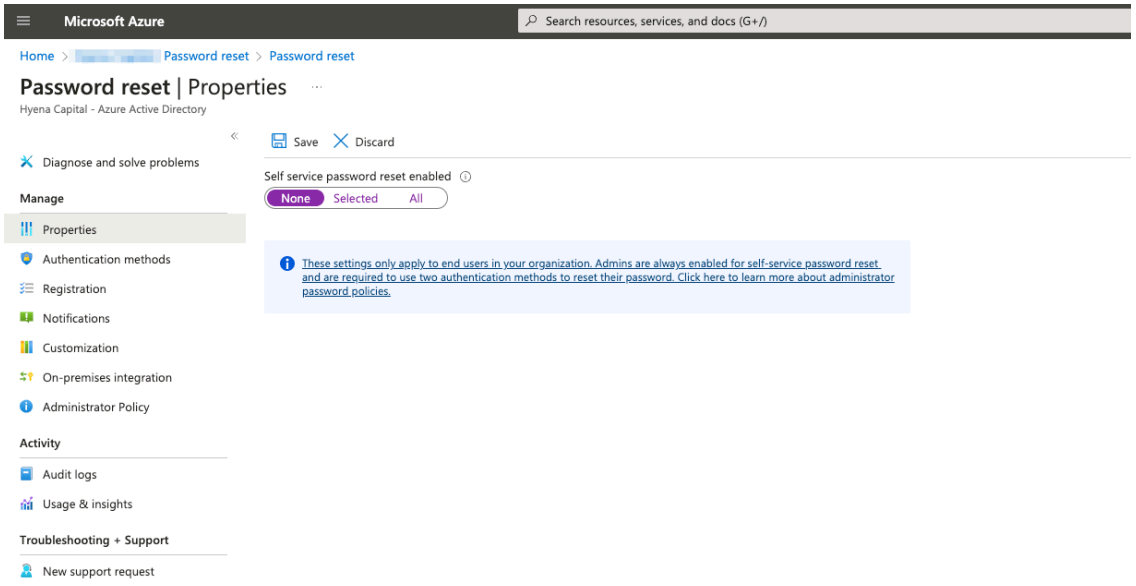
Behind The Breach: Self-Service Password Reset (SSPR) Abuse in Azure AD

Archived: 2026-04-05 16:22:14 UTC

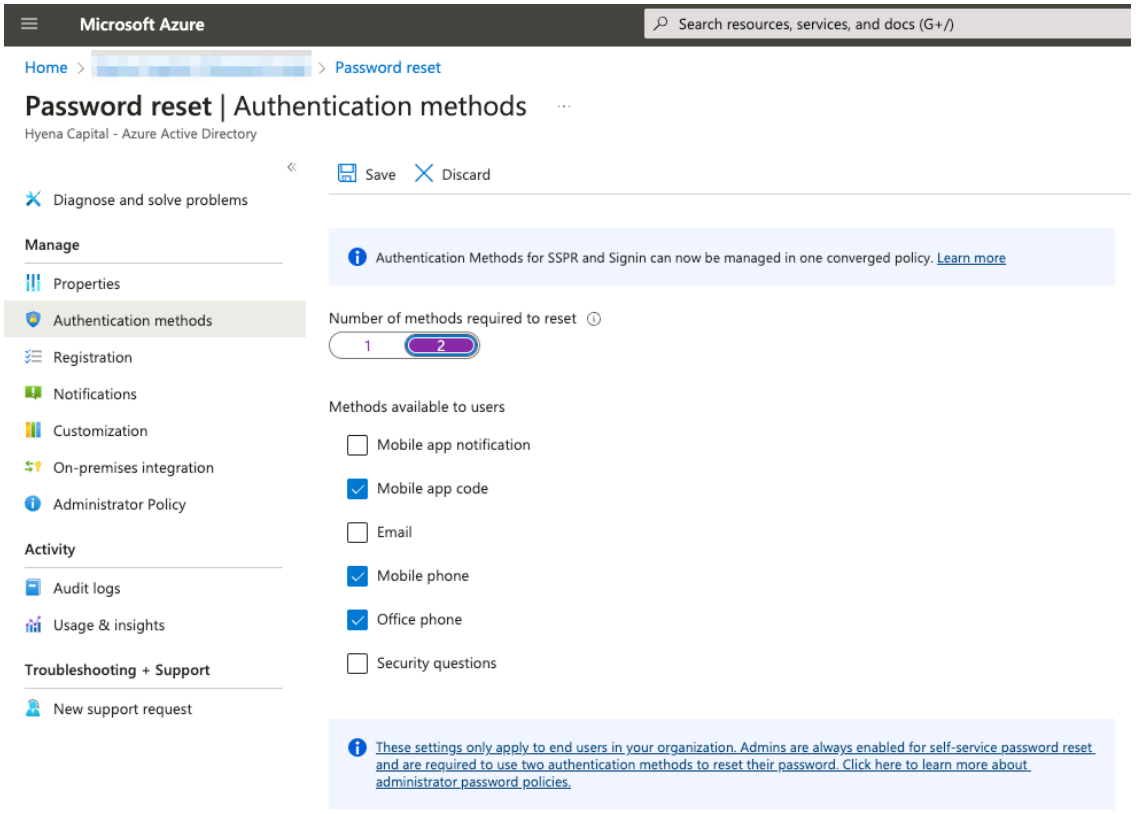
In several recent investigations of SaaS security incidents, the Obsidian threat research team identified a novel attack vector in the wild: abuse of the Azure AD self-service password reset (SSPR) feature.

