Defending against adversary-in-the-middle threats with phishing-resistant multi-factor authentication

ITSM.30.031

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Overview

In the ever-evolving landscape of cyber security, the rise of adversary-in-the-middle (AitM) phishing poses a significant threat to organizations. AitM phishing has become increasingly popular among threat actors as organizations move to the cloud, shifting the frontline from defending traditional network perimeters to prioritizing identity protection.

Security requirements have grown increasingly complex, particularly in cloud environments, and threat actors have refined their tactics. As a result, implementing phishing-resistant multi-factor authentication (MFA) is critical for organizations to maintain strong cyber security.

This publication provides details on observed AitM phishing campaigns to highlight their prevalence and demonstrate the risk of leaving cloud accounts vulnerable. All findings in this publication are based on over 100 campaigns that the Canadian Centre for Cyber Security (Cyber Centre) detected targeting Microsoft Entra ID accounts between 2023 and early 2025. Although this is not a comprehensive overview of all AitM phishing campaigns happening globally, it offers a snapshot of how widespread these campaigns have become.

This publication aims to:

- provide a comprehensive understanding of where these threats originate
- highlight the need for all organizations to strengthen defences by employing phishing-resistant MFA by default
- provide recommendations to enhance organizations' security postures against these sophisticated campaigns

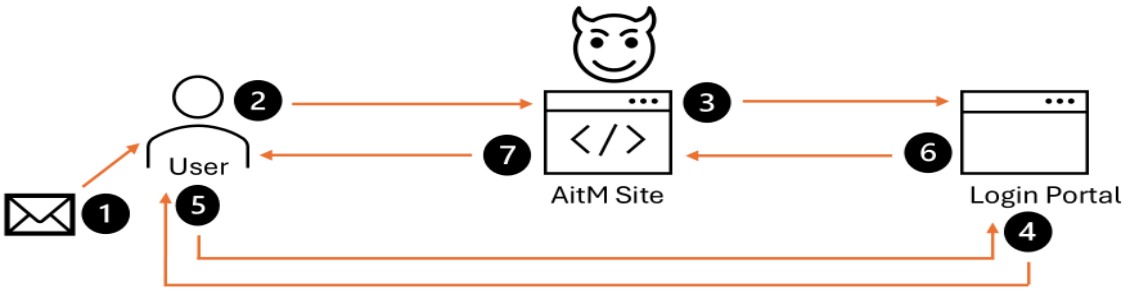
Table of Contents

List of figures

Understanding adversary-in-the-middle phishing and its impact

AitM phishing is a technique where a threat actor intercepts the connection between a user and a login server. The threat actor captures all usernames, passwords, MFA secrets and tokens transferred over that connection. Users typically receive a phishing email with a link to a malicious phishing site impersonating a legitimate website. The user is then tricked into providing their login details and completing the MFA process. The threat actor logs that information to impersonate the user later.

Figure 1: Phishing campaign by threat actor



Long description – Figure 1: Phishing campaign by threat actor

This figure illustrates how a threat actor might route and deliver a phishing email with a link to an AitM phishing site.

1. *The user receives a phishing email with a link.*
2. *The user goes to the site, where they see what appears to be a legitimate login portal.*
3. *The AitM site then proxies all connections to the login portal.*
4. *The login portal prompts the user for multi-factor authentication (MFA).*
5. *The user completes non-phishing-resistant MFA.*
6. *This action returns a validated token and session cookie to the AitM site.*
7. *The phishing site redirects the user to a different site that appears to be legitimate.*

AitM phishing is not a new concept. It has become increasingly popular among threat actors since organizations moved to the cloud. Before that, organizations worked hard to defend their frontline—the network perimeter—with firewalls and virtual private networks (VPNs). Now, organizations must strengthen cyber security to defend their new frontline, the cloud. To do this, they must protect cloud identity with a modernized set of tools, such as conditional access policies (CAPs) and MFA.

