ActivityInfo

CyberPeace Institute

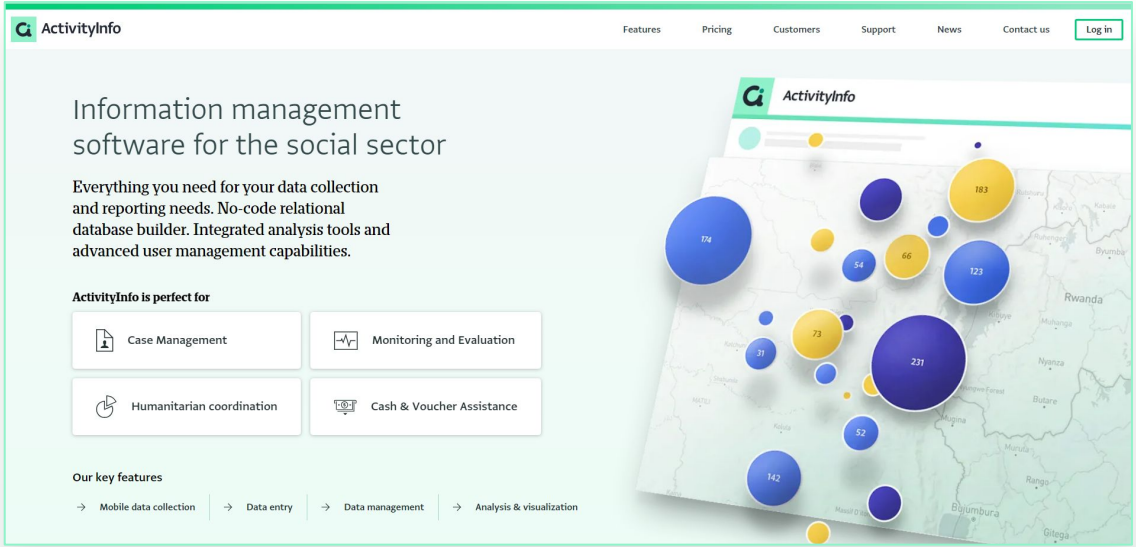
Best Practices for Cybersecurity in ActivityInfo and Beyond

Starting shortly, please wait!

Presented by the ActivityInfo Team

All in one information management software for humanitarian and development operations.

- Track activities, outcomes
- Beneficiary management
- Surveys
- Work offline/online



Outline

- **CyberPeace**
  - Practical recommendations
  - CyberPeace Builders Program

- **ActivityInfo**: Risk mitigation tools
  - Single-Sign On
  - Weekly risk report
  - Dark Web Monitoring

Introduction

Cybersecurity is the collection of technologies, processes and practices designed to protect data, devices, networks, and systems from attacks or unauthorized access.

It is every users responsibility to ensure data security and ActivityInfo provides mechanisms to help with:

Confidentiality

Ensuring that databases and form records are only accessible to authorized people.

Integrity

Ensuring that data remains accurate by preventing accidental or malicious editing of records.

Availability

Ensuring that data is accessible to authorised users when needed.

Single Sign-On (SSO)

This is an authentication process that allows a user to access multiple applications or systems with just one set of login credentials.

How to configure SSO in ActivityInfo

Advantages of SSO

Single Sign On (SSO)

- Reduces Password Fatigue
- Ease of use when logging in
- Mitigates risk of staff turnover
- Enforces your organization's two-factor requirements

