ActivityInfo

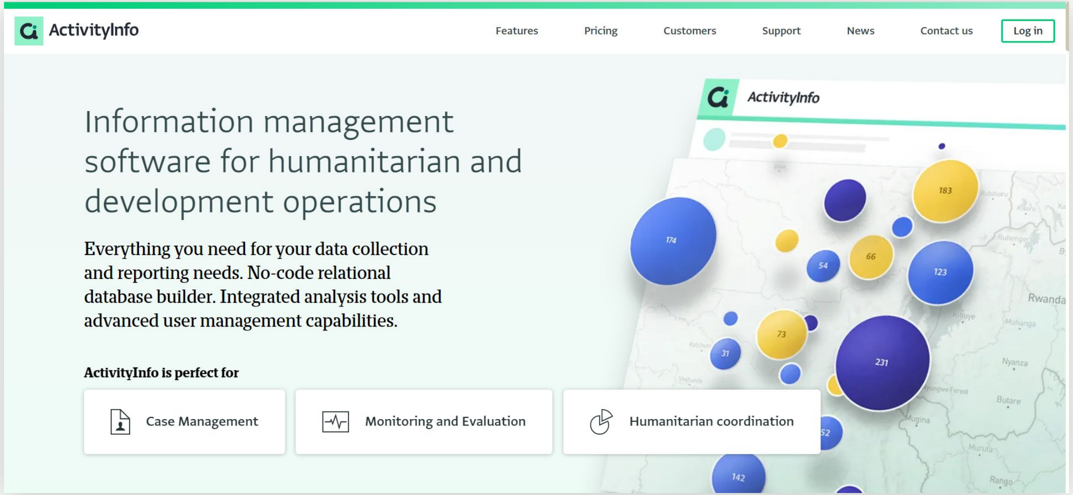
Top 5 data security risks for M&E professionals and what you can do about them

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



Information management software for humanitarian and development operations

Everything you need for your data collection and reporting needs. No-code relational database builder. Integrated analysis tools and advanced user management capabilities.

ActivityInfo is perfect for

ActivityInfo

Data security two webinar sessions

Cybersecurity Awareness month

OCT 5

SESSION 1

Top 5 data security risks for M&E professionals and what you can do about them

OCT 12

SESSION 2

Data protection in practice - Best practices for designing Roles in ActivityInfo

Outline

01 Introduction to data security

02 Top 5 data security risks and Mitigation

03 Q/A session

What is data security?

Confidentiality

Confidential data exposed to unauthorized parties

Integrity

Data changed without your permission

Availability

Ensuring data is available when needed

What role does the M&E professional play in data security?

- Planning M&E systems
- Planning data collection
- Sharing data with internal and external stakeholders
- Communicating results

