Token

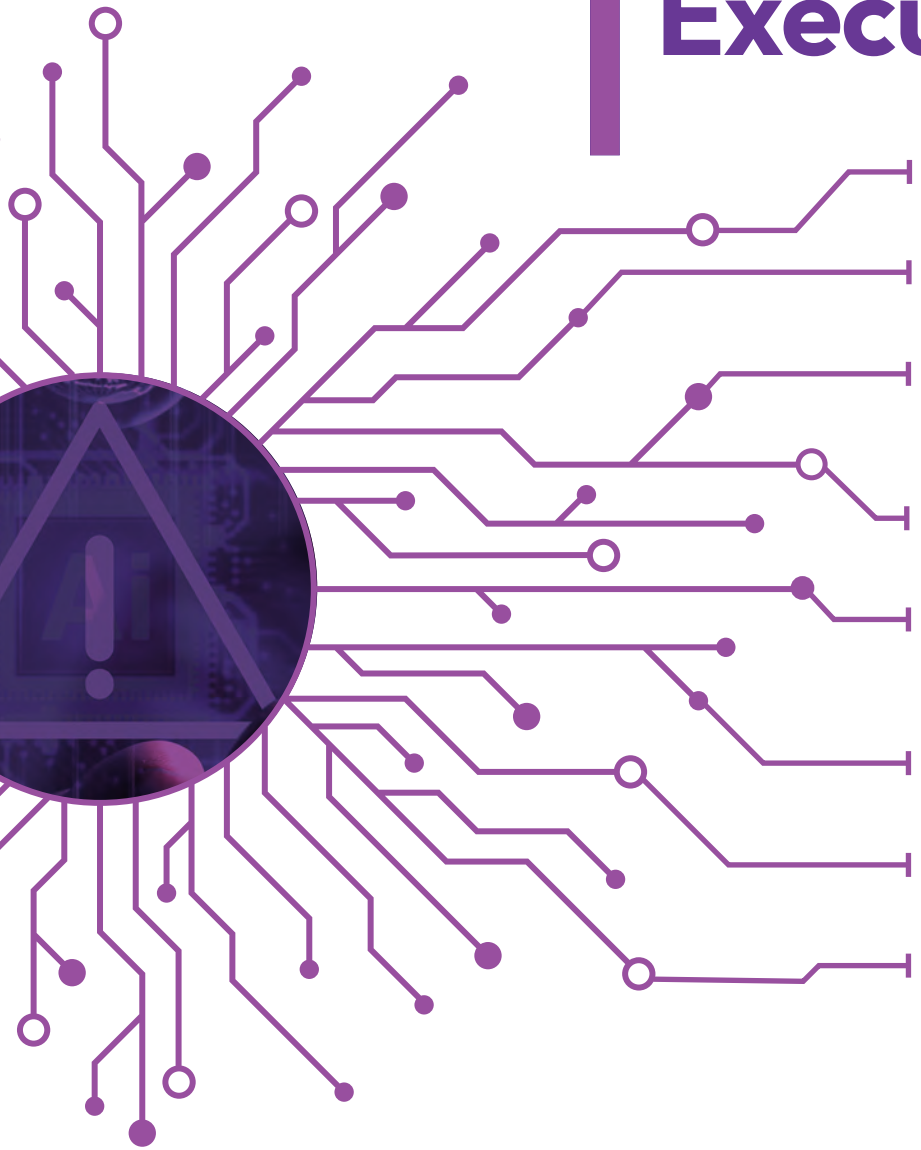
eBook

Generative AI: A Game Changer for Security and Hacker Strategy

How threat actors are using Generative AI to make phishing more dangerous, and how next-generation wearable MFA is fundamentally disrupting the battle to keep cybercriminals from breaching networks

Contents

1 Executive Summary



Cybercriminals favor targeting human users, the weakest link in cybersecurity, due to their susceptibility to manipulation and social engineering.

Generative Artificial Intelligence (GenAI) exacerbates human factor exploitation by mimicking human behavior at scale.

Phishing is by far the leading cause of data breaches. In a Splunk study, 96% of respondents encountered a ransomware attack, of which over half (52%) described the impact on their business systems and operations as significant.

Phishing extends beyond email to text messages, messaging platforms, social media, collaboration tools, and voice assistants.

GenAI tools like ChatGPT enable highly convincing and personalized phishing messages that can be impossible to detect, alongside highly targeted phishing campaigns with custom-tailored messages for specific victims.

Traditional phishing detection tools increasingly struggle to identify GenAI-generated phishing messages.

A paradigm shift focuses on eliminating the need for credentials to mitigate a primary motive for phishing attacks.

Next-generation Multi-Factor Authentication (MFA) from Token disrupts the credential attack surface by rendering stolen passwords useless and eliminating the vulnerabilities of legacy MFA — enhancing overall cybersecurity.

2 The Weakest Link in the Security Chain: People

Cybercrime has become a daily reality for organizations of all sizes, and cybercriminals have become more sophisticated in their methods. Many have learned to bypass increasingly robust cybersecurity technology, turning their attention instead to the weakest link in the security chain — human users.

