GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

D

Data Breach: What It Means and What to Do Next

A data breach exposes protected or sensitive information without authorization. Learn what to do based on the data involved and how organizations should contain, assess, notify, and recover.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What is a data breach?

02 Data breach vs. data leak vs. security incident

03 How data breaches happen

04 What to do if your personal data was exposed

05 Response by type of exposed data

06 What if the breached service says passwords were hashed?

07 How an organization should respond to a data breach

08 How to reduce data breach risk

09 Frequently asked questions

10 References

01 What is a data breach?

A data breach is an incident in which protected, confidential, or sensitive information is accessed, disclosed, copied, changed, lost, or made available without authorization. It can result from an external attack, a malicious insider, human error, a lost device, an exposed cloud resource, or information sent to the wrong recipient.

A breach is not limited to a hacker stealing a database. An accidentally public file, an email containing personal data sent to the wrong person, or ransomware that exposes data can also qualify. The exact legal definition and notification duties depend on the type of data, organization, and jurisdiction.

02 Data breach vs. data leak vs. security incident

Term	Meaning	Example
Security incident	An event that may threaten systems or information	An attacker accesses a server, but investigation has not yet shown data exposure
Data exposure or leak	Information is accessible where it should not be, sometimes because of error	A cloud storage folder is configured as public
Data breach	Unauthorized access, disclosure, loss, or other compromise of protected data	Customer records are downloaded or sent to an unauthorized recipient

The terms overlap in everyday use. Do not delay containment while debating the label. Record what is known, what remains uncertain, and which data may be affected.

03 How data breaches happen

- Stolen or phished credentials and weak authentication.

- Unpatched internet-facing software or insecure applications.
- Malware, ransomware, or information-stealing tools.
- Misconfigured databases, cloud storage, backups, or access controls.
- Lost or stolen laptops, phones, drives, paper records, or backup media.
- Insiders who intentionally misuse access or accidentally disclose information.
- A supplier, cloud service, or software dependency that is compromised.
- Data retained longer than needed or copied into unmanaged locations.

04 What to do if your personal data was exposed

1. **Verify the notice independently.** Breach-themed phishing is common. Visit the organization's official site or use a known phone number instead of links and numbers in an unexpected message.
2. **Find out exactly what was involved.** The response to an exposed email address differs from the response to a password, bank account, identity document, health record, or authentication secret.
3. **Secure the affected account.** Change a compromised or reused password, sign out other sessions, remove unknown recovery methods, and enable strong MFA.
4. **Watch for follow-up fraud.** Criminals can combine breached data with public information to make convincing calls, emails, and account-recovery attempts.
5. **Keep records.** Save the notification, dates, case numbers, suspicious transactions, and steps you took. These may be useful for disputes, insurance, or reports.

05 Response by type of exposed data

Data exposed	Priority actions
Password or password hash	Change that password and every reused copy; revoke sessions; enable MFA; review login and recovery activity

Data exposed	Priority actions
Email address or phone number	Expect targeted phishing, fake support calls, SIM-related scams, and password-reset attempts; verify contacts independently
Payment card	Contact the card issuer, review transactions, replace the card if advised, and enable alerts
Bank account details	Contact the financial institution through a verified channel and ask about monitoring, transfer controls, or account replacement
Government ID or national identifier	Follow the issuing authority's guidance; consider fraud alerts, credit monitoring, or a credit freeze where available
Health or insurance information	Review claims and explanations of benefits; report unfamiliar services or changes to the provider and insurer
Authentication keys, API keys, or certificates	Revoke and replace them; do not rely only on changing an account password; inspect use from the exposure date

Credit freezes and fraud alerts are country-specific. Use official consumer-protection and credit-bureau resources for your location. Paid monitoring can help detect some misuse, but it does not replace revoking exposed credentials or reviewing accounts.

06 What if the breached service says passwords were hashed?

Hashing is designed to protect stored passwords, but the risk depends on the algorithm, configuration, password strength, and information exposed with it. Treat a notified password as compromised when the organization advises a reset. If you reused it elsewhere, change those accounts too, starting with email and financial services.

07 How an organization should respond to a data breach

1. Activate the response team

Bring together incident response, security, IT, privacy or legal counsel, leadership, communications, and the affected business owners. Establish decision authority, a protected case record, and a reliable timeline.

2. Contain without destroying evidence

Isolate affected hosts, accounts, applications, or storage; stop public access; revoke compromised credentials and tokens; and block confirmed malicious activity. Preserve relevant logs, system images, cloud audit records, email, identity events, and configuration history before they expire or are overwritten.

3. Determine scope and impact

- Which systems, identities, vendors, and data stores were involved?
- What categories and approximate volume of data were accessible, copied, changed, or destroyed?
- When did unauthorized access begin and end?
- Was the data encrypted, and were the keys also exposed?
- Which people, customers, employees, partners, or jurisdictions are affected?
- Does the attacker retain access through another account, token, device, or supplier?

4. Assess notification and reporting duties

Involve qualified privacy or legal counsel early. Requirements vary by location, sector, contract, and data type, and some deadlines begin when the organization becomes aware of a breach. Coordinate notices to regulators, law enforcement, insurers, partners, and affected people without making unsupported claims.

5. Communicate clearly

State what happened, what information was involved, what has been done, what remains under investigation, and which concrete steps recipients should take. Provide a verified contact channel and warn about impersonation scams. Update the message when material facts change.

6. Recover and prevent recurrence

Remove persistence, patch the entry point, rotate secrets, rebuild systems that cannot be trusted, restore verified data, and monitor for renewed access or data misuse. Convert lessons into owners and deadlines: access reduction, logging, data retention, vendor controls, backup protection, testing, and staff procedures.

08 How to reduce data breach risk

- Know where sensitive data is stored, who can access it, and why it is retained.
- Collect and keep only the data the organization needs.
- Use least privilege, strong MFA, privileged-access controls, and prompt offboarding.
- Patch exposed systems and test applications, cloud configurations, and supplier access.
- Encrypt sensitive data in transit and at rest while protecting keys separately.
- Centralize audit logs and rehearse containment, notification, and recovery decisions.
- Maintain tested, isolated backups and a documented incident-response plan.

09 Frequently asked questions

Does a breach mean my identity has been stolen?

No. Exposure increases risk, but it is not proof of misuse. Take actions matched to the data involved and monitor for suspicious activity.

Should an organization immediately power off affected systems?

Usually isolation is safer than an unplanned shutdown because volatile evidence may be lost. Follow the incident-response and forensic team's direction, especially for business systems.

Can deleted online data still be exposed?

Yes. Copies may exist in backups, caches, logs, exports, vendor systems, or attacker collections. Removal limits continued exposure but cannot guarantee every copy is gone.

10 References

- NIST SP 1800-29: Data Confidentiality - Detect, Respond to, and Recover from Data Breaches
- U.S. FTC: Data Breach Response - A Guide for Business
- FBI IC3: Data Breach

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com