Top five risks to data security

05 Social engineering

04 Password management

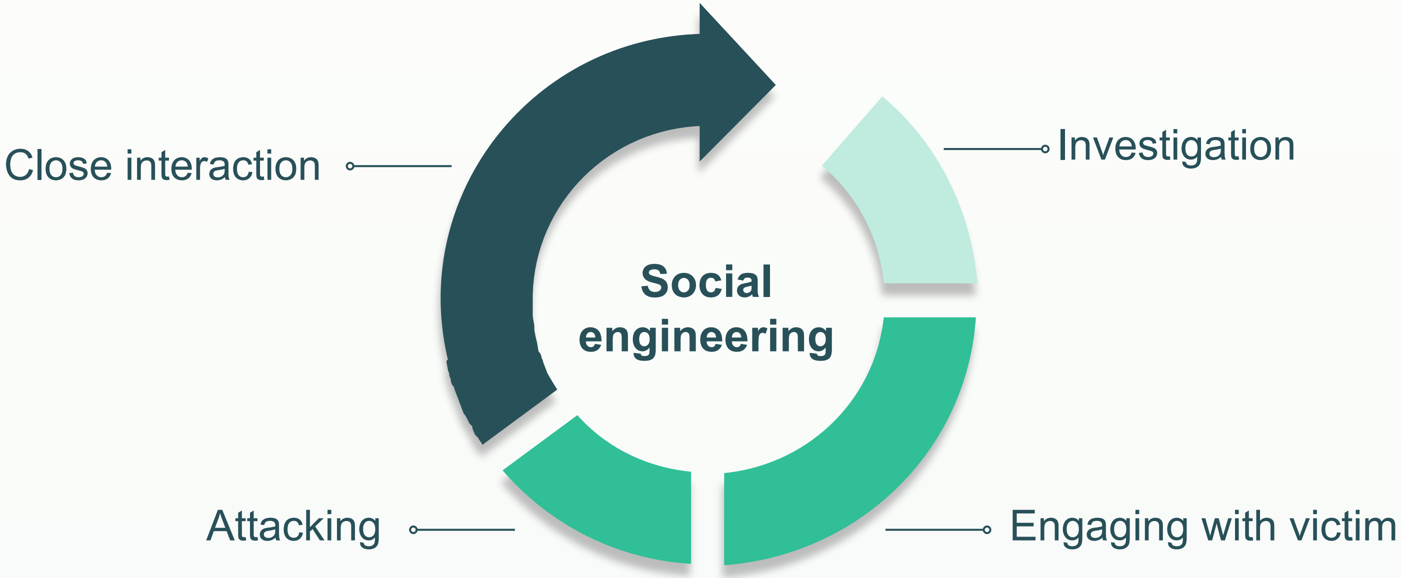
03 IT operations error

02 Insider attacks

01 User error

05
Social engineering

Social engineering: How does it happen?



ActivityInfo

Types of social engineering

Phishing

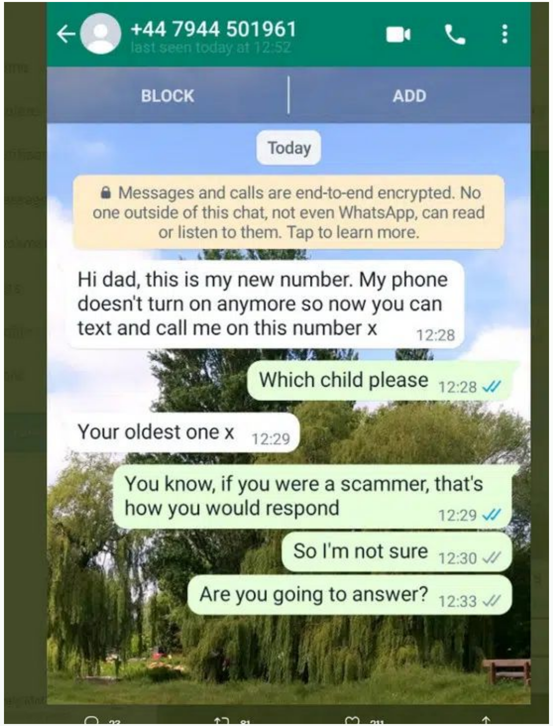
- Attackers impersonate legitimate businesses
- Urgency created by presenting consequences
- Rely on spamming large groups

Types of social engineering

Spear-Phishing

- Sophisticated form of phishing
- Extensive research to the target
- Impersonating a trusted partner

Whatsapp Fraud



🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hi dad, this is my new number. My phone doesn't turn on anymore so now you can text and call me on this number x 12:28