It is difficult to secure a cloud environment against AitM phishing campaigns. The cloud comes with complex security requirements that are constantly changing as threat actors increase campaigns against cloud identities. This highlights the importance of the shared responsibility model, where both clients and cloud service providers (CSPs) work together to build a robust security posture. Phishing-resistant MFA is the new industry standard. It ensures stronger identity security and is more resilient than relying solely on passwords or traditional MFA methods.

Threat actors can execute AitM phishing easily by leveraging no-code solutions, such as dark web AitM providers or open-source AitM toolkits for self-run setups. These campaigns can be thwarted by:

- phishing-resistant MFA factors
- specific CAPs that require registered device sign-ins
- specific CAPs that only allow sign-ins from specific Internet Protocol (IP) ranges or addresses that an organization owns

Transition to proxy-based adversary-in-the-middle phishing

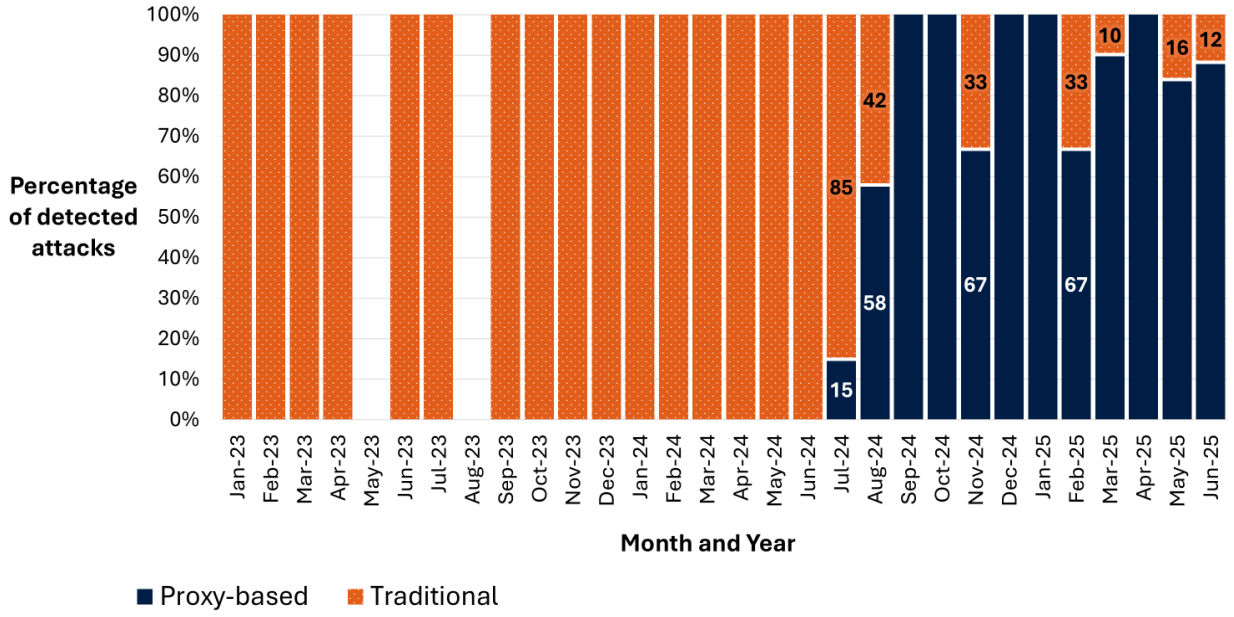
Threat actors conducting AitM phishing campaigns evade detection by using relay proxy-based AitM phishing kits. A phishing kit is a pre-assembled set of digital tools that allows threat actors to easily create fake websites and harvest sensitive user information. These fake websites often mimic trusted brands to deceive users.

Before proxy-based AitM phishing kits, organizations could detect AitM phishing by looking for suspicious logins to their cloud environment and comparing those IP addresses with network connections from their network. A login from a suspicious IP and network connections to a suspicious website hosted on that same IP was a good indication of an AitM campaign.