With the glaring lack of coverage around this specific threat vector, our team felt it would be an important topic for discussion. In this blog, we'll explore the self-service password reset technique in more detail, share some firsthand examples from the field, and discuss measures for mitigating this risk.

Self-service password reset is an Azure AD feature that allows users to reset their password without the involvement of an administrator or help desk. It is designed for convenience and productivity so that users who forgot their password or get locked out can easily reset it themselves with minimal friction.



Administrators are able to configure SSPR for the entire organization or a subset of groups via the Azure portal. They can also define requirements for permitted forms of verification and the number of verification methods required to perform the reset.



How is self-service password reset being abused?

We've already seen several organizations suffer breaches that began with SSPR as the initial access vector. There are two primary methods through which adversaries have been abusing this tool:

- SIM swapping to gain initial access
- Attacker registered MFA to establish persistence

SIM swapping is an increasingly popular tactic that adversaries use to take control of a target phone number. This typically involves social engineering a mobile carrier in order to initiate a number transfer to a new SIM card or bribing (via a broker) internal employees to execute a swap. If an adversary controls your number and your organization's SSPR is configured to only require a single verification method, the attacker should have no problem gaining entry.

After establishing initial access, adversaries were seen enrolling their own MFA methods—typically mobile authenticator applications or disposable emails—to guarantee their own persistence.

In one of our investigations, the victim recovered their phone service and regained access to their account with the help of their IT/security team. They still failed to reverse the malicious MFA enrollment, allowing the attacker to initiate another SSPR and take back the account. Now imagine this technique at scale against a large user base and how overwhelming it would be for any security team to address.

The screenshot below shows a timeline of events where an adversary battled IT efforts to reset the victim's password. Unsure of what to do, the IT team temporarily disabled the account and ultimately decided to delete it entirely.

Date (UTC)	Service	Event	Description
Apr 2023	Microsoft	Delete user.	deleted the Azure AD user
Apr 2023	Microsoft	Disable account.	disabled the Azure AD account for
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Reset user password.	fim_password_service@support.onmicrosoft.com reset the password for the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Reset user password.	fim_password_service@support.onmicrosoft.com reset the password for the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Change user password.	changed the Azure AD password of the user
Apr 2023	Microsoft	Update user.	The service principal Microsoft password reset service changed the settings for the user
Apr 2023	Microsoft	Change user password.	On-Premises Directory Synchronization Service Account changed the Azure AD password of the user
Apr 2023	Microsoft	Reset user password.	fim_password_service@support.onmicrosoft.com reset the password for the user

Stealing a target's phone number and resetting their password might seem like a noisy method for initial access, but our intel reveals time and time again that sophisticated adversaries can operate with extreme efficiency in SaaS environments. A few hours alone can allow bad actors to accomplish a wide variety of goals and cause significant damage to your business. After initial access, reconnaissance, and post-authentication operations, an attacker has access to a trove of internal intelligence which helps them carry out subsequent attacks with a higher likelihood of success.

What can I do to remain secure?