Which child please 12:28

Your oldest one x 12:29

You know, if you were a scammer, that's how you would respond 12:29

So I'm not sure 12:30

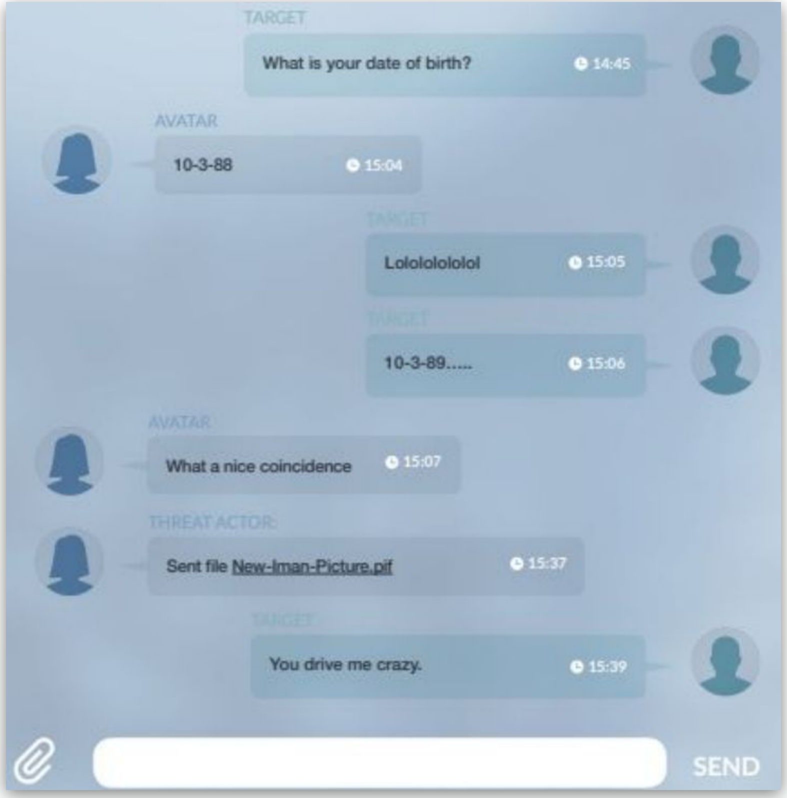
Are you going to answer? 12:33

ActivityInfo

Social engineering

2013, Syrian opposition forces and humanitarians targeted via Skype. Stolen data included:

- Humanitarian needs assessments
- Lists of materials for the construction of major refugee camps
- Humanitarian financial assistance disbursement records