However, proxy-based AitM phishing kits work by adding a series of proxies in between the user and the identity provider. This means the IP from the user login will not be the same IP that appears to be hosting the phishing website. There are many ways that threat actors can achieve this, so organizations can no longer rely on IP-based correlation to detect all AitM phishing campaigns.

In mid-2024, the Cyber Centre added new internal detection capabilities for proxy-based AitM phishing and began detecting many more campaigns. This correlated with a decline in detected traditional AitM phishing. Threat actors have almost entirely shifted from traditional AitM phishing campaigns to proxy-based AitM phishing campaigns.

Figure 2: Comparison of detected traditional and proxy-based AitM phishing campaigns



Long description – Figure 2: Comparison of detected traditional and proxy-based AitM phishing campaigns

This bar graph illustrates a comparison of detected traditional and proxy-based AiTM phishing campaigns, based on campaigns that the Cyber Centre was able to confidently categorize between 2023 and mid-2025.

January 2023: Traditional AitM: 100%; proxy-based AitM: 0%

February 2023: Traditional AitM: 100%; proxy-based AitM: 0%

March 2023: Traditional AitM 100%; proxy-based AitM 0%

April 2023: Traditional AitM: 100%; proxy-based AitM: 0%

May 2023: Traditional AitM: NIL; proxy-based AitM: NIL

June 2023: Traditional AitM: 100%; proxy-based AitM: 0%

July 2023: Traditional AitM: 100%; proxy-based AitM: 0%

August 2023: Traditional AitM: NIL; proxy-based AitM: NIL

September 2023: Traditional AitM: 100%; proxy-based AitM: 0%

November 2023: Traditional AitM: 100%; proxy-based AitM: 0%

December 2023: Traditional AitM: 100%; proxy-based AitM: 0%

January 2024: Traditional AitM: 100%; proxy-based AitM: 0%

February 2024: Traditional AitM: 100%; proxy-based AitM: 0%

March 2024: Traditional AitM: 100%; proxy-based AitM: 0%

April 2024: Traditional AitM: 100%; proxy-based AitM: 0%

May 2024: Traditional AitM: 100%; proxy-based AitM: 0%

June 2024: Traditional AitM: 86%; proxy-based AitM: 14%

July 2024: Traditional AitM: 42%; proxy-based AitM: 58%

August 2024: Traditional AitM: 0%; proxy-based AitM: 100%

September 2024: Traditional AitM: 0%; proxy-based AitM: 100%

October 2024: Traditional AitM: 33%; proxy-based AitM: 67%

November 2024: Traditional AitM: 10%; proxy-based AitM: 90%

December 2024: Traditional AitM: 0%; proxy-based AitM: 100%

January 2025: Traditional AitM: 0%; proxy-based AitM: 100%

February 2025: Traditional AitM: 33%; proxy-based AitM: 67%

March 2025: Traditional AitM: 10%; proxy-based AitM: 90%

April 2025: Traditional AitM: 0%; proxy-based AitM: 100%

May 2025: Traditional AitM: 16%; proxy-based AitM: 84%

June 2025: Traditional AitM: 12%; proxy-based AitM: 88%

One major contributor to this shift was threat actors' use of a particular proxy-based AitM phishing kit. For more information on this kit, refer to the Field Effect article Field Effect discovers M365 adversary-in-the-middle campaign.

Phishing-resistant MFA continues to prevent AitM campaigns, whether from traditional kits or proxy-based AitM phishing kits. Both phishing-resistant MFA and registered device CAPs break the authentication flow when there is an AitM phishing kit in the middle of the connection.

Adversary-in-the-middle phishing trends and techniques

AitM phishing kits are increasingly sophisticated and challenging to detect. It might seem logical to focus on stopping these campaigns at their source by enhancing phishing email filtering. However, threat actors know that organizations are constantly improving their phishing protection programs and are therefore adjusting their techniques.

