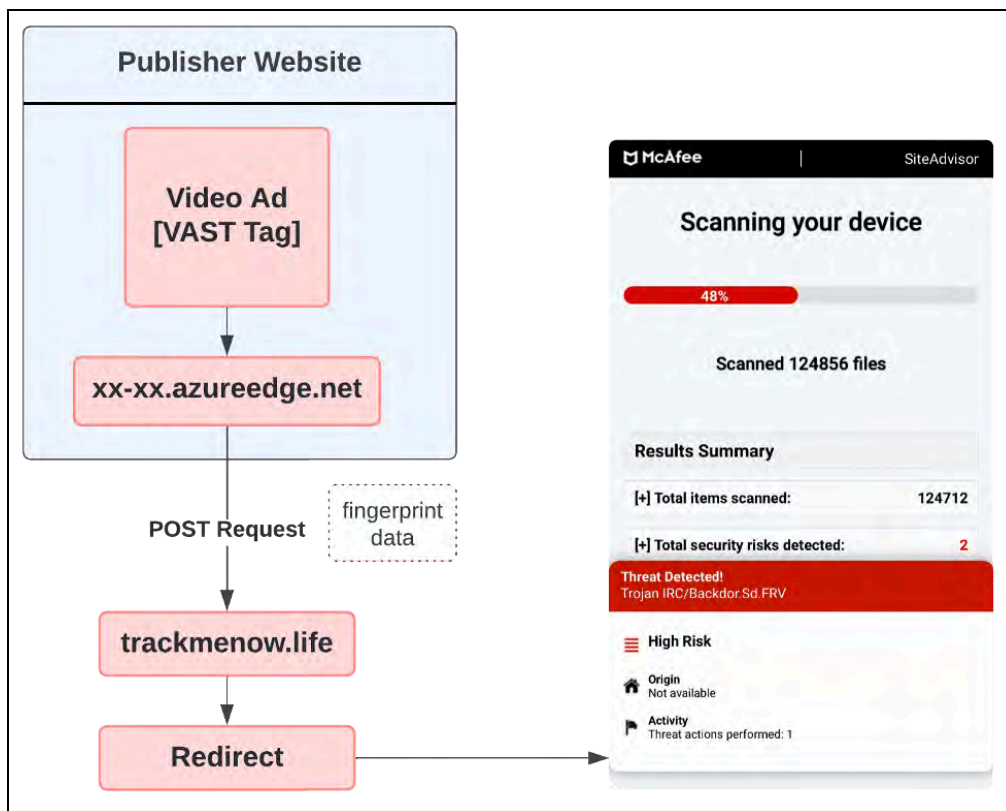


Figure 7: Overview of Ghostcat's use of malicious VAST tags (Source: [The Media Trust](#))

Mitigations

Organizations can use the following measures to mitigate against the key threats discussed in this report.

QR Code Phishing

- **Employee Education:** Organizations should conduct regular training sessions and phishing simulations incorporating QR code-based scenarios to help users identify and report suspicious QR codes.
- **Secure QR Code Scanning Apps:** Organizations and users can use QR code scanning apps that incorporate security features such as URL filtering and the ability to check links against a database of known malicious sites before accessing them. These apps help detect malicious QR codes and prevent recipients from being redirected to phishing websites or downloading harmful software.
- **Endpoint Security Solutions:** Organizations can enhance the security of mobile devices used within the corporate environment with comprehensive endpoint security solutions. This includes the use of mobile device management (MDM) systems that enforce security policies, manage device security features, and provide the ability to remotely wipe lost or stolen devices. Additionally, although Android and iOS phones feature built-in protection, individual users can strengthen the security of their mobile devices by installing third-party antivirus solutions.
- **2/MFA:** Implementing phishing-resistant 2/MFA solutions, such as FIDO/WebAuthn authentication or public key infrastructure (PKI)-based MFA, can help organizations and individuals add a layer of security to their corporate and personal devices. Although malicious QR codes have been implemented in phishing attacks seeking to capture 2/MFA tokens, using multiple authentication methods remains a viable mitigation against the technique.
- **Recorded Future Threat Intelligence:** Recorded Future customers can use [Threat Intelligence](#) to stay abreast of the latest QR code phishing incidents, mobile malware campaigns, and relevant indicators of compromise (IoCs) using relevant queries (such as for references to cyberattacks involving QR codes, QR codes and phishing, or mobile malware).

