SAME SEA, NEW PHISH

Russian Government-Linked Social Engineering Targets App-Specific Passwords

June 18th, 2025
Report No. 188

By John Scott-Railton, Rebekah Brown, Bill Marczak

THE CITIZEN LAB
munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO

Copyright

Suggested Citation

John Scott-Railton, Rebekah Brown, and Bill Marczak. “Same Sea, New Phish: Russian Government-Linked Social Engineering Targets App-Specific Passwords,” Citizen Lab Report No. 188, University of Toronto, June 18, 2025.

Acknowledgements

We thank Mr. Giles for his extraordinarily gracious willingness to share the material of this attack and describe how he experienced it. When targets elect to speak out and share their experiences, it helps make us all safer.

Special thanks to Alyson Bruce for editorial and graphics support, and Ksenia Ermoshina, Alberto Fittarelli, Micah Lee, Cooper Quintin, M Scott, and Adam Senft for review.

Special thanks to the Google Threat Intelligence Group.

Research for this project was supervised by Professor Ronald J. Deibert.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Excerpt

In May 2025, Keir Giles, a well-known expert on Russian military operations, was targeted with a highly sophisticated and personalized phishing attack. Using a method not previously observed by the Citizen Lab, the attacker posed as a U.S. State Department employee to convince Mr. Giles to create and send app-specific passwords for his email accounts, bypassing multi-factor authentication. Google spotted and blocked the attack, attributing it to a Russian state-backed operator.

Key Findings

- Keir Giles, a prominent expert on Russian information operations, was targeted with a sophisticated and personalized novel social engineering attack.
- The attacker took extensive measures to avoid raising Mr. Giles' suspicions, and deceived him into creating and sending them App-Specific Passwords for his accounts, bypassing Multi-Factor Authentication (MFA).
- Google later spotted and blocked the attacker. Their Google Threat Intelligence Group (GTIG) labels the operator Russian state-backed UNC6293, which they link with low confidence to APT29, which is attributed to Russia's Foreign Intelligence Service (SVR).
- We expect more social engineering attacks leveraging App-Specific Passwords in the future.

Click here to read Google's blog post on this campaign.

Introduction: New Pressures on Attackers

In recent years, users' familiarity with common phishing tactics, increasingly advanced detection and blocking by platforms, and the rise in use of Multi-Factor Authentication (MFA), have all contributed to changes in the ways that attackers phish accounts. The introduction of more secure forms of MFA, such as hardware security keys, has also closed off certain avenues of social engineering.

These pressures, among others, are driving attackers towards more complex social-engineering tactics, and more technically sophisticated attack frameworks, including targeting MFA. For example, a recent analysis by Cisco's Talos reported that nearly half of all recent incidents that their team responded to involved attackers trying to bypass MFA.

As past reporting highlights, attackers need to improve their technical methods, and adapt their social engineering approaches to bypass both platform detections, as well as avoid the subtle cues associated with phishing attempts that many users have now been trained to spot.

Looking for a Side Door

While many state-backed attackers still focus on phishing a target’s passwords and MFA codes, others are constantly experimenting with novel ways to access accounts. Often, these efforts involve blending social engineering and targeting alternate account access flows, such as access tokens. Attackers have also gravitated towards cross-platform attacks, where initial outreach may happen on one messaging platform (e.g. Signal or WhatsApp), and later move to another channel, such as email. These attacks split attack elements between different ecosystems, making it more challenging for platforms and defenders to put the pieces together.

Volexity recently reported on several such efforts, and the Citizen Lab has also tracked similar attacks against civil society groups in the course of our investigations of Russian state-sponsored groups. The attack described in this research note is yet another effort to gain account access through a novel method: convincing the target user to create and share a screenshot of an App-Specific Password (ASP).

What are App-Specific Passwords?