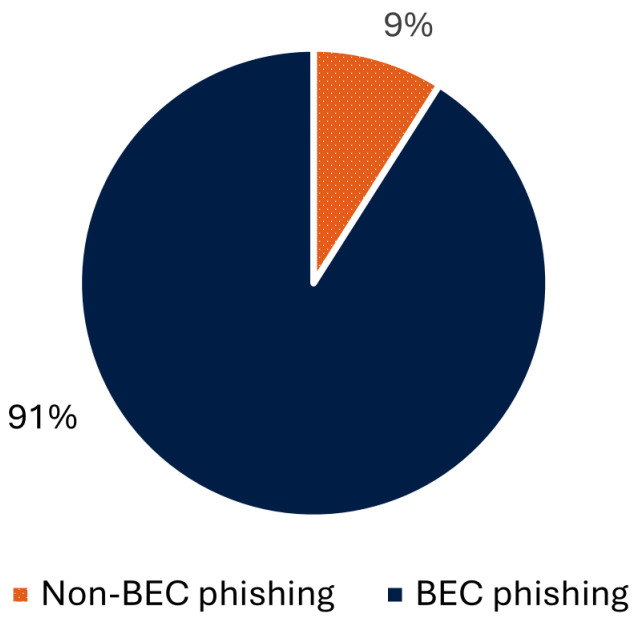
The Cyber Centre analyzed over 100 campaigns between 2023 and early 2025 and found that threat actors used a combination of vendor email compromise (VEC), which is a type of business email compromise (BEC), and a phishing technique that uses living off trusted sites (LOTS).

Business email compromise phishing campaigns

In BEC phishing campaigns, threat actors compromise legitimate organizations, steal their trusted contacts, and send AitM phishing emails with links to legitimate services like SharePoint, Dropbox, or other trusted hosting providers. The files hosted on these trusted providers contain a link to the AitM phishing site, but the link is within a file hosted on the trusted provider, not in the phishing email itself. This makes detecting and tracking the source of an AitM compromise more difficult.

From the user's perspective, they have received an email from a trusted contact with a shared file, which they may regularly receive from this contact. Threat actors can tailor the file-sharing service based on previous communications between 2 users to make their AitM phishing campaigns more difficult to identify.

Figure 3: Distribution of BEC phishing



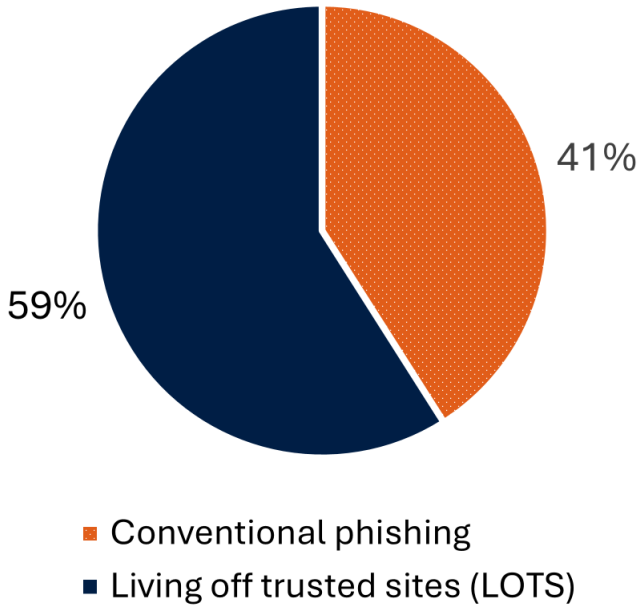
Long description – Figure 3: Distribution of BEC phishing

This pie chart shows the distribution of BEC phishing campaigns compared to non-BEC phishing campaigns that the Cyber Centre analyzed and categorized between 2023 and mid-2025. BEC phishing campaigns made up 91% of the analyzed campaigns.

Living off trusted sites techniques

LOTS-based AitM phishing made up over half of the campaigns that the Cyber Centre was able to categorize, with the remaining campaigns using conventional phishing methods (such as malicious links or attachments directly in an email). Organizations should educate users on the risks of LOTS-based AitM phishing campaigns and provide training on how to identify these campaigns.

