Defending against evolving identity attack techniques | Microsoft Security Blog

By Igor Sakhnov

Published: 2025-05-29 · Archived: 2026-04-05 13:51:13 UTC

In today's evolving cyber threat landscape, threat actors are committed to advancing the sophistication of their attacks. The increasing adoption of essential security features like multifactor authentication (MFA), passwordless solutions, and robust email protections has changed many aspects of the phishing landscape, and threat actors are more motivated than ever to acquire credentials—particularly for enterprise cloud environments. Despite these evolutions, social engineering—the technique of convincing or deceiving users into downloading malware, directly divulging credentials, or more—remains a key aspect of phishing attacks.

Implementing phishing-resistant and passwordless solutions, such as passkeys, can help organizations improve their security stance against advanced phishing attacks. Microsoft is dedicated to enhancing protections against phishing attacks and making it more challenging for threat actors to exploit human vulnerabilities. In this blog, I'll cover techniques that Microsoft has observed threat actors use for phishing and social engineering attacks that aim to compromise cloud identities. I'll also share what organizations can do to defend themselves against this constant threat.

While the examples in this blog do not represent the full range of phishing and social engineering attacks being leveraged against enterprises today, they demonstrate several efficient techniques of threat actors tracked by Microsoft Threat Intelligence. Understanding these techniques and hardening your organization with the guidance included here will help contribute to a significant part of your defense-in-depth approach.

Pre-compromise techniques for stealing identities

Modern phishing techniques attempt to defeat authentication flows

Adversary-in-the-middle (AiTM)

Today's authentication methods have changed the phishing landscape. The most prevalent example is the increase in adversary-in-the-middle (AiTM) credential phishing as the adoption of MFA grows. The phish kits available from phishing-as-a-service (PhaaS) platforms has further increased the impact of AiTM threats; the Evilginx phish kit, for example, has been used by multiple threat actors in the past year, from the prolific phishing operator Storm-0485 to the Russian espionage actor Star Blizzard.

Evilginx is an open-source framework that provides AiTM capabilities by deploying a proxy server between a target user and the website that the user wishes to visit (which the threat actor impersonates). Microsoft tracked Storm-0485 directing targets to Evilginx infrastructure using lures with themes such as payment remittance, shared documents, and fake LinkedIn account verifications, all designed to prompt a quick response from the

recipient. Storm-0485 also consistently uses evasion tactics, notably passing initial links through obfuscated Google Accelerated Mobile Pages (AMP) URLs to make links harder to identify as malicious.