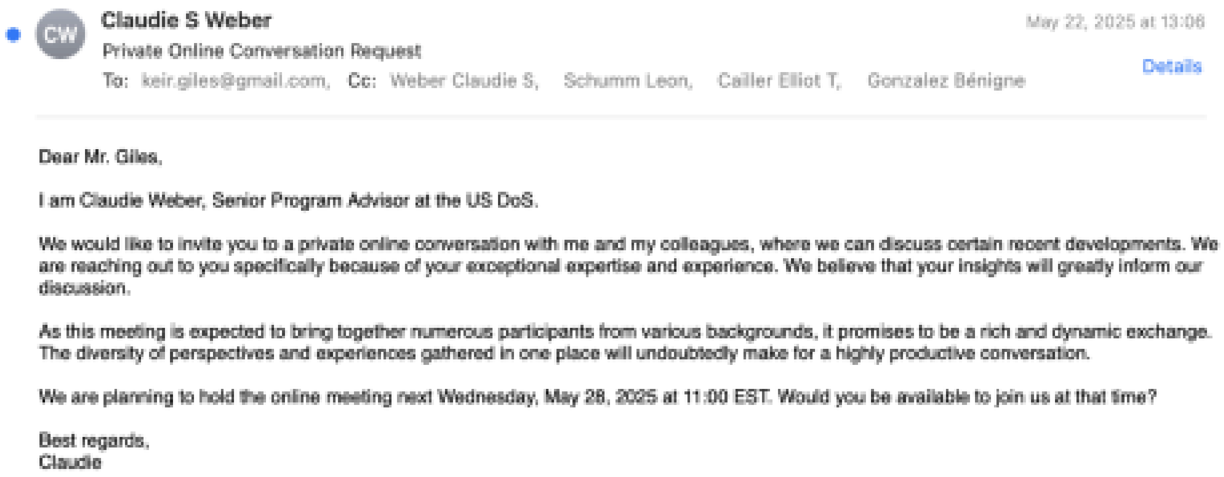
Certain applications do not support Multi-Factor authentication, or are otherwise incompatible with platforms’ standard login workflows. In order to allow these apps to access online accounts with MFA enabled, a user can create an App-Specific Password (ASP). For example, a user might add an ASP to allow a legacy third-party mail client access to their email account. Google refers to these apps as Less Secure Apps (LSAs) and has been phasing out support in Google Workspaces; however Google still allows users to create and remove these passwords on their personal Gmail accounts.

Enter the App-Specific Password Attack

Keir Giles is a well-known and outspoken academic expert on countering Russian information and influence operations and the Russian military. He is a senior associate of the Russia programme at Chatham House, a UK-based policy institute, and his work has uncovered covert Russian campaigns. He has also written extensively on Russia’s actions following their invasion of Ukraine. Mr. Giles contacted the Citizen Lab for assistance with the attack, and we are publishing this note with his consent.

The Attack Begins

On May 22, 2025, a sender purporting to be U.S. State Department official “Claudie S. Weber” sent an email to Mr. Giles. The message purports to be an invitation for a consultation, something that would be common for him to receive.



Claudie S Weber
Private Online Conversation Request
To: keir.giles@gmail.com, Cc: Weber Claudie S, Schumm Leon, Cailler Elliot T, Gonzalez Bénigne
May 22, 2025 at 13:06

Dear Mr. Giles,

I am Claudie Weber, Senior Program Advisor at the US DoS.

We would like to invite you to a private online conversation with me and my colleagues, where we can discuss certain recent developments. We are reaching out to you specifically because of your exceptional expertise and experience. We believe that your insights will greatly inform our discussion.

As this meeting is expected to bring together numerous participants from various backgrounds, it promises to be a rich and dynamic exchange. The diversity of perspectives and experiences gathered in one place will undoubtedly make for a highly productive conversation.

We are planning to hold the online meeting next Wednesday, May 28, 2025 at 11:00 EST. Would you be available to join us at that time?

Best regards,
Claudie

Figure 1: May 22, 2025, the first outreach offering a highly plausible scenario of a consultation.

We could find no evidence that “Claudie S. Weber” exists or is a U.S. State Department employee. The attacker used a Gmail account for the entire interaction:

```
claudie.s.weber@gmail.com
```

However, four emails at @state.gov are also included on the CC line, including a “Claudie S. Weber” @state.gov email address. This lends to the perceived credibility and safety of the email exchange.

A target might reason “if this isn’t legitimate, surely one of these State Department employees would say something, especially if I reply and keep them on the CC line.”