Figure 4: Distribution of phishing techniques



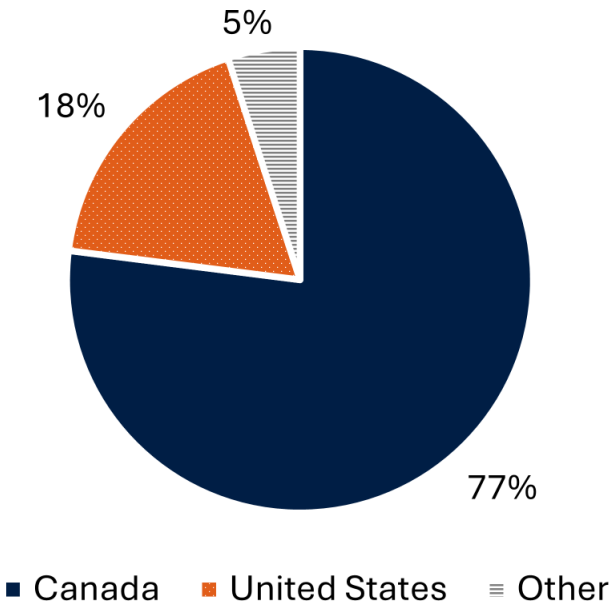
Long description – Figure 4: **Distribution of phishing techniques**

This pie chart shows the distribution of phishing techniques that the Cyber Centre analyzed and categorized between 2023 and mid-2025. LOTS made up 59% of the analyzed campaigns while conventional phishing (such as embedded links or files) made up 41%.

Targeted sectors

The Cyber Centre examined the sectors and organizations that are being targeted by AitM phishing campaigns. In Figure 5 below, the breakdown of BEC victims by country shows that most of the organizations that were compromised and that sent AitM phishing emails to the Government of Canada and to critical infrastructure partners were based in Canada. This finding underscores that threat actors are leveraging VEC since many Canadian organizations predominantly interact with other Canadian organizations in their daily operations.

Figure 5: Breakdown of BEC victims by country



***Long description – Figure 5:* Breakdown of BEC victims by country**

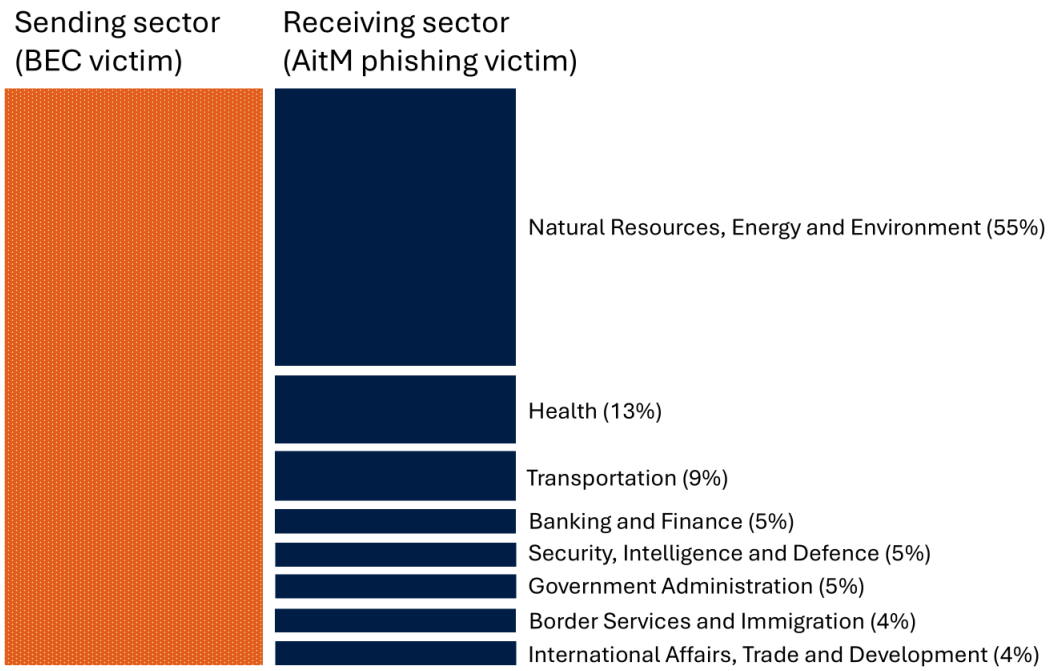
This pie chart shows the breakdown of BEC victims by country that the Cyber Centre analyzed and categorized between 2023 and mid-2025. Canada represents 77%, the United States represents 18%, and the remaining 5% is divided among other unspecified countries.