TARGET
What is your date of birth? 14:45

AVATAR
10-3-88 15:04

TARGET
Lolololololol 15:05

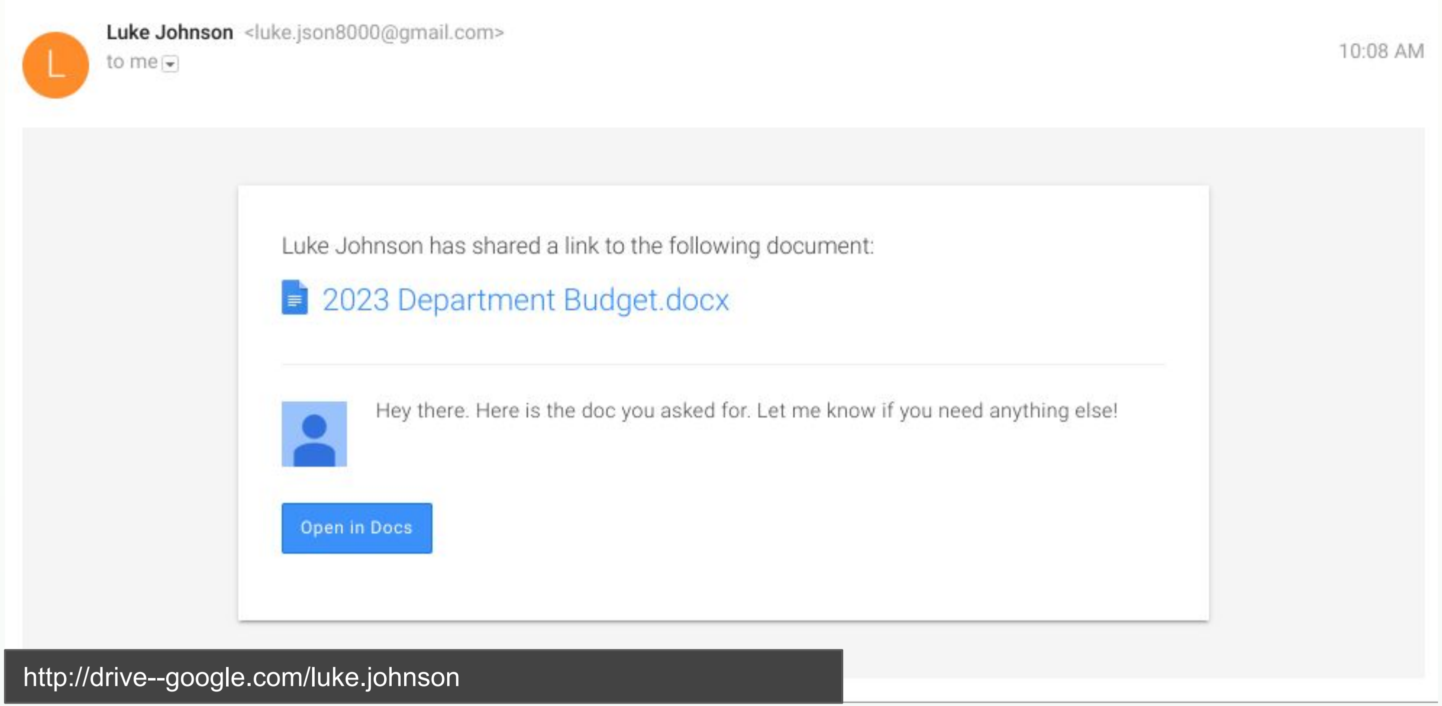
TARGET
10-3-89..... 15:06

AVATAR
What a nice coincidence 15:07

THREAT ACTOR:
Sent file New-Iman-Picture.pif 15:37

TARGET
You drive me crazy. 15:39

Real or phishing?



Luke Johnson <luke.json8000@gmail.com>
to me

10:08 AM

Luke Johnson has shared a link to the following document:

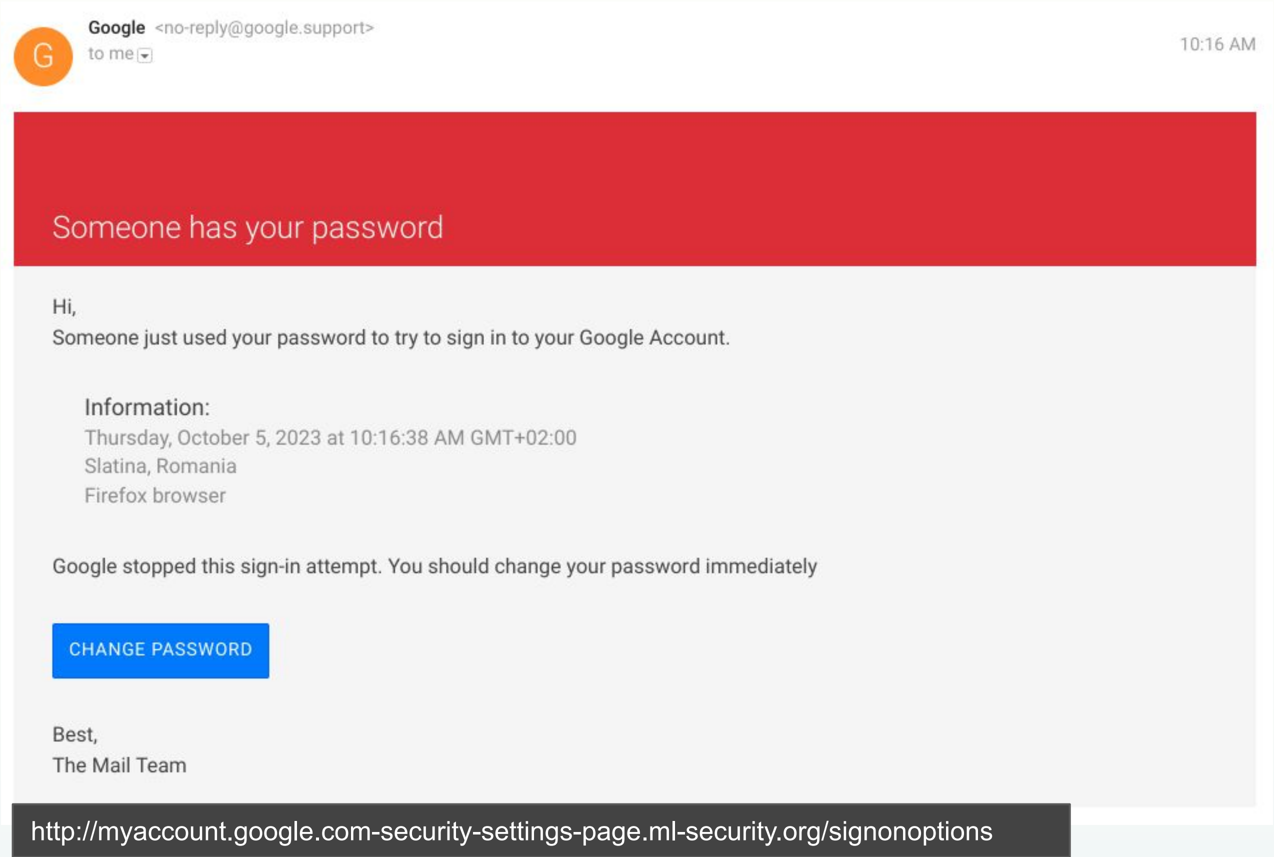
2023 Department Budget.docx

Hey there. Here is the doc you asked for. Let me know if you need anything else!

http://drive--google.com/luke.johnson

ActivityInfo

Real or phishing?