Combating SSPR Abuse

There are a few options available to eliminate the SSPR vector entirely or, at minimum, provide warnings of potential abuse.

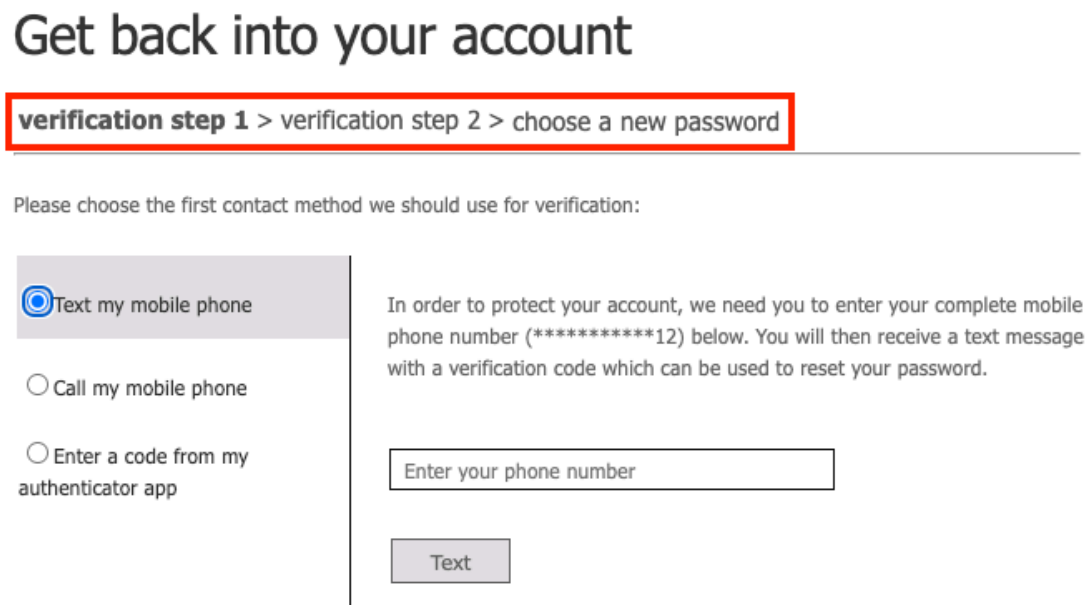
Disable SSPR globally. Microsoft recommends that SSPR be enabled for all users to reduce the burden on IT and minimize employee downtime should they forget their passwords. As many security practitioners know, this type of convenience often sits opposite of security.

Obsidian insights reveal that 39% of Microsoft tenants have SSPR disabled for more than 75% of their user population.

This demonstrates that organizations can function fine without the feature enabled. Disabling SSPR completely blocks initial access via SIM swap and opportunities for re-entry.

In cases where we've seen SSPR abuse lead to an incident, it is often enough motivation for the affected organization to disable it completely.

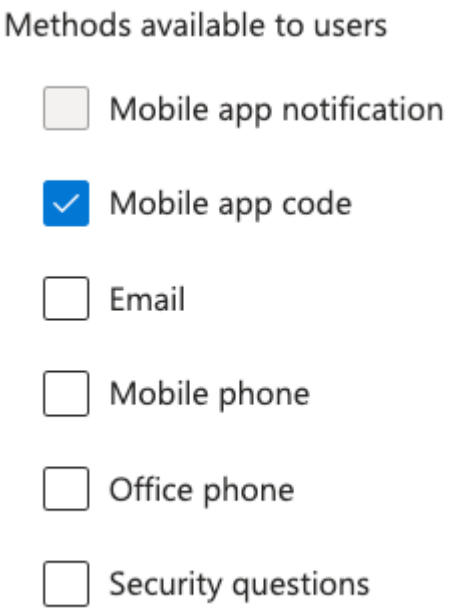
Require more than one method for SSPR. In a SIM swap attack, the stolen phone number can be used as a verification method to reset the password, essentially downgrading MFA to single factor authentication. It is possible to configure SSPR to require 2 verification methods in order to perform the reset. This way the attacker will need more than just the target's phone number to complete the SSPR flow. Requiring two verification methods in SSPR would raise the bar higher as it is for MFA, with a caveat of what methods are chosen.



SSPR prompt where 2 methods are required for verification.