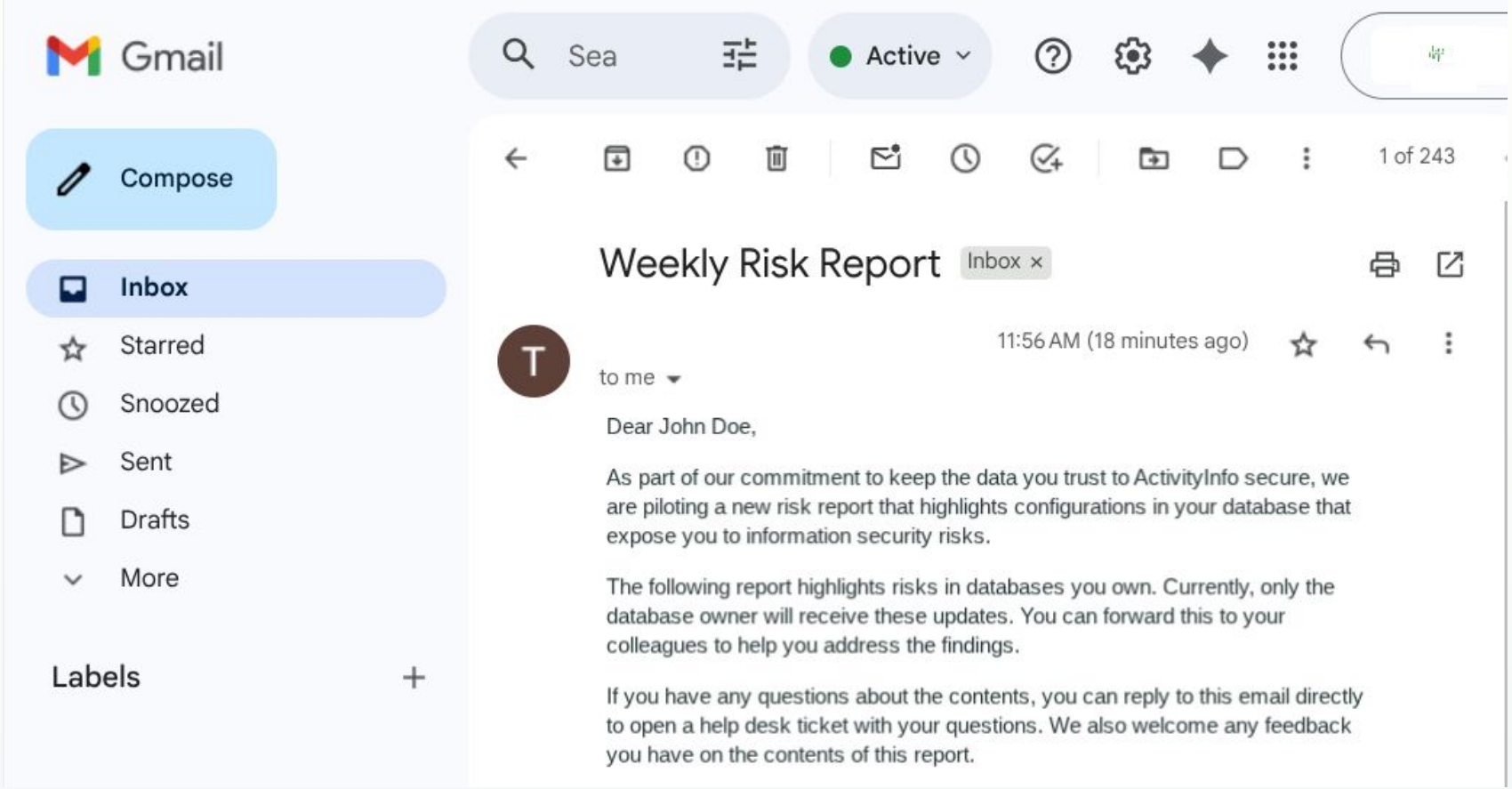
Passwords

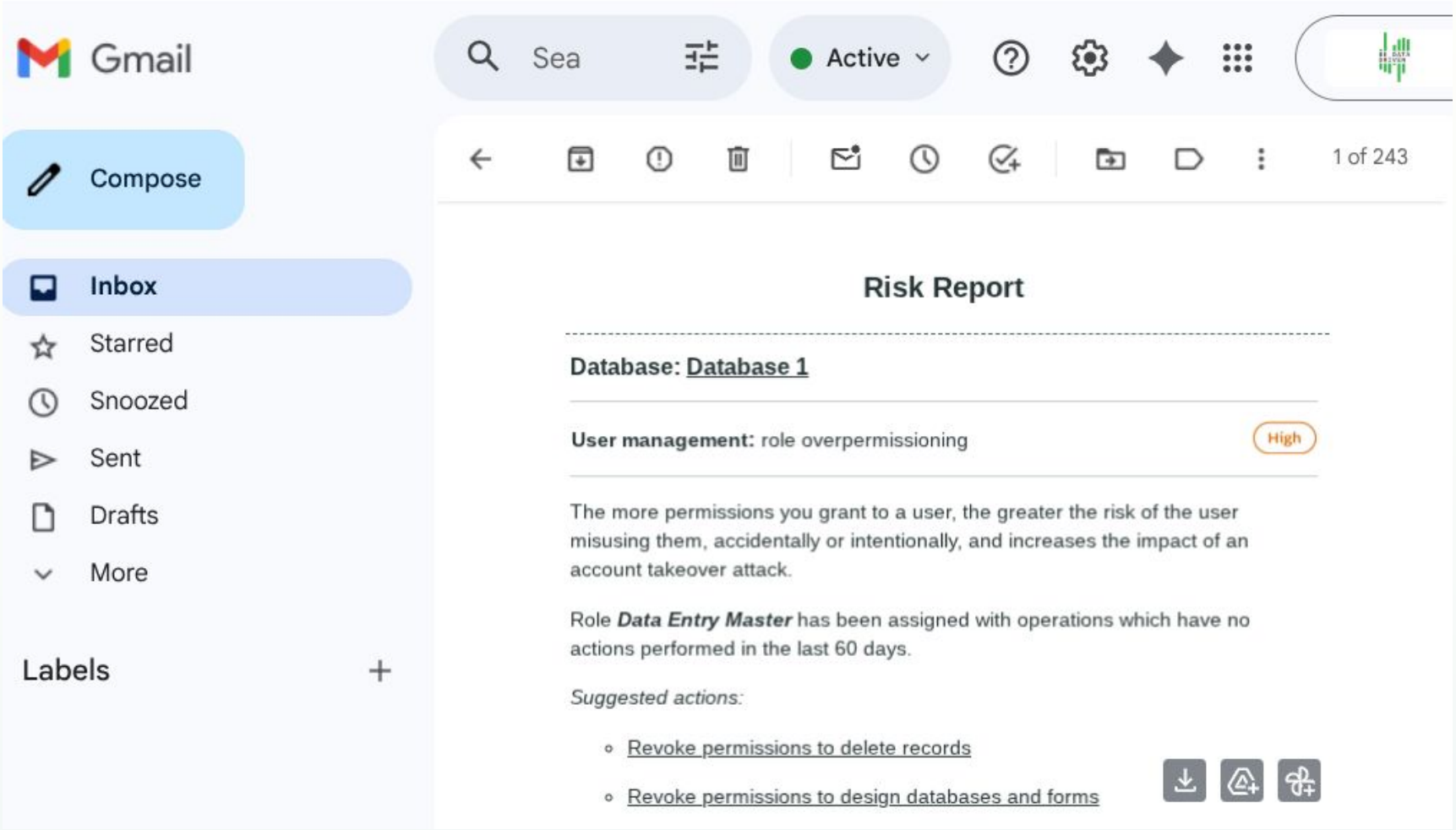
- Password Fatigue
- Repeated reset requests
- Weak passwords
- Risk of password reuse

Weekly ActivityInfo Risk Report

Database owners receive a Weekly Risk Report on Mondays that summarizes the following key indicators:

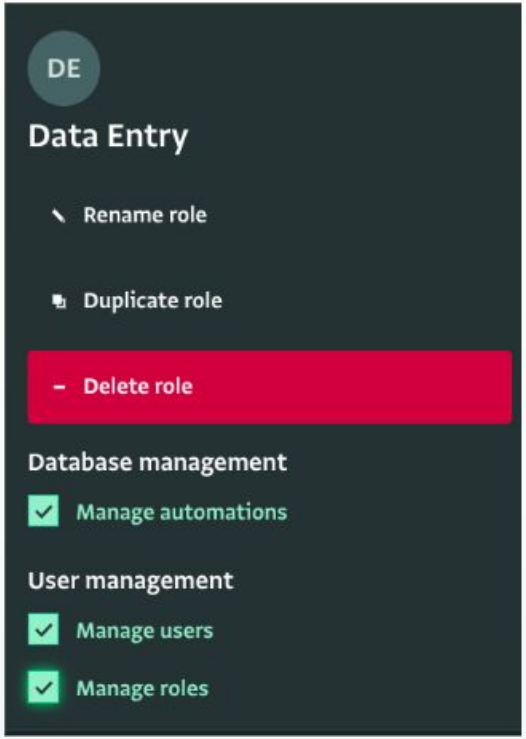
- Dormant or inactive users
- Overly permissive or shared access
- Misconfigurations that could expose data

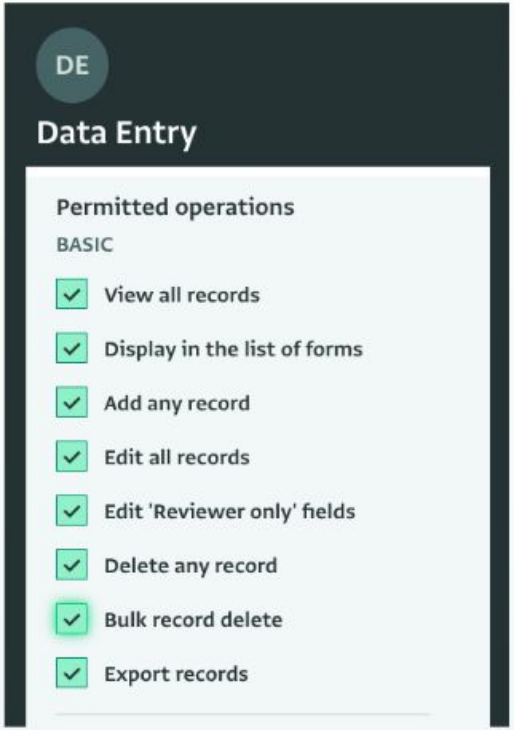

Gmail
Sea
Active
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
1 of 243
Weekly Risk Report
Inbox ×
T
11:56 AM (18 minutes ago)
to me
Dear John Doe,
As part of our commitment to keep the data you trust to ActivityInfo secure, we are piloting a new risk report that highlights configurations in your database that expose you to information security risks.
The following report highlights risks in databases you own. Currently, only the database owner will receive these updates. You can forward this to your colleagues to help you address the findings.
If you have any questions about the contents, you can reply to this email directly to open a help desk ticket with your questions. We also welcome any feedback you have on the contents of this report.


Gmail
Sea
Active
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
1 of 243
Risk Report
Database: Database 1
User management: role overpermissioning
High
The more permissions you grant to a user, the greater the risk of the user misusing them, accidentally or intentionally, and increases the impact of an account takeover attack.
Role Data Entry Master has been assigned with operations which have no actions performed in the last 60 days.
Suggested actions:
Revoke permissions to delete records
Revoke permissions to design databases and forms