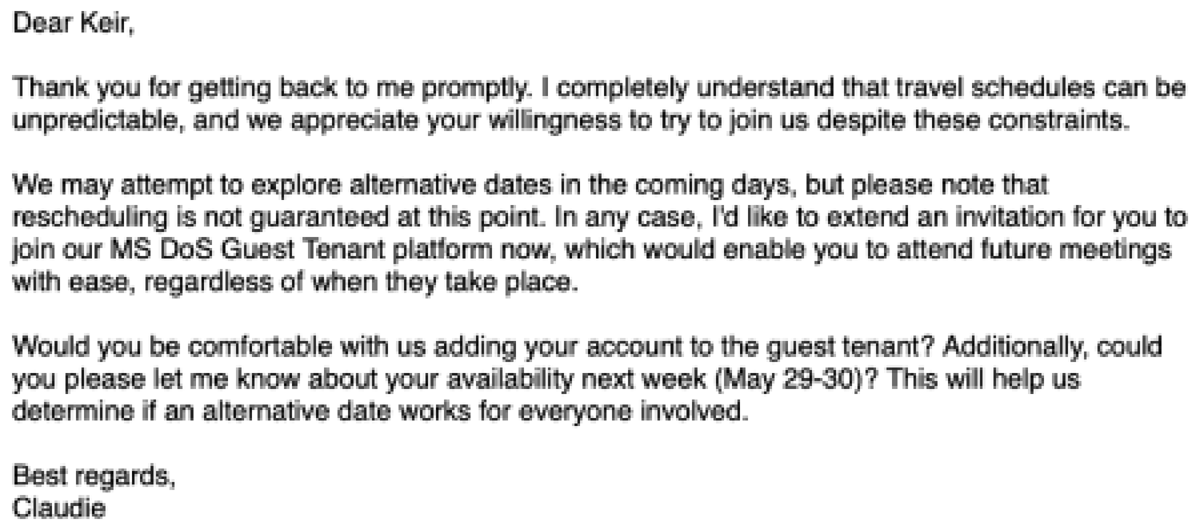
In fact, the attacker has likely created fictitious personas and @state.gov email addresses purely as a credibility signal. We believe that the attacker is aware that the State Department’s email server is apparently configured to accept all messages and does not emit a ‘bounce’ response even when the address does not exist.

The message's English is grammatical and fluent, but somewhat generic in tone, raising the possibility that the attacker used a large language model (LLM) or similar tools to help craft the outreach. The message was also received within Washington D.C. working hours, adding an additional element of credibility.

Setting the Stage

The message content, timing, and inclusion of official .gov email addresses in the CC field combined to create the appearance of a safe and credible approach. Mr. Giles described these techniques to us as establishing "pillars of plausibility."

Mr. Giles responded to the message indicating interest, but noted that the date might not work for him. The attacker responded, introducing the core deception: inviting him to join the State Department's "MS DoS Guest Tenant" platform.



Dear Keir,

Thank you for getting back to me promptly. I completely understand that travel schedules can be unpredictable, and we appreciate your willingness to try to join us despite these constraints.

We may attempt to explore alternative dates in the coming days, but please note that rescheduling is not guaranteed at this point. In any case, I'd like to extend an invitation for you to join our MS DoS Guest Tenant platform now, which would enable you to attend future meetings with ease, regardless of when they take place.