Google <no-reply@google.support>
to me

10:16 AM

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Thursday, October 5, 2023 at 10:16:38 AM GMT+02:00
Slatina, Romania
Firefox browser

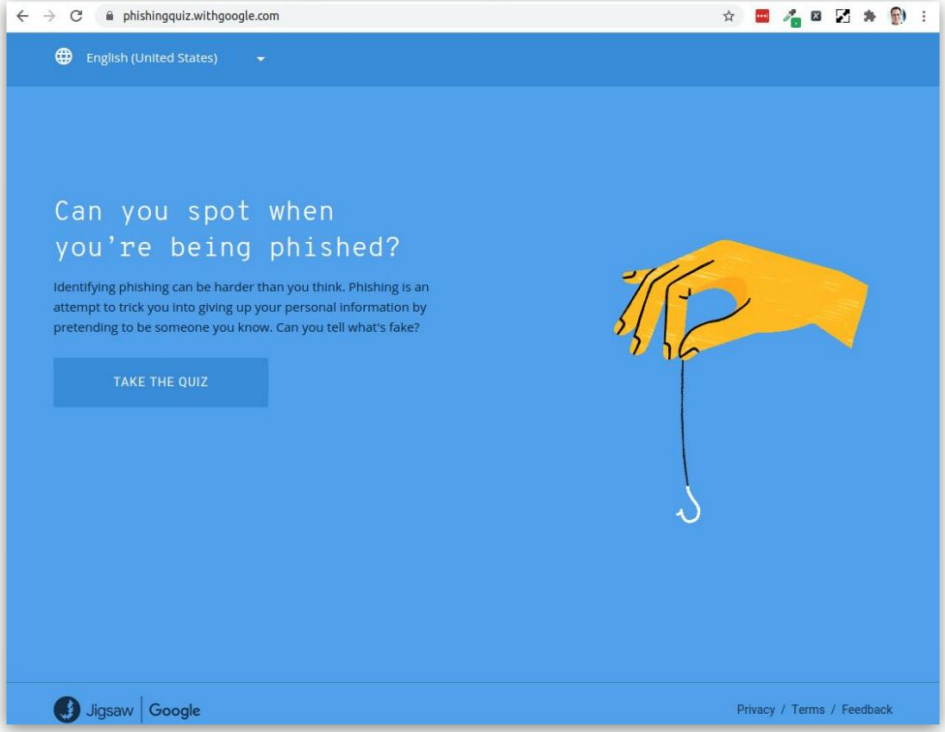
Google stopped this sign-in attempt. You should change your password immediately

Best,
The Mail Team

http://myaccount.google.com-security-settings-page.ml-security.org/signonoptions

Mitigation: social engineering

- ✓ Training and awareness
- ✓ Check the sources!
- ✓ Confirm through an additional channel
- ✓ Don’t rush it!



Can you spot when you’re being phished?

