VITALS
A product by Innova Group

PLAYBOOK

A sign-in method nobody can account for

A passkey, security key, temporary access pass or Authenticator registration appears in the audit log, and the person whose account it is on did not add it — or an administrator's account gained one and the administrator does not remember doing it.

Treat it as an intrusion in progress until shown otherwise. The attack this playbook exists for begins with exactly this entry: a phone call from "IT" about passkeys, a walk-through, and a credential the caller controls registered against a real account. From the moment it exists, every sign-in with it is genuine, multi-factor is satisfied, and what follows — bulk reads through Microsoft Graph, SharePoint and OneDrive downloads, mailbox collection — leaves nothing on the identity side to stop it.

GOES WITH	DATE	PREPARED BY
The Credential Registration finding	11 September 2026	Innova Group

The order below matters. Removing the method first and asking questions afterwards costs nothing if it was a new phone. The other way round costs the estate.

hello@innovagroup.tech · innovagroup.tech

PLAYBOOK

A sign-in method nobody can account for

The first hour

Do these in order, for every account involved. Fifteen minutes per account if the people are available.

1. Cut the access.

- Entra admin centre → Users → the account → **Authentication methods** → delete the method that cannot be accounted for. If the account is an administrator, delete every method registered in the window and re-register the ones the person confirms in person.
- **Revoke sessions** on the account (Users → the account → Revoke sessions). This invalidates every refresh token; anything the attacker holds stops working within the hour.
- **Reset the password** — not because the password was necessarily taken, but because the attacker may have been given a chance to set one during the walk-through.
- If a **temporary access pass** was issued and cannot be accounted for, delete it, and revoke sessions on the *issuing* administrator's account as well. A helpdesk account issuing passes nobody asked for is a helpdesk account somebody else is driving.

2. Look at what the account did after the registration.

- **Sign-in logs** (Entra → Monitoring → Sign-in logs, filter to the account, from the registration time). Note every location, device and application that is not the person's usual. An interactive sign-in from a new country using the new method is confirmation, not suspicion.
- **Mailbox rules** — a forward to an outside address or a rule that deletes anything mentioning "invoice" or "payment" is the standard second move. Remove any that the owner does not recognise.
- **Sharing and downloads** — the SharePoint and OneDrive activity reports for the account (Microsoft 365 admin centre → Reports → Usage), and the unified audit log if it is on (Purview → Audit, search FileDownloaded, FileSyncDownloadedFull, SharingSet for the account since the registration). Anything synced or shared to an address outside the organisation in that window is assumed taken.
- **Consented applications** — Entra → Enterprise applications, filter by created date. A third-party application consented by the account in the window holds access that survives everything in step 1. Remove it.

3. Decide whether it is one account. The same caller works a list. Search the directory audit log for every *registered security info* and *admin registered security info* event in the same 48 hours (Entra → Monitoring → Audit logs, service *Authentication Methods*). Each account on that list goes through steps 1 and 2.

The first day

Talk to the person. Not as an accusation — as the fastest way to know what happened. Ask what the caller said, what they were asked to read out or approve, and whether anyone else in the team had the same call. The script tends to be consistent, and the second person it was used on has usually not reported it.

Close the door it came through. Whatever let the registration happen from the attacker's machine is still open:

- If there is no Conditional Access policy on the *Register security information* user action, create one requiring a compliant device, a trusted location, or a phishing-resistant authentication strength. Keep a temporary access pass as the deliberate exception for people registering their first method.
- If there is one and it only requires MFA, change the grant. The employee satisfied that prompt because a caller asked them to; it is not the control that stops this.
- Set temporary access passes to one-time use and an hour's lifetime.
- Disable text message and voice as registrable methods if anyone still can.

Tell the people who need to know. Whoever owns the data the account could reach — finance for a finance account, HR for HR. If the account could read customer data and step 2 found downloads or external shares, the decision about notification is a legal and contractual one and needs to be made by the person accountable for it, that day, with what is known written down.

The first week

- Re-run the assessment. The Credential Registration dimension will show whether the registration controls are now in place and whether any further methods have appeared.
- Review every temporary access pass issued in the last 30 days and confirm each went through the joiner or reset process.
- Check the accounts that *issue* passes are the ones meant to be issuing them, and that those accounts hold a phishing-resistant method themselves. The helpdesk is the target that pays best.
- Decide who reads the security-info audit events weekly, and put it in their diary. It takes a minute and is the only place this shows up.

What this is not

Not a forensic investigation, and not a substitute for one where the account could reach regulated data. It is what an organisation with no security team can do in the first hours, in the right order, so that the forensic question — if it comes — is "what was taken" rather than "what is still being taken".

Where an administrator account was involved, or where step 2 found downloads, external shares or a consented application, that is the point to bring in someone whose job this is. Our Secure practice at Innova Group can do that or can help you brief whoever you use.