Restrict the methods that can be used to perform an SSPR. If globally disabling SSPR or requiring two methods for all users isn't an option, you can also choose to restrict which methods can be used to perform a password reset. Disabling mobile and office phones as a method will completely block SIM swap attacks.

However, since SSPR is not completely disabled, re-entry by an attacker via a malicious MFA method is still possible.



Microsoft UI for SSPR method selection

Detect early signs of SSPR recon. Successful SIM swapping necessitates sufficient preliminary reconnaissance to identify a viable target. Aside from requiring the information to social engineer a mobile carrier, the adversary needs to determine whether or not the target is even susceptible to SSPR abuse.

Given any email address, it is easy to validate if it is a valid Microsoft 365 account. The below curl command can be used to determine if a given email address is a managed account in Microsoft 365:

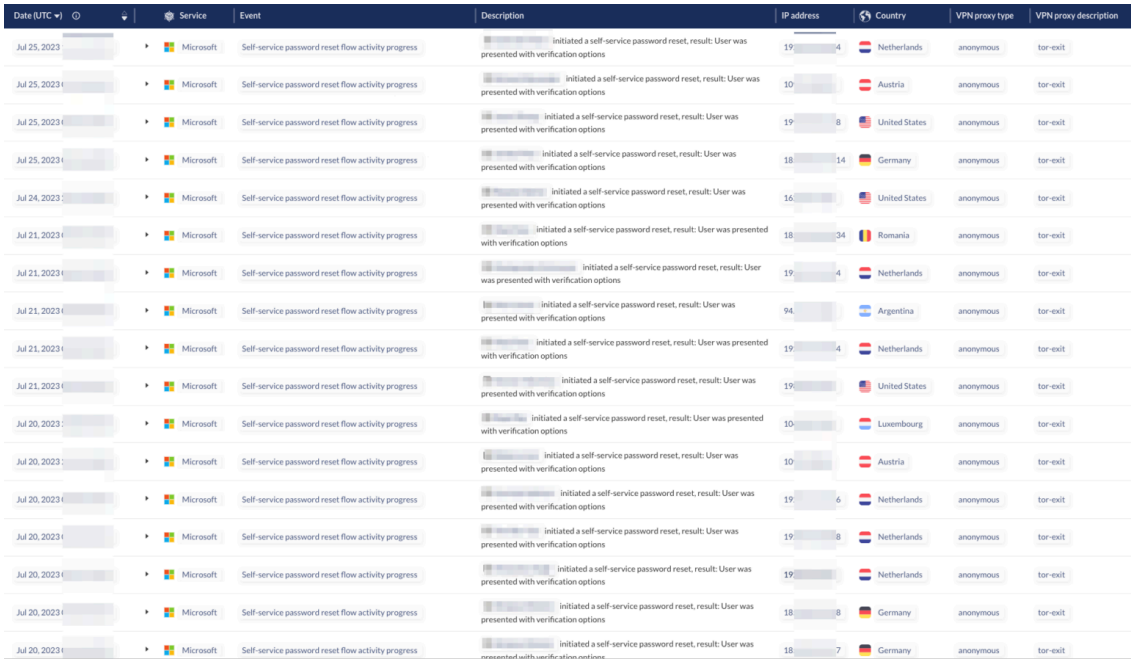
curl -s -X POST https:///login.microsoftonline.com/common/GetCredentialType –data '{"Username":"user@domain.com"}'

Once you have valid Microsoft 365 accounts, you can initiate the SSPR flow and see which verification options are available. Attackers likely need to perform this recon as well if they are going to spend the time and effort performing the initial SIM swap.

The Microsoft interface that appears during a SSPR clearly indicates whether one or two verification methods are required, making it easier for attackers to select vulnerable target accounts. Examining SSPR initiations that were never completed from suspicious IPs can serve as an early warning of potential recon. A burst of these activities for multiple accounts—especially high-value targets—reveals that your organization is likely being targeted and can serve as justification for the reconfiguration or disabling of SSPR.