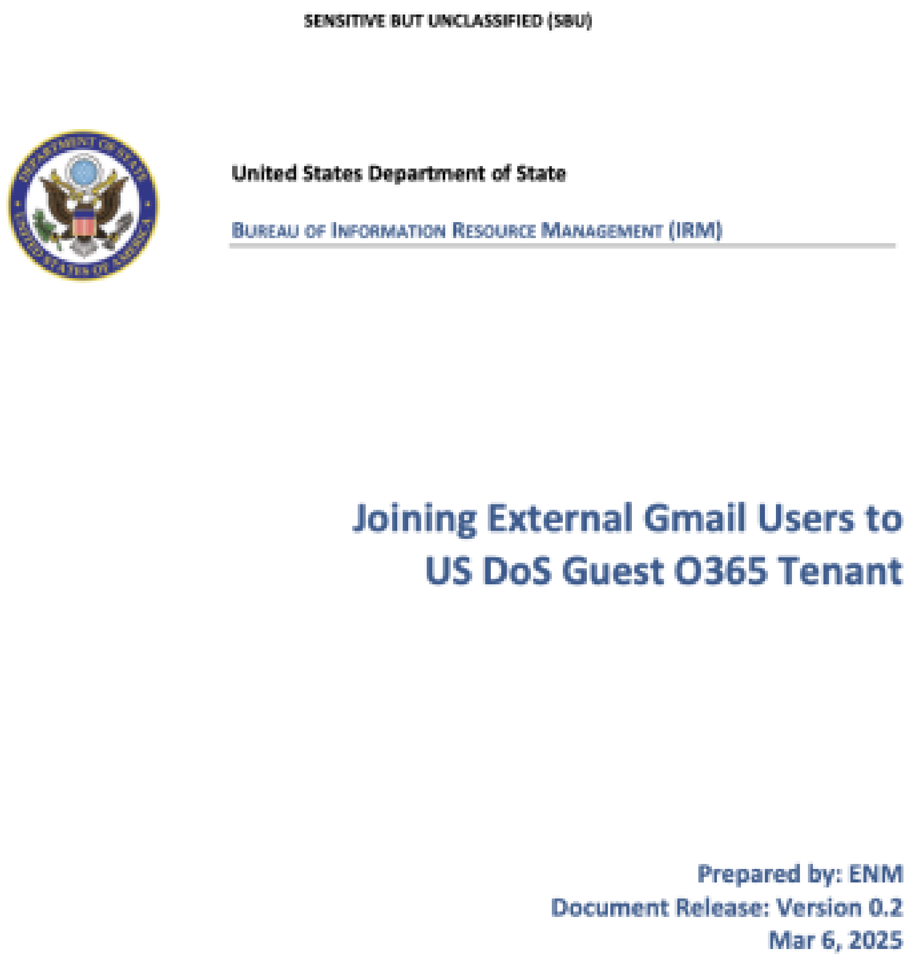
Would you be comfortable with us adding your account to the guest tenant? Additionally, could you please let me know about your availability next week (May 29-30)? This will help us determine if an alternative date works for everyone involved.

Best regards,
Claudie

Figure 2: May 23, 2025, the attacker introduces the concept of an "MS DoS Guest Tenant" registration.

As the conversation unfolded (ultimately involving at least 10 exchanges), the attacker sent a PDF file with instructions to register for an "MS DoS Guest Tenant" account.

The PDF appears to be an official document with markings and revision history. It walks the target through the creation of an App-Specific Password on a Google email account.



SENSITIVE BUT UNCLASSIFIED (SBU)

United States Department of State

BUREAU OF INFORMATION RESOURCE MANAGEMENT (IRM)

Joining External Gmail Users to
US DoS Guest O365 Tenant

Prepared by: ENM
Document Release: Version 0.2
Mar 6, 2025

Figure 3: The fake "MS DoS" State Department PDF was crafted to feature numerous visual elements reminiscent of a legitimate State Department document.

The document does not appear to have any of the telltale errors of language, grammar issues or other mistakes that characterize many previous generations of lure documents used by state-backed attackers.

The instructions PDF (note, this file does not contain malware):

```
SHA256: 329fda9939930e504f47d30834d769b30ebeaced7d73f3c1aadd0e48320d6b39
```