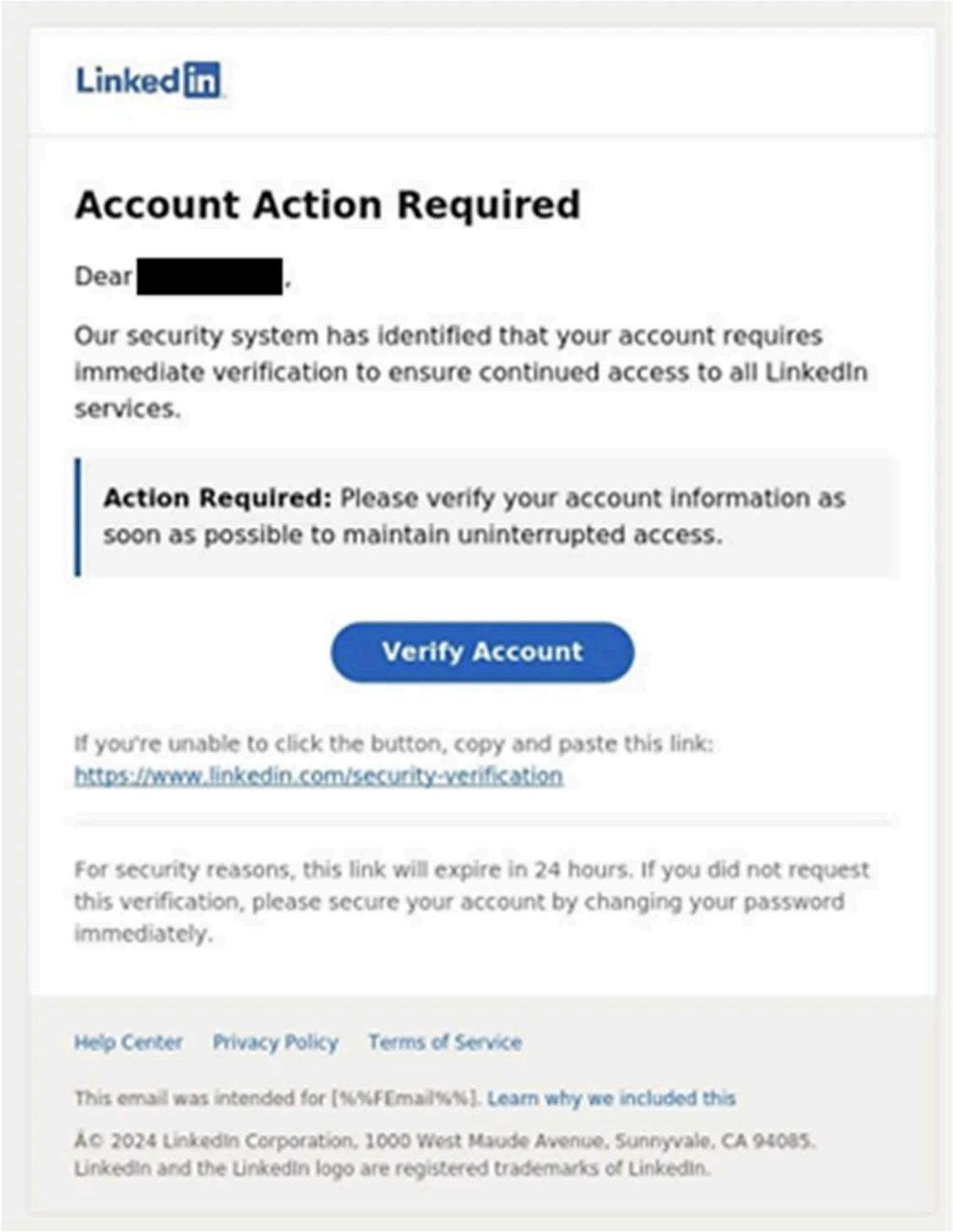


Figure 1. Example of Storm-0485's fake LinkedIn verify account lure

To protect against AiTM attacks, consider complementing MFA with risk-based Conditional Access policies, available in Microsoft Entra ID Protection, where sign-in requests are evaluated using additional identity-driven signals like IP address location information or device status, among others. These policies use real-time and offline detections to assess the risk level of sign-in attempts and user activities. This dynamic evaluation helps mitigate risks associated with token replay and session hijacking attempts common in AiTM phishing campaigns.

Additionally, consider implementing Zero Trust network security solutions, such as Global Secure Access which provides a unified pane of glass for secure access management of networks, identities, and endpoints.

Device code phishing

Device code phishing is a relatively new technique that has been incorporated by multiple threat actors into their attacks. In device code phishing, threat actors like Storm-2372 exploit the device code authentication flow to capture authentication tokens, which they then use to access target accounts. Storm-1249, a China-based espionage actor, typically uses generic phishing lures—with topics like taxes, civil service, and even book pre-orders—to target high-level officials at organizations of interest. Microsoft has also observed device code phishing being used for post-compromise activity, which are discussed more in the next sections.

At Microsoft, we strongly encourage organizations to block device code flow where possible; if needed, configure Microsoft Entra ID's device code flow in your Conditional Access policies.

OAuth consent phishing

Another modern phishing technique is OAuth consent phishing, where threat actors employ the Open Authorization (OAuth) protocol and send emails with a malicious consent link for a third-party application. Once the target clicks the link and authorizes the application, the threat actor gains access tokens with the requested scopes and refresh tokens for persistent access to the compromised account. In one OAuth consent phishing campaign recently identified by Microsoft, even if a user declines the requested app permissions (by clicking Cancel on the prompt), the user is still sent to the app's reply URL, and from there redirected to an AiTM domain for a second phishing attempt.