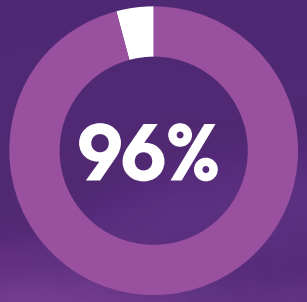
Unlike technology, people are susceptible to deception and social engineering. Technology and systems can be fortified with security measures — human weaknesses cannot. For ages, criminals have exploited human traits like curiosity and trust, and cybercriminals are no different.

The rise of Generative Artificial Intelligence (GenAI) — with its many benefits — has exacerbated the exploitation of the human factor by cybercriminals. Combining the capabilities of artificial intelligence with generative models, GenAI can understand, create, and adapt content in a human-like manner — transforming the cyber threat landscape. Human behavior can now be imitated in a lifelike manner, in real time, and at scale. And nowhere are cybercriminals putting this to more nefarious use than in phishing attacks.

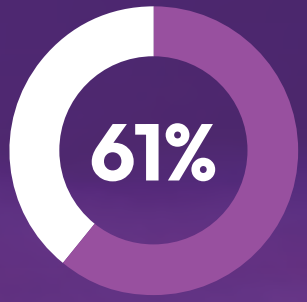
800K
cybercrime complaints reported to the FBI in 2022[1]

40%
of complaints were about phishing attacks

$10 Billion
monetary losses from phishing attacks



Percentage of companies that report falling victim to at least one phishing attack a year[2]



Year-over-year increase in phishing attacks in the second half of 2022

1 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof#:~:text=the%20following%20sections.-,Phishing%20attacks%20are%20common,successful%20phishing%20attack%20last%20year.

3 Phishing: Wildly Popular Threat Vector

Phishing stands out as the most common social engineering attack vector. Phishing involves the use of deceptive emails, messages, or websites that trick users into revealing sensitive information — login credentials, one-time passwords, personal information, financial data and more. The rapid growth in phishing incidents underscores the constantly evolving tactics employed by cybercriminals to deceive and exploit unsuspecting individuals and organizations.

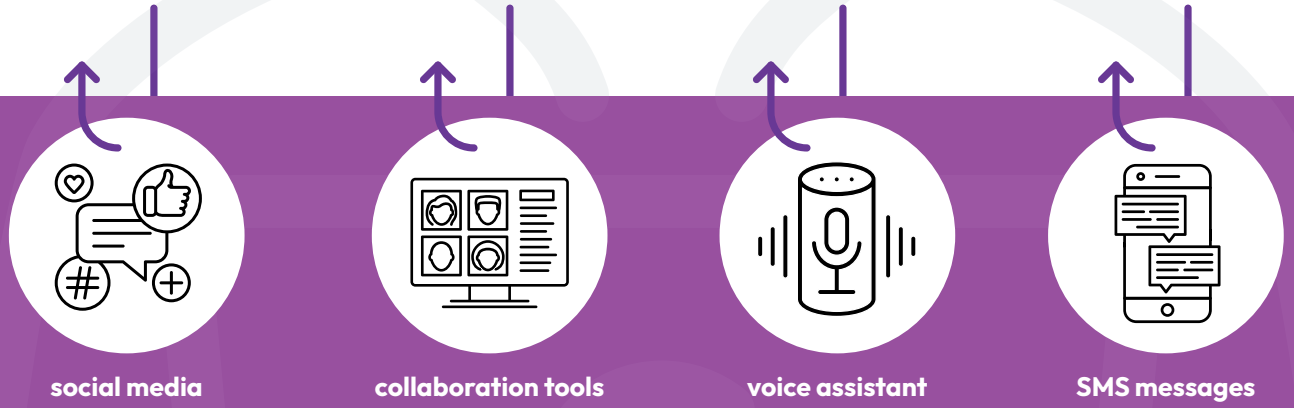
And it's working. Of over 800,000 cybercrime complaints reported to the FBI last year, nearly 40% were about phishing attacks — resulting in monetary losses exceeding $10 billion. An astonishing 96% of companies report falling victim to at least one phishing attack a year. And the scale of the phishing problem continues to escalate — with a remarkable 61% year-over-year increase in phishing attacks in the second half of 2022.

4 Phishing:
Not Just Email Anymore

Attackers are continuously adapting their tactics to exploit new vectors, beyond traditional email-based phishing.

While email phishing remains prevalent, cybercriminals are diversifying. They're increasingly targeting individuals and organizations through text messages, messaging platforms and other popular communication channels — WhatsApp, Signal, SMS, and more. In messaging-based phishing attacks, attackers craft convincing messages that imitate legitimate communications from ostensibly trusted sources yet contain links to malicious websites or attachments that contain malware.

Attackers have also begun exploiting vectors like social media platforms, collaboration tools like Slack and Microsoft Teams, and even voice assistants. On social media, threat actors craft deceptive messages to manipulate users into sharing sensitive information or clicking on malicious links. Collaboration platforms are targets for malicious attachments or messages posing as legitimate files. Even voice assistants can be tricked into executing commands that compromise security.



While email phishing remains prevalent, cybercriminals are diversifying.