The Cyber Centre found that a third of the BEC victims were in the natural resources, energy, and environment sector. This was closely followed by the industry and business development sector and the Indigenous services sector.

When examining the victims who received AitM phishing emails, the Cyber Centre observed a similar breakdown. A quarter of the victims were in the natural resources, energy, and environment sector, followed by the security, intelligence and defence sector; the health sector; and the government administration sector.

The Cyber Centre can correlate the sectors affected by BEC and those impacted by AitM phishing to spot patterns between the sectors sending and receiving emails. We observed that 41% of sectors impacted by BEC also sent phishing emails to organizations within the same sector, consistent with previously cited VEC findings. The graph below illustrates an example of this. Notable exceptions to this trend were the hospitality and legal sectors, likely because hotels and law firms serve clients across diverse sectors.

Figure 6: BEC victims in the natural resources, energy and environment sector sending emails to AitM phishing victims



Long description – Figure 6: **BEC victims in the natural resources, energy and environment sector sending emails to AitM phishing victims**

The figure depicts BEC victims in the natural resources, energy and environment sector sending emails to AitM phishing victims. This is based on results that the Cyber Centre analyzed and categorized between 2023 and mid-2025. The natural resources, energy and environment sector sent 55% of phishing emails within its sector, 13% to the health sector, 9% to the transportation sector, 5% to the banking and finance sector, 5% to the security, intelligence and defence sector, 5% to the government administration sector, 4% to the border services and immigration sector, and 4% to the international affairs, trade and development sector.

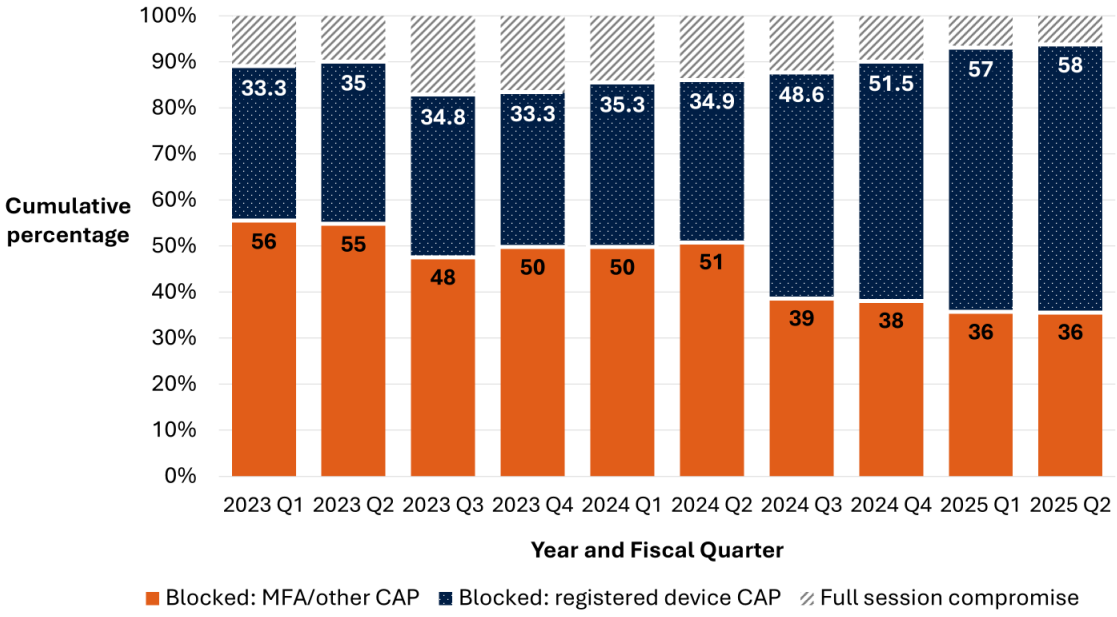
The importance of phishing-resistant multi-factor authentication