High-impact permissions

- Delete
- Bulk delete
- Share reports
- Manage users
- Manage roles



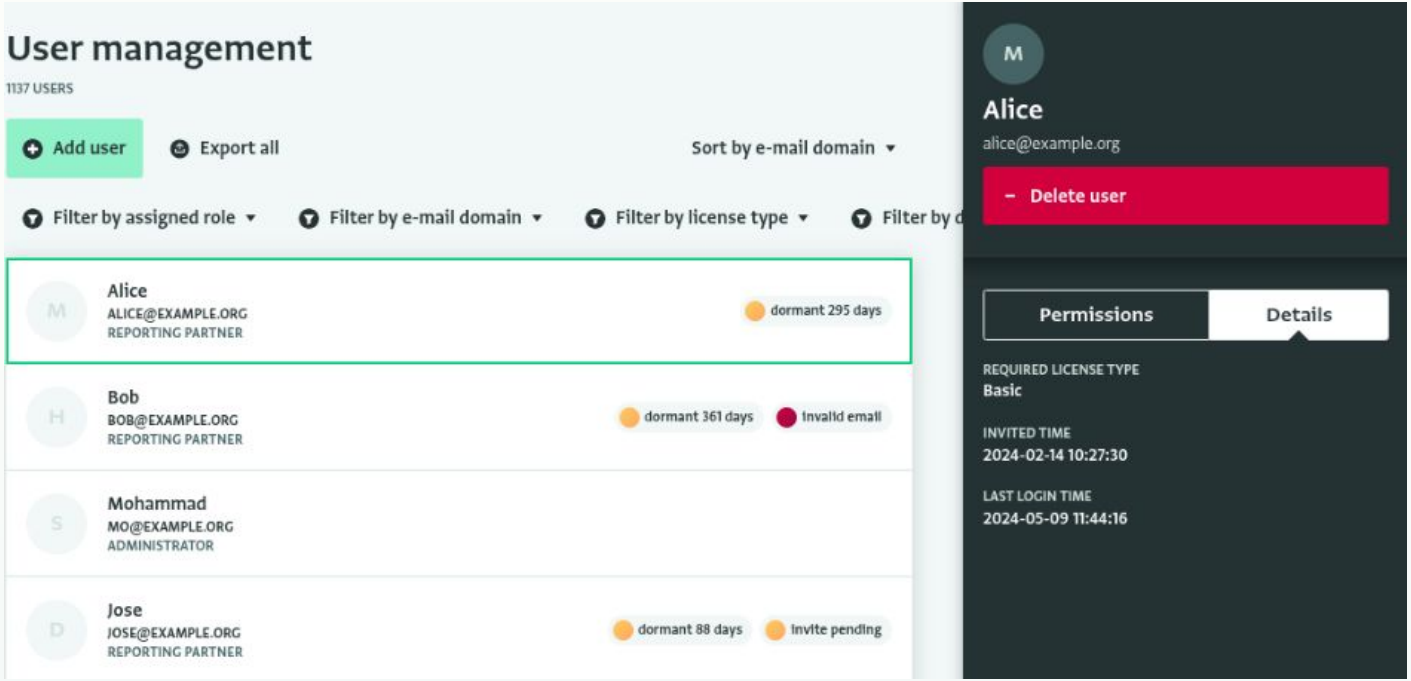


More permissions tools

- Record-level permissions (conditions)
- Assigning users to specific records (user fields)