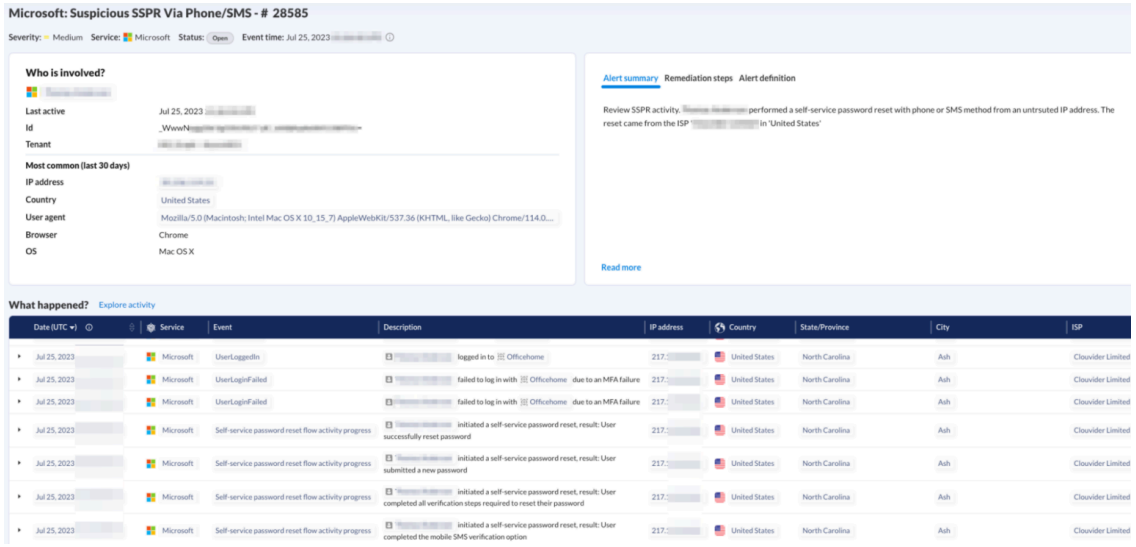
The below screenshot shows a variety of user accounts initiating SSPR flows from TOR exit nodes, but never finishing them. This is a strong indicator that an attacker is performing recon and identifying potential targets for

an SSPR attack.



Date (UTC)	Service	Event	Description	IP address	Country	VPN proxy type	VPN proxy description
Jul 25, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 4	Netherlands	anonymous	tor-exit
Jul 25, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	10	Austria	anonymous	tor-exit
Jul 25, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 8	United States	anonymous	tor-exit
Jul 25, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	18 14	Germany	anonymous	tor-exit
Jul 24, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	16	United States	anonymous	tor-exit
Jul 21, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	18 34	Romania	anonymous	tor-exit
Jul 21, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 4	Netherlands	anonymous	tor-exit
Jul 21, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	94	Argentina	anonymous	tor-exit
Jul 21, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 4	Netherlands	anonymous	tor-exit
Jul 21, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19	United States	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	10	Luxembourg	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	10	Austria	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 6	Netherlands	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19 8	Netherlands	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	19	Netherlands	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	18 8	Germany	anonymous	tor-exit
Jul 20, 2023	Microsoft	Self-service password reset flow activity progress	initiated a self-service password reset, result: User was presented with verification options	18 7	Germany	anonymous	tor-exit

Detect suspicious SSPR activity. While migrating away from tenant configurations that make SSPR abuse possible, it is important to have the appropriate detections in place that would detect its abuse by an attacker. If a SSPR flow is completed via SMS or phone call options from a rare and suspicious IP, it may indicate a potential SIM Swap attack that was then used to perform SSPR. While detecting the initial SIM Swap may be out of reach for security teams due to the lack of visibility into phone numbers and ICCID binding, identifying the follow-up attack methods are still within scope.