Getting the Target to Create and Share an App-Specific Password

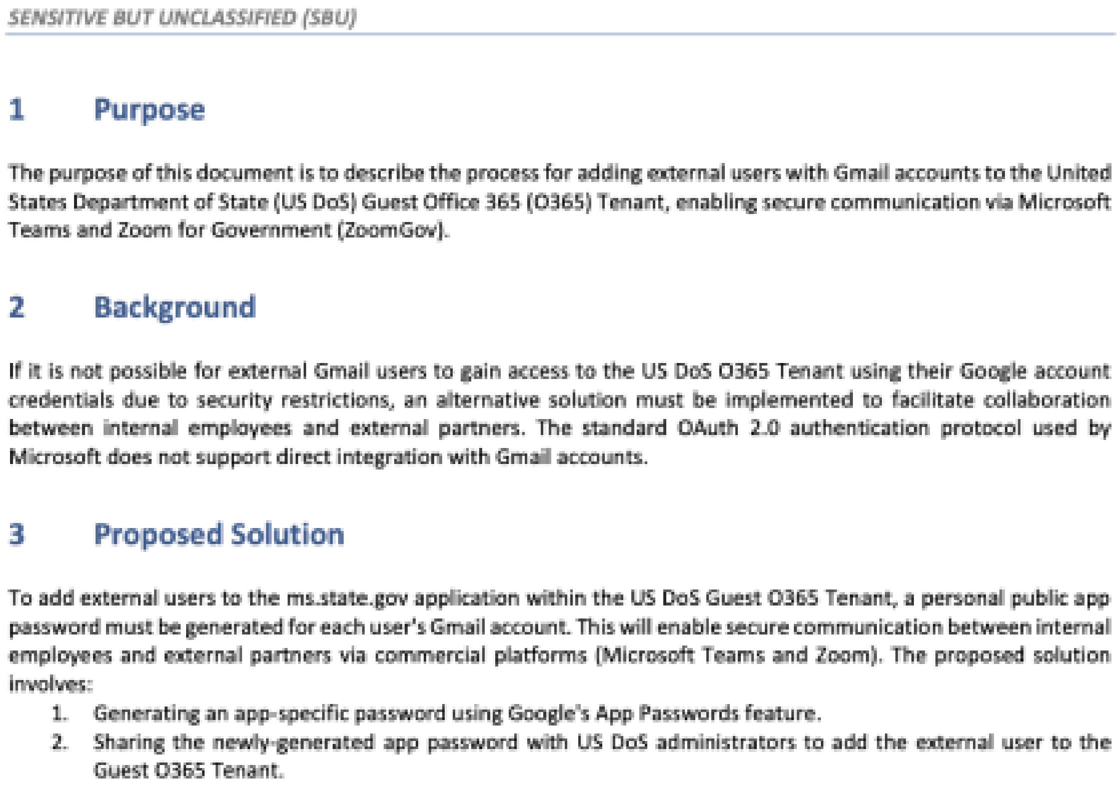
This attack hinged on deceiving Mr. Giles into believing that, by creating and sharing an App-Specific Password (ASP), he would gain access to a secure government resource enabling him to participate in the consultation.

To establish the deception, the attacker sought to persuade Mr. Giles that he was following in a process of “adding your work account... to our MS DoS Guest Tenant platform.” The document and emails outlined the procedure: creating an ASP to “enable secure communications between internal employees and external partners.”

Logic of the Deception

What you think is happening	What is actually happening
You are creating and sharing an App-Specific Password to access a “secure” State Department resource.	You are creating and sharing an ASP credential that gives the attacker full access to your account.

The attackers skillfully reframed creating and sending them an ASP as creating and sharing a code to obtain access to an application maintained by the State Department. In reality, of course, the ASP would provide them complete and persistent access to his accounts.



SENSITIVE BUT UNCLASSIFIED (SBU)

1 Purpose

The purpose of this document is to describe the process for adding external users with Gmail accounts to the United States Department of State (US DoS) Guest Office 365 (O365) Tenant, enabling secure communication via Microsoft Teams and Zoom for Government (ZoomGov).