Although AitM phishing campaigns are widespread, a solution already exists to mitigate all known campaigns: phishing-resistant MFA. This is the only way to completely stop these campaigns before a threat actor can get hold of an MFA-verified session.

According to the Cyber Centre's findings, full-session compromises within the Government of Canada and critical infrastructure partners have decreased over the last few years. This is primarily because

these organizations have adopted registered device CAPs and other CAPs requiring phishing-resistant MFA and have implemented strictly controlled IP restrictions on logins. Full-session compromises decreased from a high of almost 20% at the end of the third quarter of 2023 to less than 10% of all compromises as of early 2025.

Figure 7: Cumulative percentage of AitM phishing results over time



***Long description – Figure 7:* Cumulative percentage of AitM phishing results over time**

This bar graph illustrates the cumulative percentage of AiTM phishing results that the Cyber Centre analyzed and categorized between 2023 and mid-2025.

2023 Q1: Blocked: MFA/other CAP: 55.6%; blocked: registered device CAP: 33.3%; full session compromise: 11.1%

2023 Q2: Blocked: MFA/other CAP: 55%; blocked: registered device CAP: 35%; full session compromise: 10%

2023 Q3: Blocked: MFA/other CAP: 47.8%; blocked: registered device CAP: 34.8%; full session compromise: 17.4%

2023 Q4: Blocked: MFA/other CAP: 50%; blocked: registered device CAP: 33.3%; full session compromise: 16.7%

2024 Q1: Blocked: MFA/other CAP: 50%; blocked: registered device CAP: 35.3%; full session compromise: 14.7%

2024 Q2: Blocked: MFA/other CAP: 51.2%; blocked: registered device CAP: 34.9%; full session compromise: 14%

2024 Q3: Blocked: MFA/other CAP: 38.9%; blocked: registered device CAP: 48.6%; full session compromise: 12.5%

2024 Q4: Blocked: MFA/other CAP: 38.4%; blocked: registered device CAP: 51.5%; full session compromise: 10.1%

2025 Q1: Blocked: MFA/other CAP: 35.9%; blocked: registered device CAP: 57%; full session compromise: 7%

2025 Q2: Blocked: MFA/other CAP: 35.9%; blocked: registered device CAP: 58%; full session compromise: 6.1%

The Cyber Centre continues to observe a steady stream of AitM phishing campaigns stemming from BEC. This indicates that threat actors remain confident that enough accounts lack phishing-resistant MFA protection, making AitM phishing campaigns a worthwhile technique for compromising accounts.

Enhancing defences against evolving adversary-in-the-middle threats

Phishing-resistant MFA can prevent AitM campaigns, but it can be difficult for organizations to implement. Cloud configuration can also be challenging, and most phishing-resistant MFA methods are fee-based.

Organizations should weigh the risk and impact of cyber incidents against the cost of implementing phishing-resistant MFA. Organizations that choose to implement phishing-resistant MFA should consider the following:

- Compared with the cost of remediating and recovering from a data breach, providing phishing-resistant MFA methods (FIDO2 security keys, passkeys, Windows Hello for Business) to users is a cost-effective investment
- Data and information may be critical to business operations or contain highly sensitive private information, and any compromise can have a significant impact and cost for the organization
- An identity compromise can have a significant impact on an organization's reputation

Some organizations are moving to devices that are registered with their IT departments and phishing-resistant MFA. However, threat actors are often a step ahead and launch AitM phishing campaigns before organizations can move to phishing-resistant options.