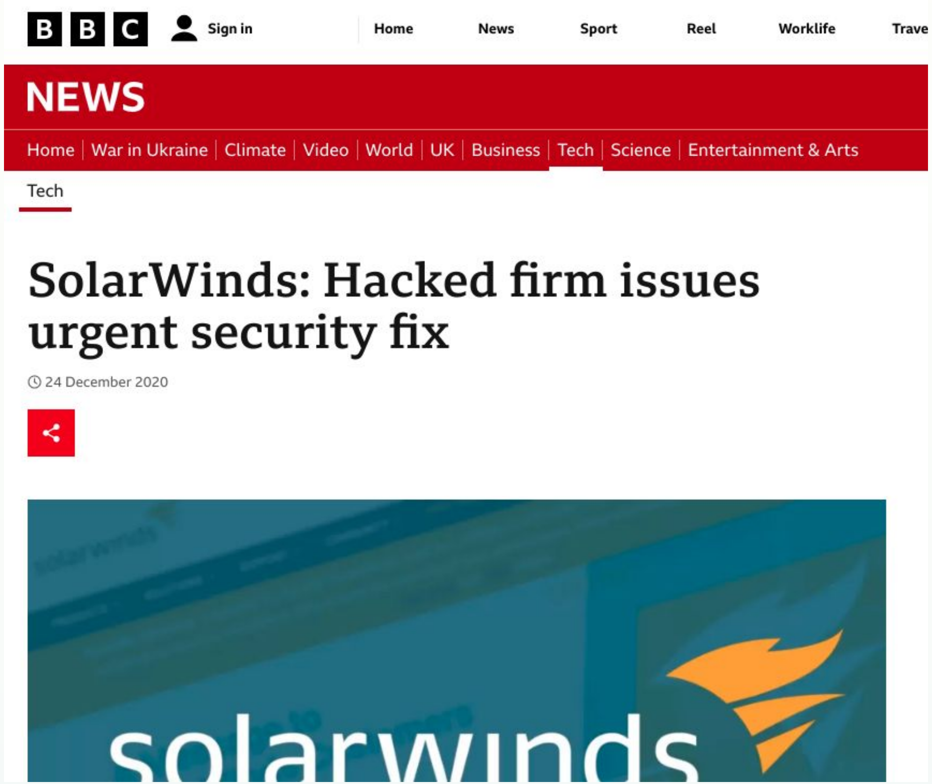
Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

04

Password management

Weak passwords

"... report that root cause of the supply chain attack was a weak password: an intern had been using the password "solarwinds123", and that password was publicly accessible via a misconfigured GitHub repository."



BBC
Sign in
Home
News
Sport
Reel
Worklife
Trave
NEWS
Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Entertainment & Arts
Tech

SolarWinds: Hacked firm issues urgent security fix

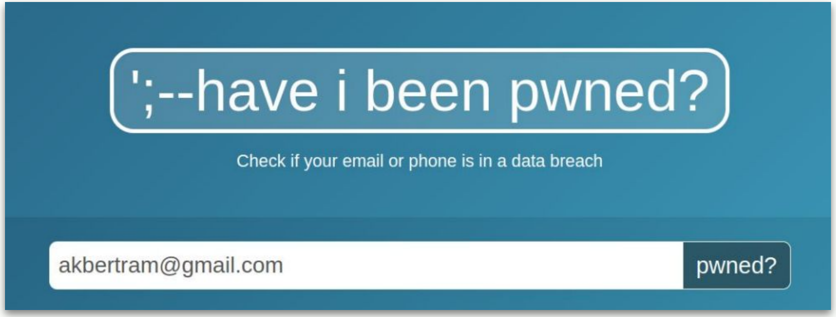
24 December 2020

ActivityInfo

Weak passwords

Use of default admin password allowed competitor of RedRose to access more than 8,000 names, photos, family details and map coordinates of beneficiaries in West Africa.