2 Background

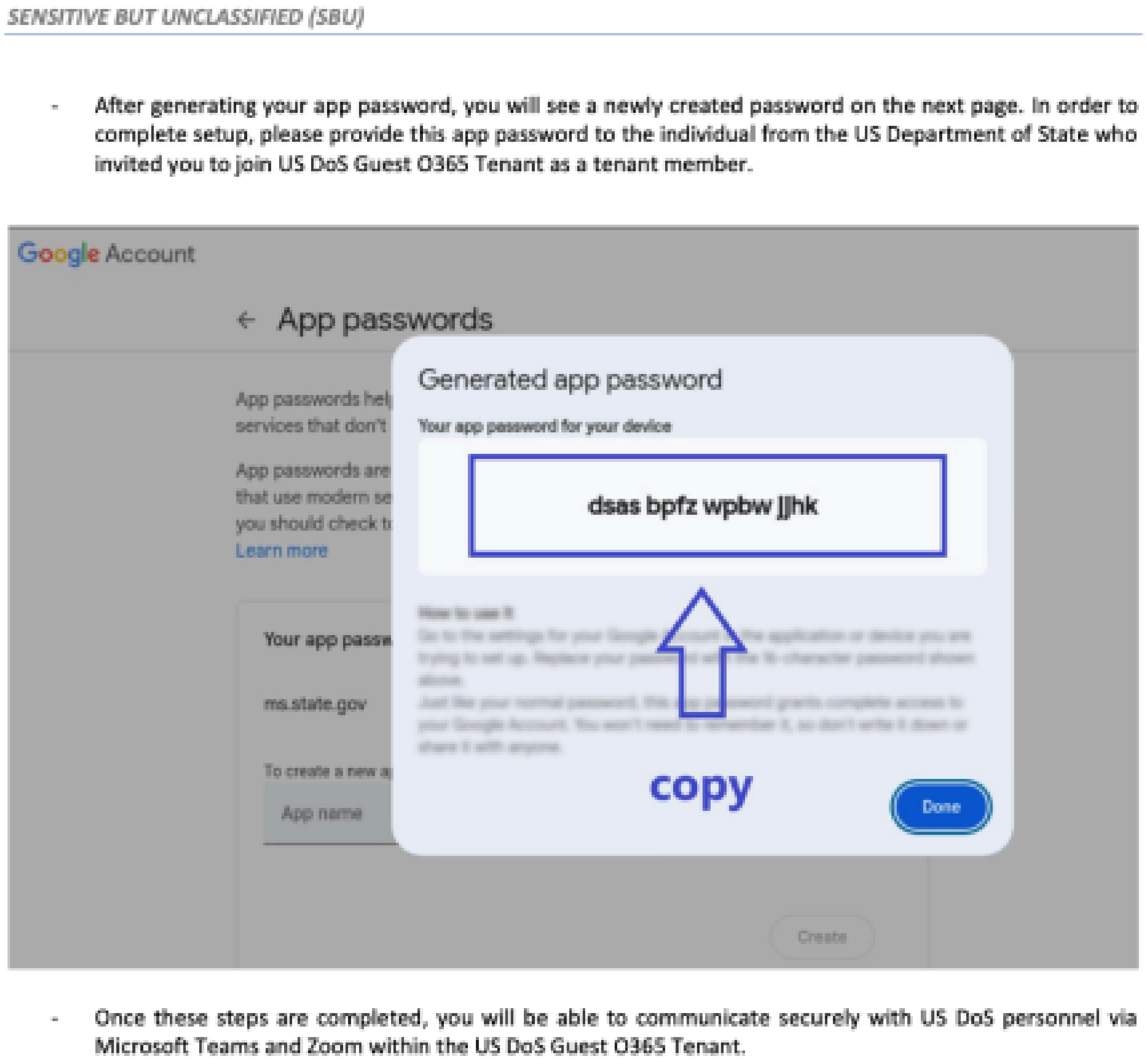
If it is not possible for external Gmail users to gain access to the US DoS O365 Tenant using their Google account credentials due to security restrictions, an alternative solution must be implemented to facilitate collaboration between internal employees and external partners. The standard OAuth 2.0 authentication protocol used by Microsoft does not support direct integration with Gmail accounts.

3 Proposed Solution

To add external users to the ms.state.gov application within the US DoS Guest O365 Tenant, a personal public app password must be generated for each user's Gmail account. This will enable secure communication between internal employees and external partners via commercial platforms (Microsoft Teams and Zoom). The proposed solution involves:

1. Generating an app-specific password using Google's App Passwords feature.
2. Sharing the newly-generated app password with US DoS administrators to add the external user to the Guest O365 Tenant.

Figure 4: Inauthentic "MS DoS" PDF provides detailed instructions on how to create an App-Specific Password



SENSITIVE BUT UNCLASSIFIED (SBU)

- After generating your app password, you will see a newly created password on the next page. In order to complete setup, please provide this app password to the individual from the US Department of State who invited you to join US DoS Guest O365 Tenant as a tenant member.

- Once these steps are completed, you will be able to communicate securely with US DoS personnel via Microsoft Teams and Zoom within the US DoS Guest O365 Tenant.

Figure 5: A page from the "MS DoS" PDF that includes a screenshot instructing the user to copy their ASP and provide it to the individual at the State Department who invited them to join the platform.

