

Check who has access to your Microsoft 365 email

Third-party apps can keep access to company emails and files for years, even after you stop using them.

WHAT IS INSIDE

- ☐ 6 access checks for your IT team
- ☐ Ready-to-send message for your IT provider
- ☐ Breach steps and a decision worksheet

For: Owners, managers, IT leads and finance staff at Ukrainian companies



The last 2 pages are for printing



Veiltrack

Independent security testing

The situation

Unused backup apps may still access Microsoft 365 without employee passwords.

In October 2026, attackers used stolen ConnectWise Cloud Backup app credentials and existing permissions. Huntress reported at least 162 affected Microsoft 365 environments. Not all third-party apps were affected.

The owner approves decisions. IT reviews access, makes changes and verifies results. Use one worksheet per app.

01 / 06

Find connected third-party apps

Open Entra → Enterprise applications. Compare apps with company services. Note unfamiliar ones.

An app has access, but nobody knows who connected it.

→ IT records the app's name and ID and identifies who connected it.

02 / 06

Find out who uses the app

Ask the department head or contractor why the app is needed, who uses it and when it was last used. Record the answer.

Nobody can explain why the company needs the app, yet it still has access.

→ The owner assigns someone to establish the app's purpose and the impact of disconnection.

03 / 06

HIGH RISK

Check email and file access

Open Entra → Enterprise applications → Permissions. Check email and file access. Note unnecessary permissions.

- | The app can access or change data beyond its needs.
- **The responsible person confirms required access. IT removes agreed unnecessary permissions and tests the service.**

04 / 06

HIGH RISK

Check unnecessary admin access

Open Entra → Roles and administrators. Identify apps allowed to manage email or other services.

- | An app can manage Microsoft 365 without a justified need.
- **IT reviews permissions, obtains approval, removes unnecessary access and verifies the result.**

05 / 06

HIGH RISK

Review third-party app sign-ins

Open Entra → Sign-in logs → Service principal sign-ins. Compare times and sources with expected activity.

| An app signs in from an unexplained source.

→ IT investigates unusual sign-ins and immediately restricts confirmed unauthorised access.

06 / 06

Plan how to stop access

Ask IT how to stop access and whether backups, email recovery or essential services depend on it.

| Nobody knows how to disconnect the app safely.

→ The owner approves any planned change. IT implements it when needed and verifies the result.

What should we decide for each app?

Keep

Confirm the need. IT reviews permissions and available sign-ins. The owner approves continued use and the next review date. Record who decided.

Change permissions

Confirm required access. The owner approves changes. IT removes unnecessary permissions using a supported method, tests the service and records results.

What should we decide for each app?

Disconnect

The owner reviews dependencies and approves. IT stops access, checks remaining connections and tests essential services. Record the date and result. Restrict confirmed unauthorised access immediately.

Unsure, decision needed

The owner assigns an investigator and deadline. IT records permissions and available sign-ins. Do not expand unexplained access. Start incident response if unauthorised use is confirmed.

What to send your IT lead or contractor

«Please list third-party apps accessing Microsoft 365 email and files, their owners, permissions and unexplained sign-ins. Flag unused apps. Recommend which to keep, change or disconnect, with assigned owners.»

DO NOT

Check service dependencies before planned disconnection. Restrict confirmed unauthorised access immediately.

● ACT NOW

If someone used an app without your permission

- 1** IT immediately restricts suspicious access. Do not delay protection to preserve records.
If unauthorised use is confirmed or strong breach evidence exists.
- 2** IT saves available sign-in records, app permissions and discovery time.
If available. Saving records must not delay restricting access.
- 3** Inform the owner and service lead. Explain which unauthorised actions are confirmed.
- 4** IT checks admin permission changes and possible unauthorised email or file access.
If relevant records are available.
- 5** IT replaces compromised credentials, checks remaining access and restores verified connections.
If a breach is confirmed or app credentials are untrusted.

Stopping access does not undo exposure. Incomplete logs cannot rule out breaches.

Fill in

Print it and fill it in by hand. One form per app or case.

Which app?

Who uses it and why?

What data can it access?

Can it manage Microsoft 365?

What did sign-ins show?

Owner's approved decision?

Who acts and by when?

What verifies the result?

Who Has Access to Your Microsoft 365 Email?

Print it and hand it to the team. Keep it in sight for 30 days and tick each day you followed it. Once it is a habit, the sheet can come down.

Review new apps, contractor changes and unused connections. One sheet per app:

- ☐ I compare connected apps with company services.
- ☐ I find out who uses the app and why.
- ☐ I check what data the app can read or change.
- ☐ I check whether apps can manage Microsoft 365.
- ☐ I review sign-ins and record the period checked.
- ☐ I know how to stop access and what to check.

30 DAYS TO A HABIT: TICK THE DAY

	Mon	Tue	Wed	Thu	Fri
WEEK 1	☐	☐	☐	☐	☐
WEEK 2	☐	☐	☐	☐	☐
WEEK 3	☐	☐	☐	☐	☐
WEEK 4	☐	☐	☐	☐	☐

Name, team:

Start:

Security questions? Write to us



Vlad Kraevsky
founder of Veiltrack

WEB

veiltrack.io

EMAIL

vlad@veiltrack.io

LINKEDIN

linkedin.com/company/veiltrack