AI-Powered Phishing

- **Advanced Machine Learning Detection:** Detecting whether phishing messages have been written using LLMs [remains](#) challenging. Advanced machine learning detection systems, however, can help mitigate the threat, offering [several advantages](#) over traditional signature- and rule-based systems, such as access to contextual, linguistic, attachments, and behavioral

analysis.

- **Training and Awareness:** Since LLMs allow threat actors to generate more grammatically and syntactically correct messages, training programs should place increased emphasis on teaching employees to spot evidence of phishing beyond typos, such as suspicious senders and URLs.
- **Recorded Future Brand Intelligence:** Recorded Future customers can use [Brand Intelligence](#) to maintain real-time visibility into potential instances of brand impersonation and quickly initiate [takedown requests](#) of fraudulent domains and websites.

AWS SNS Smishing

- **Endpoint Security Solutions:** As with QR code phishing, implementing a reputable MDM platform can help to centralize control over mobile devices and enforce security settings that block SMS messages from unknown or untrusted senders.
- **SMS Filtering Technology:** SMS filtering technology can identify malicious SMS messages by analyzing links and language. More advanced SMS filtering services can also implement machine learning algorithms to adapt and improve their detection capabilities over time, further mitigating against evolving smishing techniques.
- **Training and Awareness:** As with QR code and AI-powered phishing, smishing can be mitigated by regularly educating employees about the risks and common techniques associated with malicious SMS messages, and how to report them promptly.
- **Recorded Future Threat Intelligence:** Recorded Future customers can use [Threat Intelligence](#) to monitor and be alerted of new smishing incidents potentially involving the abuse of AWS SNS and other services using relevant queries (such as for references to cyberattacks involving smishing).

VAST Tags Malvertising

- **VAST Tag Validation and Sanitization:** Thoroughly validating VAST tags before they are integrated into ad-serving environments can help determine whether they contain malicious code or links. Automated tools that scan and verify the integrity and safety of VAST tags can do this.
- **Secure Video Player:** Using video players capable of detecting and blocking suspicious activities initiated by VAST tags can help shield users from malvertising and other phishing attacks perpetrated through ads. This can be achieved by using malware sandboxes that isolate the execution of ads from the main device.

- **Recorded Future Intelligence Cloud:** Recorded Future customers can use several indicators offered by the [Recorded Future Intelligence Cloud](#), such as Risk Scores and triggered risk rules, as an additional source of truth when investigating unfamiliar domains embedded in VAST tags.

Outlook

Whether or not techniques such as QR code phishing, AWS SNS smishing, and VAST tags malvertising, will remain prevalent going forward almost certainly depends on the value they can keep offering to threat actors. So far, they have allowed attackers to effectively broaden their reach, bypass security solutions, and evade suspicion. Although it is almost certain that threat actors will continue using QR codes, AWS SNS, and VAST tags for the remainder of 2024, their popularity might decrease if security solutions catch up and users' awareness improves. For example, while malicious QR codes offer threat actors many advantages, including obfuscation and versatility, some security vendors have already [started](#) marketing email gateways that use machine learning models to analyze and detect malicious QR codes. In the short term, however, the abuse of AWS SNS is the technique most likely to decline. This is due to the constraints threat actors need to overcome to abuse the service — such as gaining access to an AWS SNS tenant properly configured to send SMS messages — and the potential additional security mechanisms Amazon can implement to make the service less prone to exploitation.

On the other hand, threat actors will almost certainly continue increasing their use of LLMs to scale up operations and more easily tailor phishing messages to victims, implementing new ways to jailbreak LLMs and using readily available models tuned to their specific phishing requirements. LLMs are already being used to counter GenAI-powered phishing attacks, such as by [analyzing](#) patterns in LLM-generated text to enhance the detection of malicious messages. Although the advantage currently lies with attackers, new advancements in security will almost certainly give defenders equal footing in the near to medium term.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: [Analytic Standards](#) (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

[Learn more at recordedfuture.com](https://www.recordedfuture.com)