5 Generative AI:
Smarter, Nearly Undetectable Phishing

Phishing threat actors are increasingly harnessing the power of Generative AI (GenAI) tools like ChatGPT to create more seductive, more convincing, and more realistic phishing messages.

GenAI models enable cybercriminals to generate text that is indiscernible from normal human communication. This makes it extremely challenging for recipients to tell the difference between genuine and fake messages. These highly personalized and context-aware messages help attackers manipulate victims into taking actions that compromise security.

What's more, GenAI tools are enabling cybercriminals to conduct highly targeted phishing campaigns at scale. Threat actors can now automate the generation of thousands of custom-tailored phishing messages for a wide range of victims. These are messages designed to exploit specific user interests, demographics, or past behaviors — creating a false sense of trust and making attacks more likely to succeed.

Traditional phishing detection tools, which rely on pattern recognition and known indicators of phishing, are missing most of the phishing messages created by GenAI. GenAI content lacks the usual telltale signs — including misspellings or generic language — rendering the majority of legacy security measures ineffective.

6 No Credentials, No Battle

The explosion in scale and sophistication of GenAI-powered phishing attacks begs the question:

Can increasingly human-like content truly be reliably detected by defensive paradigms?

In text, images, audio and video — AI-driven content blurs the boundary between genuine and fraudulent communication to a degree where it is nearly impossible to differentiate between them. In other words, is the battle against phishing lost?

Owing to this, more and more companies are choosing to eliminate one of phishing's primary objectives instead of battling phishing as an attack vector. They're taking immediate steps to eliminate the need for credentials.

"No credentials, no battle" is a promising paradigm shift in the fight against phishing attacks. By reducing or even eliminating reliance on traditional username-password credentials, organizations can significantly lower the impact of successful phishing attacks.

7 Passwordless Solutions Fall Short

Passwordless authentication relies on alternatives to traditional credential-based logins like one-time passwords, registered smartphones, or biometrics. While passwordless login is considered more secure than traditional password-based authentication, it has serious limitations:

Biometric data vulnerabilities — Passwordless login solutions that don't properly protect biometric data are vulnerable to compromise. Once an attacker gains access to a user's biometric data, it can't be changed like a password — potentially leading to permanent identity theft. Storing biometric data in a Secure Element in a device that has no Wi-Fi or cellular data access is essential.

Phishing and social engineering — While passwordless methods are more secure against traditional password-based attacks, they are not immune to phishing and social engineering attacks. Attackers can trick users into providing biometric data or approving login requests on malicious websites or apps.

Device trustworthiness — Passwordless methods often rely on the security of the device being used. If a device is lost, stolen, or compromised, it can be used to gain unauthorized access to an account.

For these reasons and more, security-conscious companies are seeking new paradigms to close the credentials security gap — new paradigms like next-generation multi-factor authentication.

8 Next-Generation MFA:
Disrupting the Credential Attack Surface

Next-generation Multi-Factor Authentication (MFA) is a powerful and effective tool in the fight against credential phishing attacks — fundamentally disrupting the credential attack surface.

Next-generation MFA replaces static and vulnerable credentials, alongside legacy MFA solutions that are subject to Adversary-in-the-Middle attacks and MFA-bombing attacks. The next-generation MFA paradigm relies on a physical device (ideally an always-accessible wearable hardware token like the Token Ring) that eliminates the vulnerabilities of humans and BYOD devices — making it phishing-proof and hack-proof.

By nullifying the value of stolen credentials and eliminating the vulnerabilities of legacy MFA, next-generation MFA eliminates key attack surfaces for organizations — freeing up security resources for other, more pressing threats. This offers peace of mind for individuals and makes life far more difficult for cybercriminals — enhancing overall cybersecurity.

9 Token Ring:
Next-Generation Wearable MFA

Token Ring is a cutting-edge biometric wearable that delivers ultra-strong next generation MFA to protect organizations against phishing attacks, BYOD vulnerabilities, lost and stolen credentials, weak passwords, credential stuffing, and easily stolen SMS one-time passcodes. It also prevents remote attacks leveraging unbreakable NFC proximity security technology.

Unlike traditional MFA, attackers simply can't bypass Token Ring with malware, MFA fatigue attacks, adversary-in-the-middle (AiTM) attacks, and others. Since it always remains with the user, Token Ring is constantly safe and immediately available for authentication. Only the authorized user can use the device and no attacker can access the secrets and keys stored on it. Since biometrics never leave the ring, they can never be stolen.

Token Ring Benefits:

- Only the authorized person can use the device for network access
- A wearable ring is less likely to be lost or misplaced like a dongle — meaning fewer help desk calls and fewer replacements
- Biometrics never leave the ring — they cannot be stolen from a phone or server
- Secrets and keys are stored on the ring in a Secure Element — and cannot be accessed by an attacker

Token

Token

tokenring.com | (866) 328-7464

About Token

In a world of stolen identities and compromised user credentials, Token is changing the way organizations secure access to their digital realms by providing passwordless, biometric, next generation multifactor authentication solutions. To learn more, **visit www.tokenring.com**.

EB-GENERATIVE AI-1.0