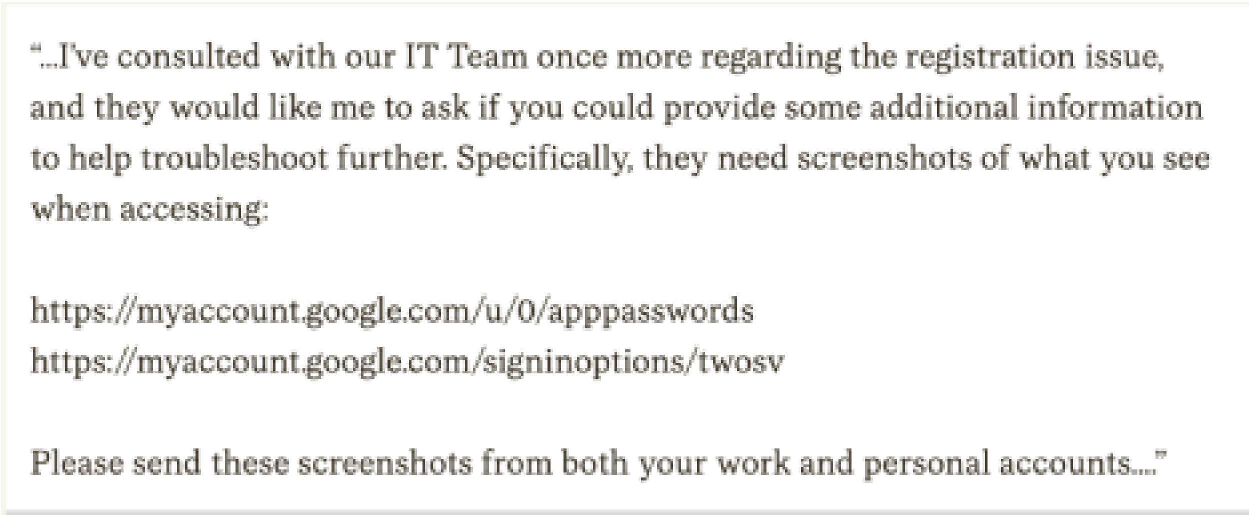
The workflow has many aspects designed to enhance plausibility, especially for a user unfamiliar with how App-Specific passwords work. For example, the attacker instructed Mr. Giles to enter "ms.state.gov" into the "App name" field of Gmail's App passwords page. In the context of the deception, the goal was to deceive him into believing that he was adding an official state.gov application. In fact, the "ms.state.gov" text is meaningless beyond furthering the ruse. Adding the text merely creates a label for the ASP that was viewable only to him in a field that accepts arbitrary text.

Flexible Attackers: Ensuring the Compromise

One factor that Mr. Giles cites as helping to preserve the credibility of the deception is what he describes as its “unhurried pacing.” Indeed, the interaction unfolded over more than 10 exchanges across several weeks, indicating substantial patience on the part of the attacker.

The attackers were also ready with answers and prepared to adapt in response to Mr. Giles’ replies. For example, after Mr. Giles stated that the initially proposed time would not work, the attackers chose to not explicitly add pressure or urgency, instead suggesting that they set up the platform for the future.

Meanwhile, when Mr. Giles managed to follow the procedure with a separate account that he had access to, the attackers then nudged him towards performing the same procedure on the accounts that they were presumably targeting.



“...I've consulted with our IT Team once more regarding the registration issue, and they would like me to ask if you could provide some additional information to help troubleshoot further. Specifically, they need screenshots of what you see when accessing:

https://myaccount.google.com/u/0/apppasswords
https://myaccount.google.com/signinoptions/twosv

Please send these screenshots from both your work and personal accounts....”

Figure 6: The attacker’s message to Mr. Giles when he encountered difficulty in accessing Google’s ASP console for specific accounts. The attackers provided him with links to check and requested screenshots, enlisting him in troubleshooting the social engineering.

Similarly, when Mr. Giles initially experienced some difficulties in creating ASPs, the attackers worked with him to ensure that he was able to successfully create them, as shown in the excerpted exchange in Figure 6.

