IT CLUB KNOWLEDGE CENTRE

Dark-Web Alert Response Checklist

Validate, contain, investigate and document exposed information

Important: A dark-web alert is intelligence to investigate, not proof of an active breach. Validate before acting.

1 Validate

- [ ] Record date, time, source and reference
- [ ] Confirm the account or asset belongs to the org
- [ ] Confirm whether the account still exists
- [ ] Check whether the employee still works here
- [ ] Confirm whether the data appears genuine
- [ ] Check whether the exposure is historic
- [ ] Check for similarly named organisations
- [ ] Assign a named response owner

2 Secure

- [ ] Disable account where necessary
- [ ] Reset password (unique, not incremented)
- [ ] Revoke active sessions and refresh tokens
- [ ] Remove app passwords and remembered devices
- [ ] Review and remove unknown MFA methods
- [ ] Confirm MFA is enabled
- [ ] Review account recovery details
- [ ] Review privileged access

A password reset alone is not enough if an attacker holds an active session or the device is infected.

3 Investigate

- [ ] Check recent sign-ins for unfamiliar locations
- [ ] Check impossible travel or unknown devices
- [ ] Check failed login attempts
- [ ] Review mailbox forwarding rules
- [ ] Review inbox rules and delegated access
- [ ] Check OAuth app consent
- [ ] Identify the affected device
- [ ] Check for information-stealing malware

4 Assess Exposed Data

- [ ] Password
- [ ] Username / email
- [ ] Session cookie / token
- [ ] Personal data
- [ ] Customer data
- [ ] Financial information
- [ ] Source code / API key
- [ ] Remote-access credentials
- [ ] Confidential documents
- [ ] Other

5 Escalate

- [ ] Incident-response lead informed
- [ ] Senior management informed
- [ ] IT or security provider informed
- [ ] Cyber insurer informed
- [ ] Data-protection adviser consulted
- [ ] ICO notification assessed

6 Contain Related Risk

- [ ] Search for password reuse across other accounts
- [ ] Rotate related credentials
- [ ] Review similar usernames and shared accounts
- [ ] Check former-employee accounts
- [ ] Review remote-access services
- [ ] Check other domains and suppliers

7 Document the Outcome

- [ ] Alert confirmed
- [ ] Alert unconfirmed / false positive
- [ ] Historic exposure
- [ ] Active compromise
- [ ] No evidence of compromise
- [ ] Accounts secured
- [ ] Sessions revoked
- [ ] Devices reviewed
- [ ] Data-breach assessment completed
- [ ] Follow-up actions assigned

8 Prevent Recurrence

- [ ] MFA strengthened
- [ ] Password manager adopted
- [ ] Old accounts disabled
- [ ] Endpoint controls reviewed
- [ ] Monitoring profile updated
- [ ] Alert routing confirmed
- [ ] Incident exercise scheduled
- [ ] Next review date set

Dark-web monitoring is a detection layer, not a protective shield. Monitoring without strong controls and a tested

Alert Severity Guide

Informational	Old credential, known historic breach, closed account
Low	Active identity in old data, account protected by MFA
Medium	Recent credentials, password reuse suspected, supplier exposure
High	Working credential, token/cookie exposure, active remote account
Critical	Admin access for sale, initial access advertised, ransomware claim

Plain-English takeaway

Treat a dark-web alert as intelligence to investigate, not automatic proof of an active breach. Confirm the affected account or asset, change exposed credentials, revoke active sessions, investigate the device and review sign-in activity. Escalate serious findings, preserve evidence and record exactly what was checked and changed.

Scan for online guide