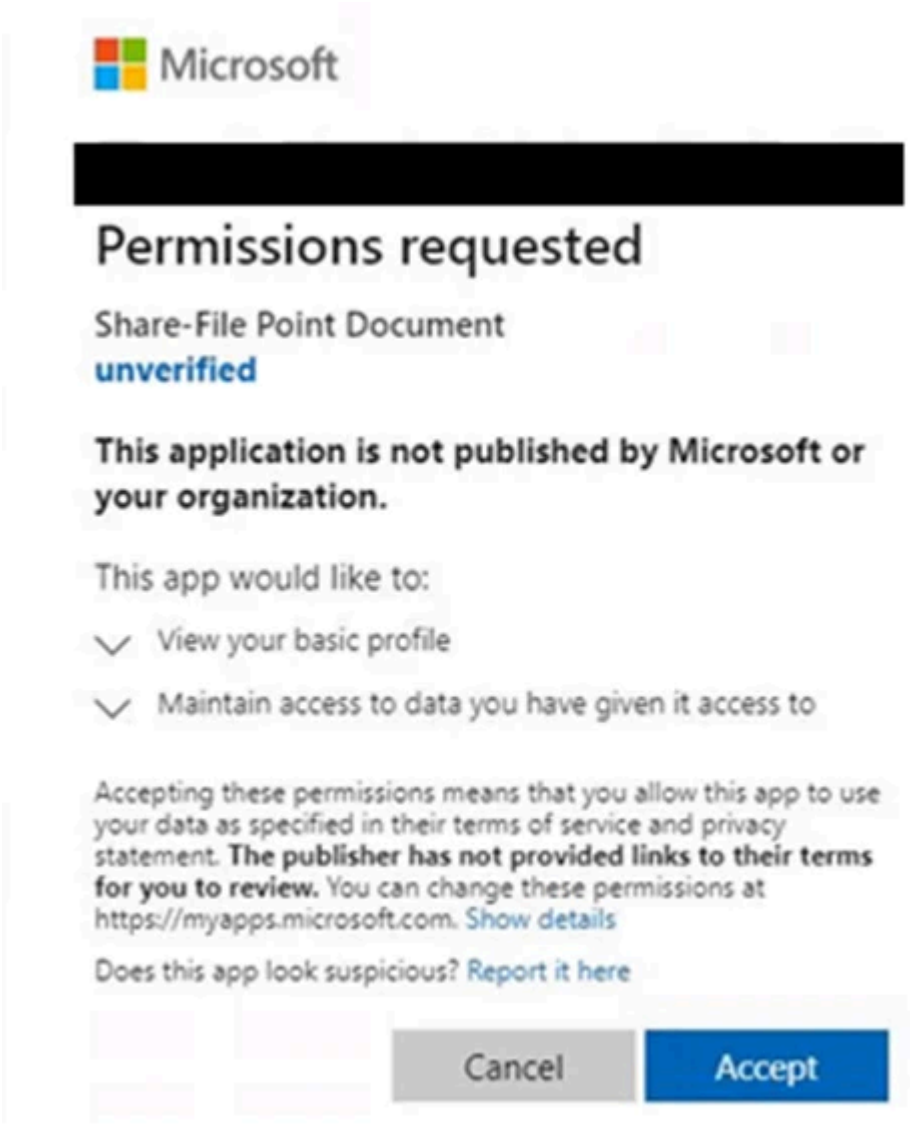


Figure 2. OAuth app prompt seeks account permissions

You can prevent employees from providing consent to specific apps or categories of apps that are not approved by your organization by configuring app consent policies to restrict user consent operations. For example, configure policies to allow user consent only to apps requesting low-risk permissions with verified publishers, or apps registered within your tenant.

