PERSONAL SECURITY / SAMPLE REPORT

After-click guide

Someone opened a suspicious link and entered a password.

EDITION 2026.10 FIXED EXAMPLE NO LIVE ASSESSMENT

02
ACTION ITEMS

RESULT SUMMARY

Your immediate next steps

Work through the actions that match what happened. Use the official service for account recovery.

THE FICTIONAL INPUT

Fictional answer	I opened a link
Fictional answer	I entered a password

Your action plan

Full findings and next steps are on page 02.

01 Secure the affected account through its official service

02 Stop interacting with the request

This example is an action list, not a security score or a safety verdict. Read the scope and limits with the findings.

AFTER-CLICK GUIDE / DETAILED FINDINGS

Your next steps, explained.

01

Secure the affected account through its official service

From a trusted device, change the exposed password and any accounts where it was reused. Revoke unfamiliar sessions and app access, and review recovery details.

YOUR NEXT STEP

If you shared a sign-in code, revoke sessions even if your password has not changed. Follow the provider's account-recovery process if you cannot sign in.

02

Stop interacting with the request

Close the suspicious page and use the official service directly. Do not reply with codes, passwords or more information.

YOUR NEXT STEP

Preserve messages and transaction references privately if you need to report the incident. Review your account activity and enable multi-factor authentication.

SCOPE & LIMITS

This tool does not inspect the device, confirm a compromise, recover an account or reverse a payment. For ongoing compromise, use the official provider and trusted local support.

Fixed fictional example. No check was run on your information.