FIELD CHECKLIST

Check passwords, unknown logins and work computers

Criminals sell stolen passwords so others can break into business systems.

WHAT IS INSIDE

- [ ] How to find stolen password alerts
- [ ] How to check and end unauthorised logins
- [ ] What to do with an infected computer

For: Business owners, managers, accountants and IT leads · ~15 min

🖨️ The last page is for printing

Veiltrack
Independent security testing

FIELD CHECKLIST

The situation

Police from nine countries helped Europol shut down servers used by three malware programs. Authorities recovered over six million stolen login credentials sold to attackers.

An employee downloads a fake document. Malware steals saved passwords, giving an attacker access to company email.

Changing passwords may not stop unauthorised access. Check accounts, sessions and computers.

FIELD CHECKLIST

01 / 06

Check for data breach alerts

WHAT GOOD LOOKS LIKE

The responsible person checks work email addresses, reviews alerts and records results.

HOW TO CHECK

Check work email addresses on Have I Been Pwned. Review alerts and identify affected accounts.

SIGN OF A PROBLEM

A stolen password was reported, but nobody checked the account.

WHAT TO DO

Assign an owner. Enable available alerts and check affected accounts.

FIELD CHECKLIST

02 / 06

Check unfamiliar logins

WHAT GOOD LOOKS LIKE

The administrator checked unfamiliar logins with employees and recorded recognised activity.

HOW TO CHECK

Review email and system login history. Ask employees about unfamiliar devices and times.

SIGN OF A PROBLEM

An employee does not recognise a successful account login.

WHAT TO DO

Save suspicious login records. Investigate and restrict unauthorised access.

03 / 06 HIGH RISK

Isolate suspicious computers

Identify computers used with stolen passwords. Review their security alerts and malware scans.

> Malware was detected, but the employee still uses the computer.

→ **Disconnect the suspicious computer. Have a specialist inspect it.**

04 / 06 HIGH RISK

End unauthorised sessions

Review active devices and sessions. Confirm unfamiliar entries with employees and check termination options.

> An unauthorised device still accesses a business account.

→ **End unauthorised sessions. Recheck login history to confirm access stopped.**

FIELD CHECKLIST

HIGH RISK

05 / 06

Replace stolen passwords

WHAT GOOD LOOKS LIKE

The employee replaced reused passwords. The responsible person verified the changes.

HOW TO CHECK

Identify password reuse. Verify replacements and check for unfamiliar account recovery methods.

RED FLAG

The stolen password still works on a business account.

WHAT TO DO

Replace reused passwords from a trusted device. Remove unfamiliar recovery methods.

FIELD CHECKLIST

06 / 06

Enable an extra login verification step

WHAT GOOD LOOKS LIKE

Employees need more than passwords to access company email and key systems.

HOW TO CHECK

Review email and system login settings. Verify extra login checks are required for everyone.

SIGN OF A PROBLEM

Company email requires only a password.

WHAT TO DO

Enable extra login verification. Have every user test it.

FIELD CHECKLIST

READY-TO-USE SCRIPT

How to check an unfamiliar employee login

«An unfamiliar device accessed your work account. Was it you? If not, notify the responsible person immediately. Never share passwords or verification codes.»

DO NOT

Contact the employee through a trusted channel, not the suspicious account.

FIELD CHECKLIST

ACT NOW

Responding to stolen passwords or unauthorised logins

1. Restrict suspicious account access. Save login records and times.
2. Disconnect the computer. Do not enter new passwords on it.
   If the computer shows signs of infection.
3. End unauthorised sessions. Change passwords from a trusted device. Check recovery settings.
4. Check email forwarding and possible data access. Record findings.
   If unauthorised access is confirmed or its impact is unclear.

Unfamiliar logins do not necessarily indicate hacking or data theft.

VEILTRACK

Independent security testing

PRINT · TEAM HANDOUT

How to protect business accounts after passwords are stolen

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 alerts daily. Verify unfamiliar logins with employees:

- [ ] I review alerts and record suspicious accounts.
- [ ] I check unfamiliar logins with employees.
- [ ] I stop using infected computers until checked.
- [ ] I end unauthorised sessions and monitor for recurrence.
- [ ] I replace stolen passwords and check account recovery.
- [ ] I check that employees have extra login verification.

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