Device join phishing

Finally, it's worth highlighting recent device join phishing operations, where threat actors use a phishing link to trick targets into authorizing the domain-join of an actor-controlled device. Since April 2025, Microsoft has observed suspected Russian-linked threat actors using third-party application messages or emails referencing upcoming meeting invitations to deliver a malicious link containing valid authorization code. When clicked, the link returns a token for the Device Registration Service, allowing registration of the threat actor's device to the tenant. You can harden against this type of phishing attack by requiring authentication strength for device registration in your environment.

Lures remain an effective phishing weapon

While both end users and automated security measures have become more capable at identifying malicious phishing attachments and links, motivated threat actors continue to rely on exploiting human behavior with convincing lures. As these attacks hinge on deceiving users, user training and awareness of commonly identified social engineering techniques are key to defending against them.

Impersonation lures

One of the most effective ways Microsoft has observed threat actors deliver lures is by impersonating people familiar to the target or using malicious infrastructure spoofing legitimate enterprise resources. In the last year, Star Blizzard has shifted from primarily using weaponized document attachments in emails to spear phishing with a malicious link leading to an AiTM page to target the government, non-governmental organizations (NGO), and academic sectors. The threat actor's highly personalized emails impersonate individuals from whom the target would reasonably expect to receive emails, including known political and diplomatic figures, making the target more likely to be deceived by the phishing attempt.