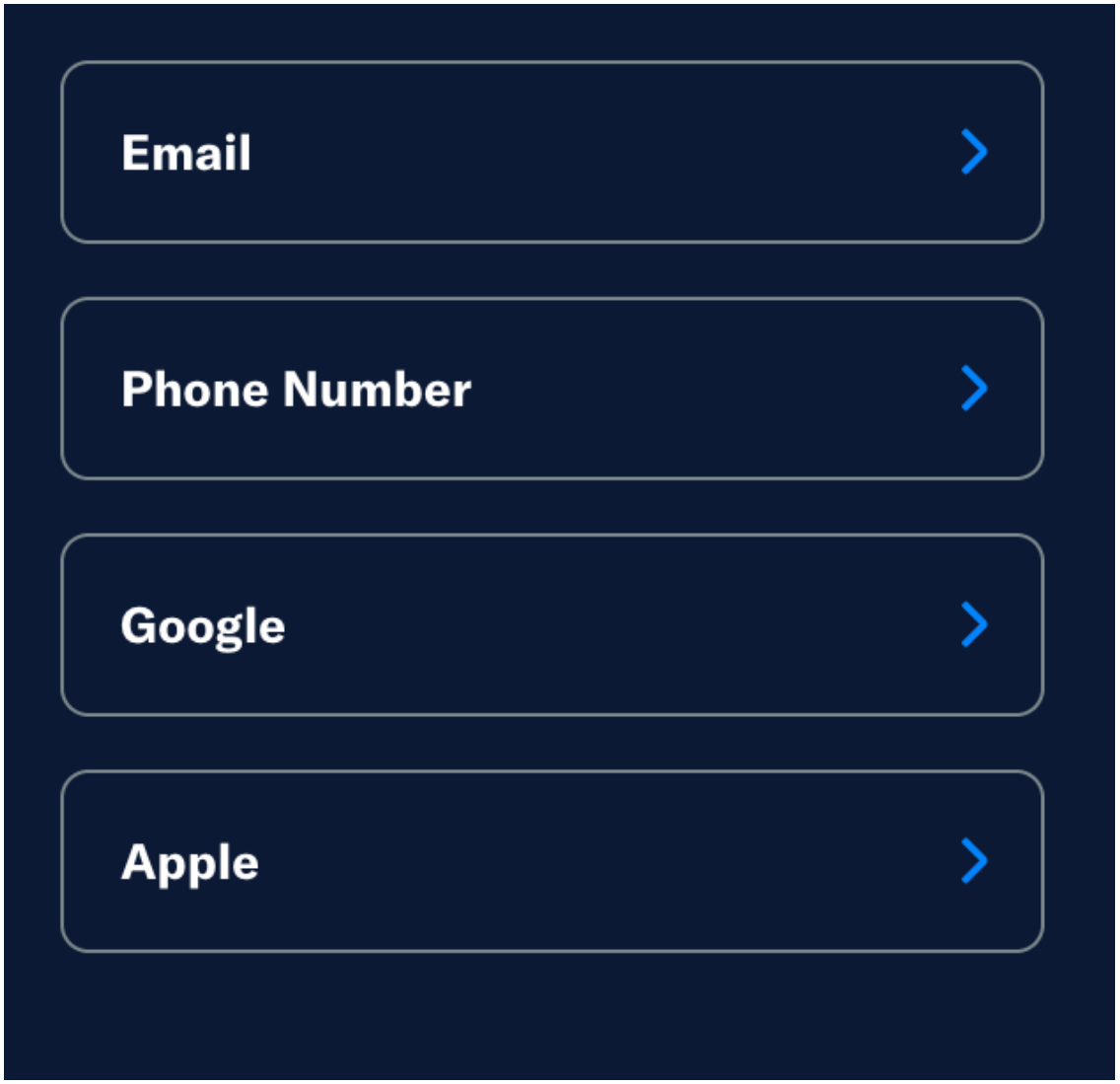


Availability of SSPR settings data

Those familiar with the Microsoft ecosystem will not be surprised when they learn that important settings related to SSPR are not available via an API or Powershell. At the time of writing this blog post, users that can perform SSPR can be pulled from a reports endpoint in the MS Graph API. However, the details around how many methods are required to perform the reset and which methods can be used can only be found via an internal API used by the Azure Portal web UI.

SSPR on other SaaS services

We've quickly checked if other SaaS services allow SSPR with a single method related to SIM. While it is not an option for the majority of services, there are indeed a few services that employ single factor SMS as an optional method for authentication, which would be vulnerable to similar SIM swapping attacks. Note that our team did not check SaaS service exhaustively. It is recommended that IT teams build awareness around SaaS services used in their organizations and make sure phone number-based authentication is disabled.



Another such example of a SaaS service offering phone number authentication.

Conclusion

As SIM swapping becomes an active attack vector in the wild, it has more significant security implications on SSPR and other features that rely on the security of SIM. Security team should be aware of this attack vector, re-evaluate the risk level of enabling such features, and closely monitor any suspicious activities coming from this venue.