Understanding roles and permissions in ActivtityInfo

Dormant Users = Hidden Risk

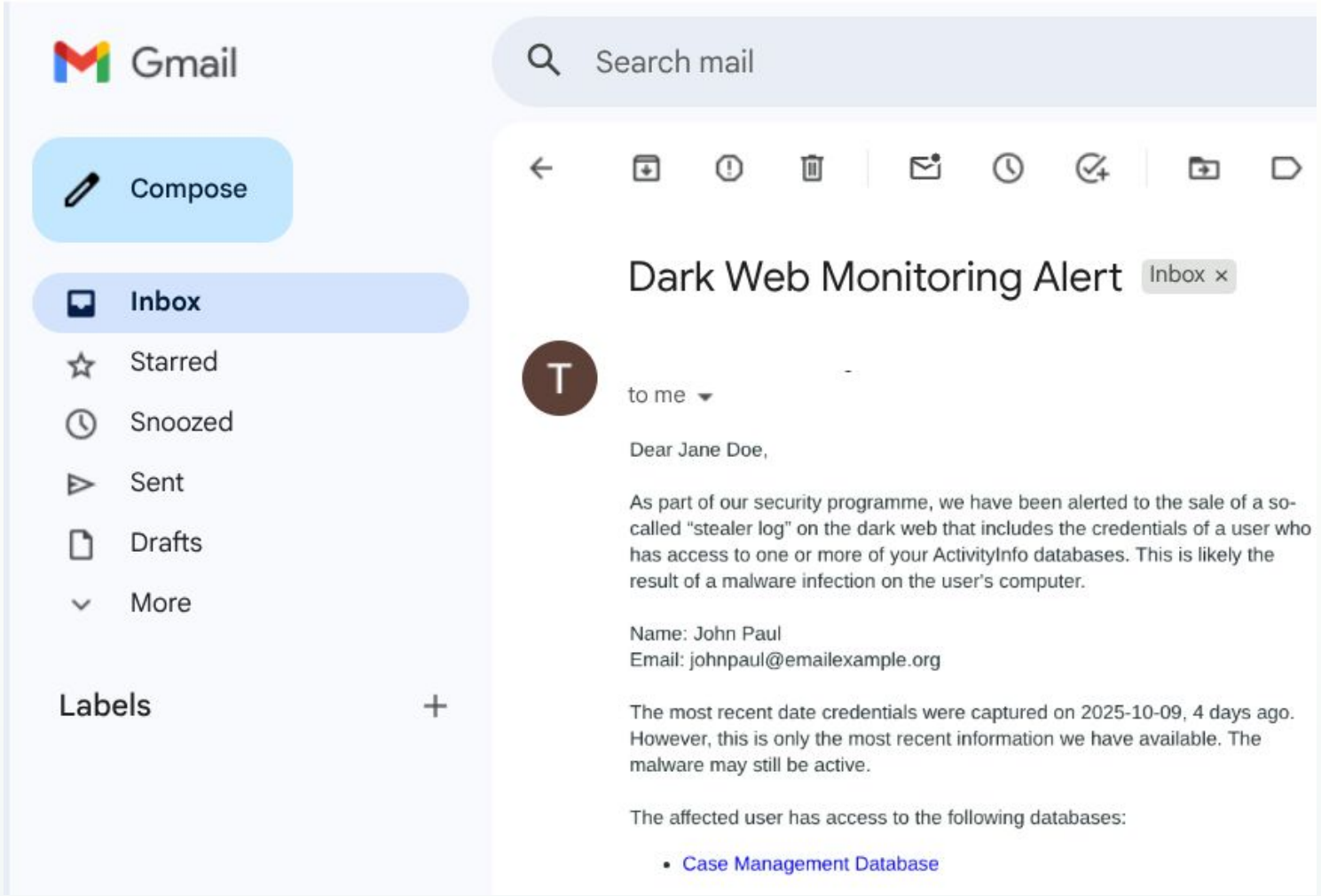


ActivityInfo
BY BEDATADRIVEN

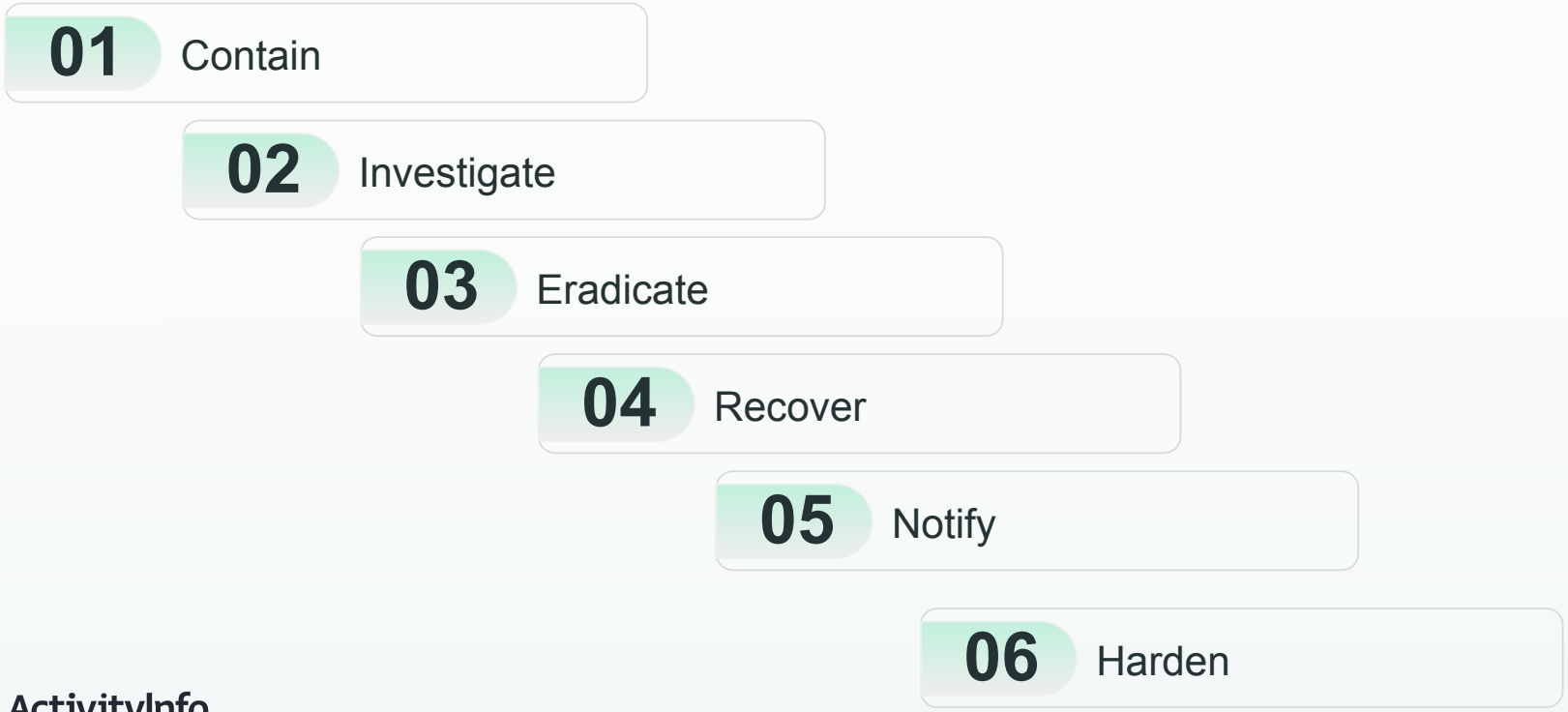
Marketplace for stolen credentials

A “**Stealer Log”** is a file created by “**Infostealer”** malware such as RedLine, Raccoon, Titan, Aurora, etc., that lists saved passwords, cookies, autofill data, and IP addresses taken from an infected device. This information is up for sale on the “**Dark Web**”.

ActivityInfo
BY BEDATADRIVEN


Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
Dark Web Monitoring Alert
Inbox ×
T
to me
Dear Jane Doe,
As part of our security programme, we have been alerted to the sale of a so-called “stealer log” on the dark web that includes the credentials of a user who has access to one or more of your ActivityInfo databases. This is likely the result of a malware infection on the user’s computer.
Name: John Paul
Email: johnpaul@emailexample.org
The most recent date credentials were captured on 2025-10-09, 4 days ago. However, this is only the most recent information we have available. The malware may still be active.
The affected user has access to the following databases:
Case Management Database

Stealer Log Incident Response



Questions?

Follow us:

LinkedIn page: https://www.linkedin.com/showcase/activityinfo/
LinkedIn group: https://www.linkedin.com/groups/5098257/