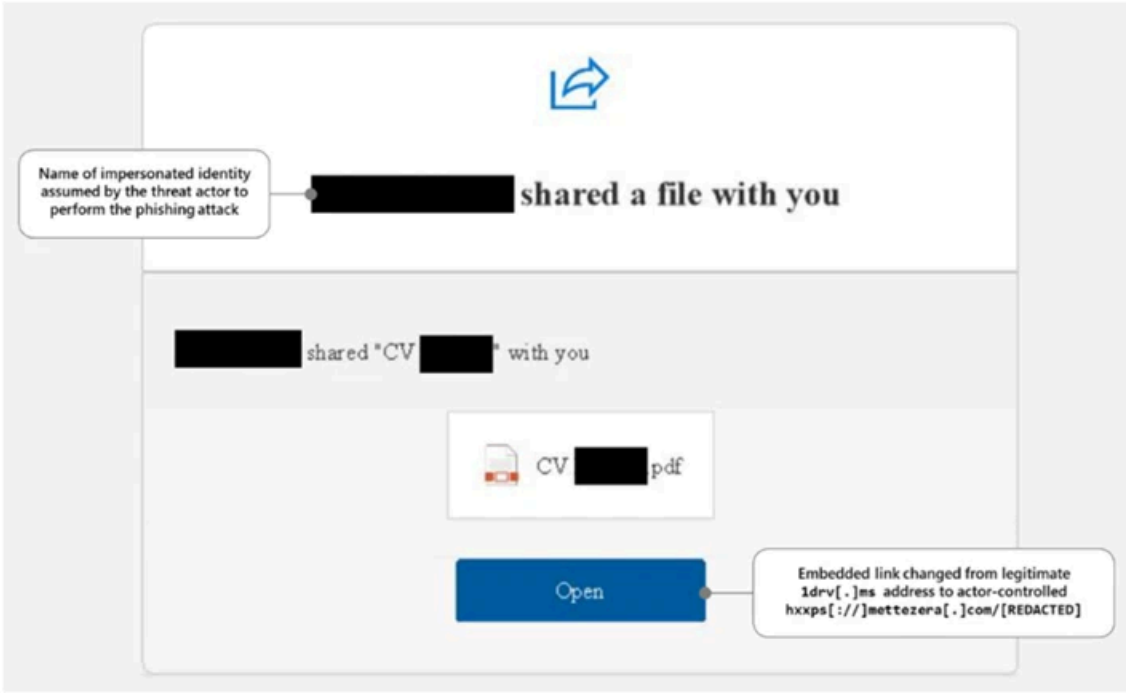


Figure 3. Star Blizzard file share spear-phishing email

QR codes

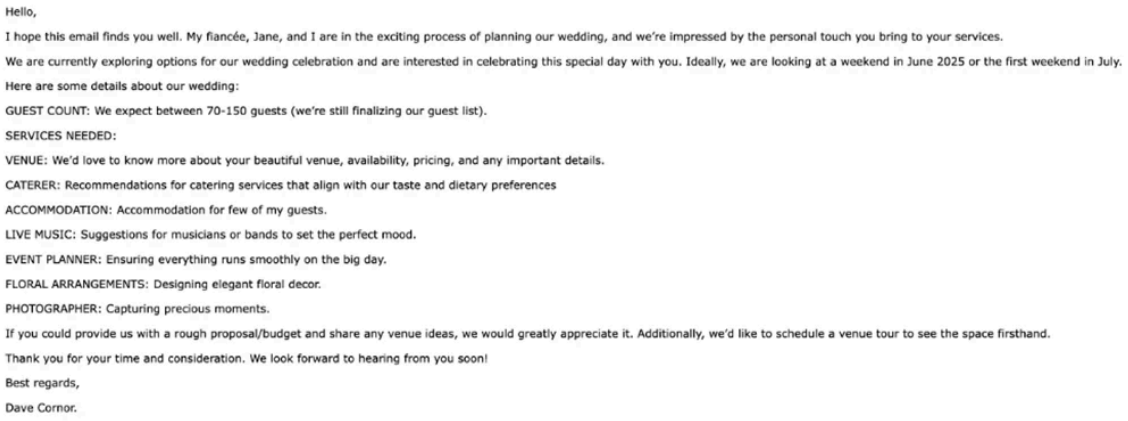
We have seen threat actors regularly iterating on the types of lure links incorporated into their attacks to make social engineering more effective. As QR codes have become a ubiquitous feature in communications, threat actors have adopted their use as well. For example, over the past two years, Microsoft has seen multiple actors incorporate QR codes, encoded with links to AiTM phishing pages, into opportunistic tax-themed phishing campaigns.

The threat actor Star Blizzard has even leveraged nonfunctional QR codes as a part of a spear-phishing campaign offering target users an opportunity to join a WhatsApp group: the initial spear-phishing email contained a broken QR code to encourage the targeted users to contact the threat actor. Star Blizzard's follow-on email included a URL that redirected to a webpage with a legitimate QR code, used by WhatsApp for linking a device to a user's account, giving the actor access to the user's WhatsApp account.

Use of AI

Threat actors are increasingly leveraging AI to enhance the quality and volume of phishing lures. As AI tools become more accessible, these actors are using them to craft more convincing and sophisticated lures. In a collaboration with OpenAI, Microsoft Threat Intelligence has seen threat actors such as Emerald Sleet and Crimson Sandstorm interacting with large language models (LLMs) to support social engineering operations. This includes activities such as drafting phishing emails and generating content likely intended for spear-phishing campaigns.

We have also seen suspected use of generative AI to craft messages in a large-scale credential phishing campaign against the hospitality industry, based on the variations of language used across identified samples. The initial email contains a request for information designed to elicit a response from the target and is then followed by a more generic phishing email containing a lure link to an AiTM phishing site.



Hello,

I hope this email finds you well. My fiancée, Jane, and I are in the exciting process of planning our wedding, and we're impressed by the personal touch you bring to your services.

We are currently exploring options for our wedding celebration and are interested in celebrating this special day with you. Ideally, we are looking at a weekend in June 2025 or the first weekend in July.

Here are some details about our wedding:

GUEST COUNT: We expect between 70-150 guests (we're still finalizing our guest list).

SERVICES NEEDED:

VENUE: We'd love to know more about your beautiful venue, availability, pricing, and any important details.

CATERER: Recommendations for catering services that align with our taste and dietary preferences

ACCOMMODATION: Accommodation for few of my guests.

LIVE MUSIC: Suggestions for musicians or bands to set the perfect mood.

EVENT PLANNER: Ensuring everything runs smoothly on the big day.