Addressing high-risk gaps and vulnerabilities

Organizations should deploy phishing-resistant MFA to every user, without exception. They should also review their identity protection posture and flag any high-risk gaps or vulnerabilities. The following are examples of high-risk gaps or vulnerabilities that organizations should address immediately to prevent AitM compromises.

Administrators using weak MFA methods

Organizations should apply phishing-resistant MFA to all administrator accounts, without exception, in any CAP. Additionally, organizations should remove any non-phishing-resistant backup methods on these accounts since these could be bypassed by AitM phishing campaigns.

Bring-your-own-device without phishing-resistant MFA or location restrictions

Threat actors' primary targets are users who are allowed to sign in from their own devices, outside of an organization's controlled IP space and without phishing-resistant MFA. This is a very high-risk gap that organizations should address immediately.

If organizations require users to use personal devices (known as bring your own device [BYOD]), they should deploy phishing-resistant MFA and ensure that users cannot use any weak fallback methods. Alternatively, organizations could require all BYOD logins to go through the organization's corporate VPN, with an accompanying CAP that restricts logins to only that specific IP space.

The greatest challenge is avoiding the temptation to make exceptions for specific users, groups or applications. As a baseline, all users should have phishing-resistant MFA by default and without exception.

Educating employees

Organizations should also train their employees on how to spot and report AitM campaigns. Many users will open emails and click on the included links if the email is from a trusted source. Organizations should consider including the following topics in their training on phishing campaigns.

BEC scenarios

The more users are aware of how common BEC campaigns are, the more they will be on the lookout for them. Before clicking on a link in an email, they should know to ask themselves a couple of questions, such as:

- Do I usually receive unsolicited Dropbox files from this contact?
- Does this contact usually send me SharePoint documents?

If a user receives unsolicited files, they should reach out to the sender through another method (for example, a phone call) to confirm that the document was shared intentionally.

Double-checking the URL when signing into login services

Verifying the legitimacy of URLs can be difficult since logins to some sites like Microsoft Entra ID contain long URLs, so users might not notice a suspicious domain in the path. Educating users on where to find the top-level domain within a URL and what domains to expect in that location can go a long way in stopping these campaigns.

Avoiding multiple logins

Users often sign into their accounts using a cloud-based identity and access management service like Microsoft Entra ID. This allows them to access applications like Microsoft SharePoint or Teams with a single sign-on. If users know that they shouldn't need to log in again to access applications or a shared file, they will think twice before re-entering their credentials.

Another helpful technique is to teach users to open a new tab and sign into the file-sharing service directly before clicking on a link. After logging into the service directly, users should not be prompted to sign in again when they click the file link in their email. If they do receive a prompt, it could be an AitM phishing campaign.

Good password hygiene

Even if users know how to spot AitM phishing campaigns, there will always be some successful campaigns that trick users into supplying their username and password before the campaigns are blocked by CAPs. This means that the threat actor can gain control of the user's username and password, even if they did not get an MFA-verified session. Therefore, organizations must remind users to not reuse passwords. Once a threat actor obtains these credentials, they can use them against other login portals within the organization that might not have MFA protections (for example, legacy web portals or less secure VPN appliances).

Summary

AitM phishing campaigns are becoming more sophisticated and are occurring across all sectors. As this publication highlights, there are a number of measures organizations can take to mitigate this threat. However, the best defence against AitM phishing campaigns is to implement phishing-resistant MFA by default and without exception.

For additional cyber security guidance, please refer to the following:

- Foundational cyber security actions for small organizations (ITSAP.10.300)
- Offer tailored cyber security training to your employees (ITSAP.10.093)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)

This is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our Contact Centre:

- contact@cyber.gc.ca
- (613) 949-7048 or 1-833-CYBER-88.

Effective date

This publication takes effect on

Revision history

Revision	Amendments	Date
1	First release.	October 30, 2025

D97-4/30-031-2025E-PDF
ISBN 978-0-660-79385-6