Attack Impact

This was a highly sophisticated attack, requiring the preparation of a range of fake identities, accounts, materials and elements of deception. The attacker was clearly meticulous, to the extent that even a vigilant user would be unlikely to spot out-of-place elements or details.

Ultimately, Mr. Giles' was successfully socially engineered into creating and providing the attacker with several ASPs on multiple accounts. Google later identified the attack, locked down the impacted accounts, and disabled the attacker email.

Mr. Giles, upon recovering his accounts and inspecting his account activity logs, found a notification indicating a suspicious login attempt on one of his accounts on June 4, 2025, associated with the following Digital Ocean IP:

```
178.62.47[.]10
```

Mr. Giles has publicly shared his suspicion that the material exfiltrated from his accounts is likely to be manipulated and selectively released as part of a future information operation. This seems likely based on the identity of the attacker, and their long track record of similar operations. Such information operations often bury falsehoods in forests of facts, adding credibility to misleading narratives

Google's Response

The Google Threat Intelligence Group (GTIG) published a blog post that identifies this attacker as the Russian state-sponsored actor UNC6293, and they make a low-confidence association to APT29 / ICECAP (historically known as "Cozy Bear").

Beyond the attack on Mr. Giles, GTIG has identified a second campaign by UNC6293 leveraging the same tactics, including Ukrainian themes.

We note that GTIG's blog post contains additional indicators associated with a residential proxy used by the attackers.

Protecting Yourself and Your Organization

App-Specific Passwords can provide value to users, but as UNC6293 has figured out, they can also be leveraged for account compromises like the case described here. While certain security risks of ASPs are known, we have not previously investigated a social-engineering attack targeting them. However, many services similar to Gmail also support ASPs (including Apple ID accounts), and we expect that future attacks are likely to attempt similar ruses.

Use Google's Advanced Protection Program

Everyone should use Multi-Factor Authentication (MFA) on every account where it is available. However, some people are at greater risk of being targeted. This especially applies to individuals and organizations in civil society, particularly those working on or around conflicts, litigation, advocacy, and other high-profile topics. For these individuals, who are at greater risk because of who they are or what they do, we recommend enrolling in Google's Advanced Protection Program. We think this program would help block similar attacks to what we described here.

Be Mindful of Changing Social-Engineering Tactics

Attackers are constantly adjusting their tactics. In this attack, for example, the unhurried pace of the conversation, the responsive back and forth communications, and the presence of other .gov emails on the CC line all deviated from what many users typically expect from phishing emails. This illustrates the lengths a sophisticated attacker may go to compromise a high-value target.

We urge everyone to exercise caution when reading an unsolicited email or message. Whenever you find yourself in an exchange that asks you to share information from your account, or modify settings, make sure you know who you are communicating with. One of the best ways to do this is to verify the communication 'out-of-band' (e.g. with a phone call to a person's workplace) before moving forward.

Security Teams: Watch Out for ASPs

For organizations, we recommend ensuring that you are aware of the services where users may enable ASPs, and ensure that they are disabled unless needed for specific users or use cases. Adding education about ASPs to user security programs, including the implications for personal accounts, will likely be helpful.

For organizations that use Google Workspaces, progress is being made to improve user security. Google is clearly aware of the risks from ASPs and LSAs, and in Google Workspaces has implemented a plan to phase them out in a process that was first announced in 2019.

Google's choice to phase out ASPs for Less Secure Apps (LSAs) on Google Workspaces is a sensible measure. We recognize that for regular Gmail users, Google may still be seeking to balance security with the diversity of LSAs on which their global userbase still depends. Thus, the risk continues for regular Gmail users who may be tricked by similar campaigns.

Recommendations for Providers

Attackers constantly learn from each other, and while this is the first case of ASP-social engineering we have seen, it is unlikely to be the last.

Google caught this attack and locked down Mr. Giles' accounts, notifying him that they had identified suspicious activity. We believe that adding additional warning text or an explanatory interstitial on the "App passwords" page alerting users of the possibility that attackers may target ASPs would be helpful. We suggest that other providers that offer ASPs consider taking similar steps.
We also think it would be useful for users to be regularly nudged about whether their accounts have any ASPs enabled, as well as potentially adding a visible approval step once the first connection is made using a new ASP.