FLORAL ARRANGEMENTS: Designing elegant floral decor.

PHOTOGRAPHER: Capturing precious moments.

If you could provide us with a rough proposal/budget and share any venue ideas, we would greatly appreciate it. Additionally, we'd like to schedule a venue tour to see the space firsthand.

Thank you for your time and consideration. We look forward to hearing from you soon!

Best regards,

Dave Cornor.

Figure 4. One of multiple suspected AI-generated phishing email in a widespread phishing campaign

AI helps eliminate the common grammar mistakes and awkward phrasing that once made phishing attempts easier to spot. As a result, today's phishing lures are more polished and harder for users to detect, increasing the likelihood of successful compromise. This evolution underscores the importance of securing identities in addition to user awareness training.

Phishing risks continue to expand beyond email

Enterprise communication methods have diversified to support distributed workforce and business operations, so phishing has expanded well beyond email messages. Microsoft has seen multiple threat actors abusing enterprise communication applications to deliver phishing messages, and we've also observed continued interest by threat actors to leverage non-enterprise applications and social media sites to reach targets.

Teams phishing

Microsoft Threat Intelligence has been closely tracking and responding to the abuse of the Microsoft Teams platform in phishing attacks and has taken action against confirmed malicious tenants by blocking their ability to send messages. The cybercrime access broker Storm-1674, for example, creates fraudulent tenants to create Teams meetings to send chat messages to potential victims using the meeting's chat functionality; more recently, since November 2024, the threat actor has started compromising tenants and directly calling users over Teams to phish for credentials as well. Businesses can follow our security best practices for Microsoft Teams to further defend against attacks from external tenants.

Outside of business-managed applications, employees' activity on social media sites and third-party communication platforms has widened the digital footprint for phishing attacks. For instance, while the Iranian threat actor Mint Sandstorm primarily uses spear-phishing emails, they have also sent phishing links to targets on social media sites, including Facebook and LinkedIn, to target high-profile individuals in government and politics. Mint Sandstorm, like many threat actors, also customizes and enhances their phishing messages by gathering publicly available information, such as personal email addresses and contacts, of their targets on social media platforms. Global Secure Access (GSA) is one solution that can reduce this type of phishing activity and manage access to social media sites on company-owned devices.

Post-compromise identity attacks

In addition to using phishing techniques for initial access, in some cases threat actors leverage the identity acquired from their first-stage phishing attack to launch subsequent phishing attacks. These follow-on phishing activities enable threat actors to move laterally within an organization, maintain persistence across multiple identities, and potentially acquire access to a more privileged account or to a third-party organization.

You can harden your environment against internal phishing activity by configuring the Microsoft Defender for Office 365 Safe Links policy to apply to internal recipients as well as by educating users to be wary of unsolicited documents and to report suspected phishing messages.

AiTM phishing crafted using legitimate company resources

Storm-0539, a threat actor that persistently targets the retail industry for gift card fraud, uses their initial access to a compromised identity to acquire legitimate emails—such as help desk tickets—that serve as templates for phishing emails. The crafted emails contain links directing users to AiTM phishing pages that mimic the federated identity service provider of the compromised organization. Because the emails resemble the organization's legitimate messages, lead to convincing AiTM landing pages, and are sent from an internal account, they could be highly convincing. In this way, Storm-0539 moves laterally, seeking an identity with access to key cloud resources.

Intra-organization device code phishing

In addition to their use of device code phishing for initial access, Storm-2372 also leverages this technique in their lateral movement operations. The threat actor uses compromised accounts to send out internal emails with subjects such as "Document to review" and containing a device code authentication phishing payload. Because of the way

device code authentication works, the payloads only work for 15 minutes, so Microsoft has seen multiple waves of post-compromise phishing attacks as the threat actor searches for additional credentials.

