

Suspected Security Incident Report Form Template

All questions are optional. Follow each question's directions.
Write your answers to the open questions in the space provided.

Report one suspected digital security concern using general descriptions. You do not need to confirm a breach. Do not include passwords, access codes, customer data, full message contents, suspicious clickable links or files. Every field is optional. Use the organization's stated urgent reporting route if immediate attention is needed; this form alone does not guarantee a response.

1. When did you first notice the concern? Include date, approximate time, and time zone if known.

2. Which kind of concern best describes what you noticed?

- ☐ Suspicious email or message
- ☐ Unexpected sign-in or account activity
- ☐ Lost work device
- ☐ Unexpected access to information
- ☐ Unusual device or application behavior
- ☐ Another concern
- ☐ Not sure

Suspected Security Incident Report Form Template

All questions are optional. Follow each question's directions.
Write your answers to the open questions in the space provided.

3. Which work service or device type appears to be involved? Use a general name, not credentials or a full technical address.

4. What did you personally observe? Describe it briefly without copying private content, links, or files.

5. What action, if any, had you already taken before making this report?

- ☐ No action yet
- ☐ Used the organization's reporting button or route
- ☐ Opened a message or link
- ☐ Entered information in response to a message
- ☐ Contacted IT or security separately
- ☐ Another action
- ☐ Prefer not to answer

Suspected Security Incident Report Form Template

All questions are optional. Follow each question's directions.
Write your answers to the open questions in the space provided.

6. Is the concerning activity still visible to you?

- ☐ Yes
- ☐ No
- ☐ Not sure
- ☐ Cannot safely check
- ☐ Prefer not to answer

7. What approved work contact can the security team use to follow up with you?