Figure 5. Storm-2372 lateral movement attempt contains device code phishing payload

Defending against credential phishing and social engineering

Defending against phishing attacks begins at the primary gateways: email and other communication platforms. Review our recommended settings for Exchange Online Protection and Microsoft Defender for Office 365, or the equivalent for your email security solution, to ensure your organization has established essential defenses and knows how to monitor and respond to threat activity.

A holistic security posture for phishing must also account for the human aspect of social engineering. Investing in **user awareness training and phishing simulations** is critical for arming employees with the needed knowledge to defend against tried-and-true social engineering methods. Training can also help when threat actors inevitably refine and improve their techniques. Attack simulation training in Microsoft Defender for Office 365, which also includes simulating phishing messages in Microsoft Teams, is one approach to running realistic attack scenarios in your organization.

Hardening credentials and cloud identities is also necessary to defend against phishing attacks. By implementing the principles of least privilege and Zero Trust, you can significantly slow down determined threat actors who may have been able to gain initial access and buy time for defenders to respond. To get started, follow our steps to configure Microsoft Entra with increased security.

As part of hardening cloud identities, **authentication using passwordless solutions like passkeys** is essential, and implementing MFA remains a core pillar in identity security. Use the Microsoft Authenticator app for passkeys and MFA, and complement MFA with conditional access policies, where sign-in requests are evaluated using additional identity-driven signals. Conditional access policies can also be scoped to strengthen privileged accounts with phishing resistant MFA. Your passkey and MFA policy can be further secured by only allowing MFA and passkey registrations from trusted locations and devices.

Finally, **a Security Service Edge solution** like Global Secure Access (GSA) provides identity-focused secure network access. GSA can help to secure access to any app or resource using network, identity, and endpoint access controls.

Among Microsoft Incident Response cases over the past year where we identified the initial access vector, almost a quarter incorporated phishing or social engineering. To achieve phishing resistance and limit the opportunity to exploit human behavior, begin planning for passkey rollouts in your organization today, and at a minimum, prioritize phishing-resistant MFA for privileged accounts as you evaluate the effect of this security measure on your wider organization. In the meantime, use the other defense-in-depth approaches I've recommended in this blog to defend against phishing and social engineering attacks.

Stay vigilant and prioritize your security at every step.

Recommendations

Several recommendations were made throughout this blog to address some of the specific techniques being used by threat actors tracked by Microsoft, along with essential practices for securing identities. Here is a consolidated list for your security team to evaluate.

- Configure Microsoft Entra with increased security.
- Use the Microsoft Authenticator app for passkeys and MFA.
- Strengthen privileged accounts with phishing resistant MFA.
- Complement MFA with risk-based Conditional Access policies, where sign-in requests are evaluated using additional identity-driven signals like IP address location information or device status, among others. Implementing Microsoft Entra ID Protection with these policies can automatically block or challenge access based on indicators like unfamiliar sign-in patterns or potential token theft attempts. When combined with Global Secure Access (GSA), organizations can extend this protection by enforcing Conditional Access decisions at the network layer to help secure access to any app or resource.
- Only allowing MFA and passkey registrations from trusted locations and devices.
- Review our recommended settings for Exchange Online Protection and Microsoft Defender for Office 365.
- Use attack simulation training in Microsoft Defender for Office 365, which also includes simulating phishing messages in Microsoft Teams, to run realistic attack scenarios in your organization for educating users.
- Use Global Secure Access to secure access to any app or resource using network, identity, and endpoint access controls.
- Block device code flow where possible; if needed, configure Microsoft Entra ID's device code flow in your Conditional Access policies.
- Configure app consent policies to restrict user consent operations. For example, configure policies to allow user consent only to apps requesting low-risk permissions with verified publishers, or apps registered within your tenant.
- Require authentication strength for device registration in your environment.
- Follow our security best practices for Microsoft Teams.
- Configure the Microsoft Defender for Office 365 Safe Links policy to apply to internal recipients.

At Microsoft, we are accelerating security with our work on the Secure by Default framework. Specific Microsoft-managed policies are enabled for every new tenant and raise your security posture with security defaults that provide a baseline of protection for Entra ID and resources like Office 365.

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.