Re-used passwords

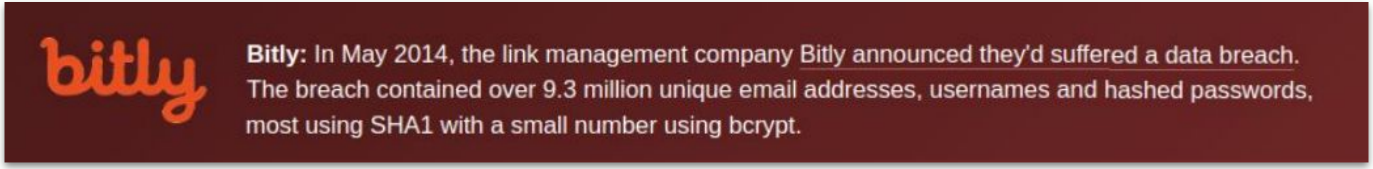


Check if your email or phone is in a data breach

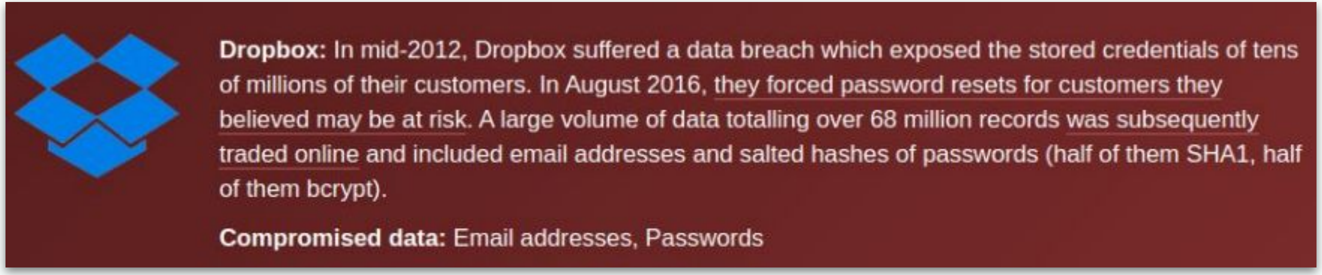
akbertram@gmail.com

Visit https://haveibeenpwned.com/

Massive data breaches mean that your go-to password may be out there in the world.



Bitly: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Mitigation: The basics of passwords

01

No more recycling

02

Use two factor authentication when possible

03

Use a password manager

Mitigation: Password Manager

- ✓ Only one password to remember
- ✓ Automatically generated passwords
- ✓ Notify when it’s time to change

Password managers:

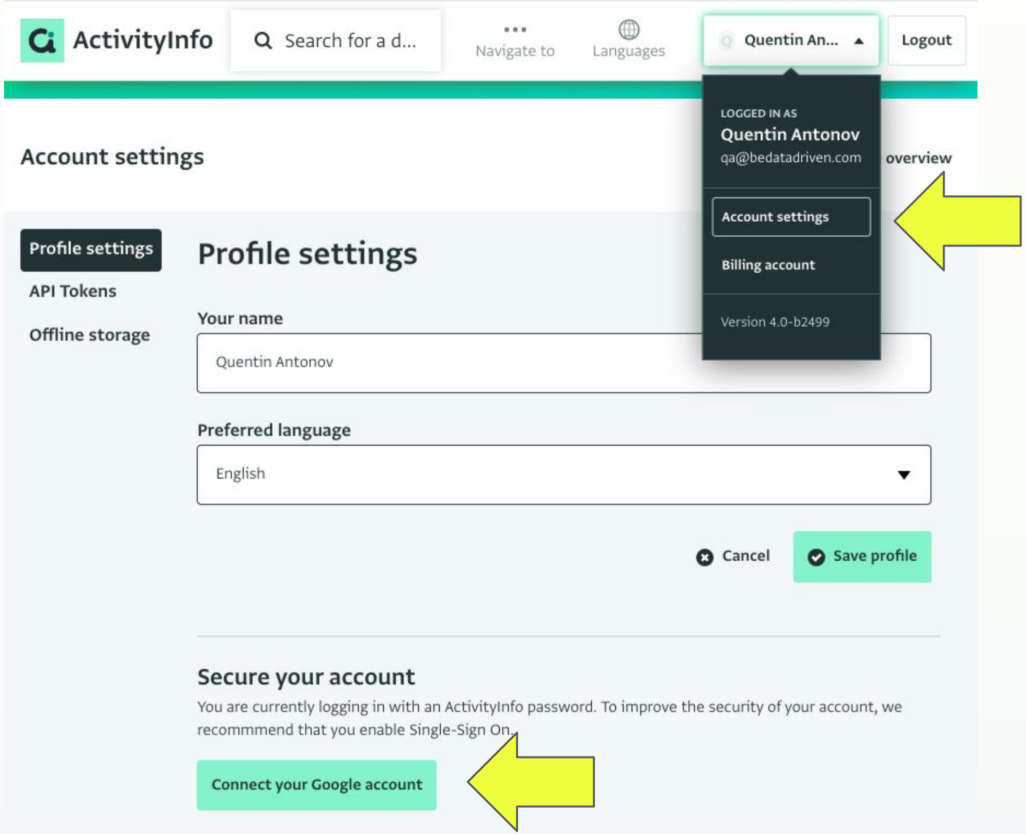
- BitWarden
- 1-password
- Default browser manager (Chrome/Firefox)

Mitigation: Migrate to SSO

Single-Sign on via your organization significantly reduces risk of Account Takeover Attacks (ATO) and Insider attacks.

○ Enforce organization-level policies on 2FA, device security
○ Eliminate sloppy passwords
○ Inherit organization-level account security
○ Ex-employees automatically blocked

Enabling SSO in ActivityInfo



Account settings

Profile settings

Your name: Quentin Antonov

Preferred language: English

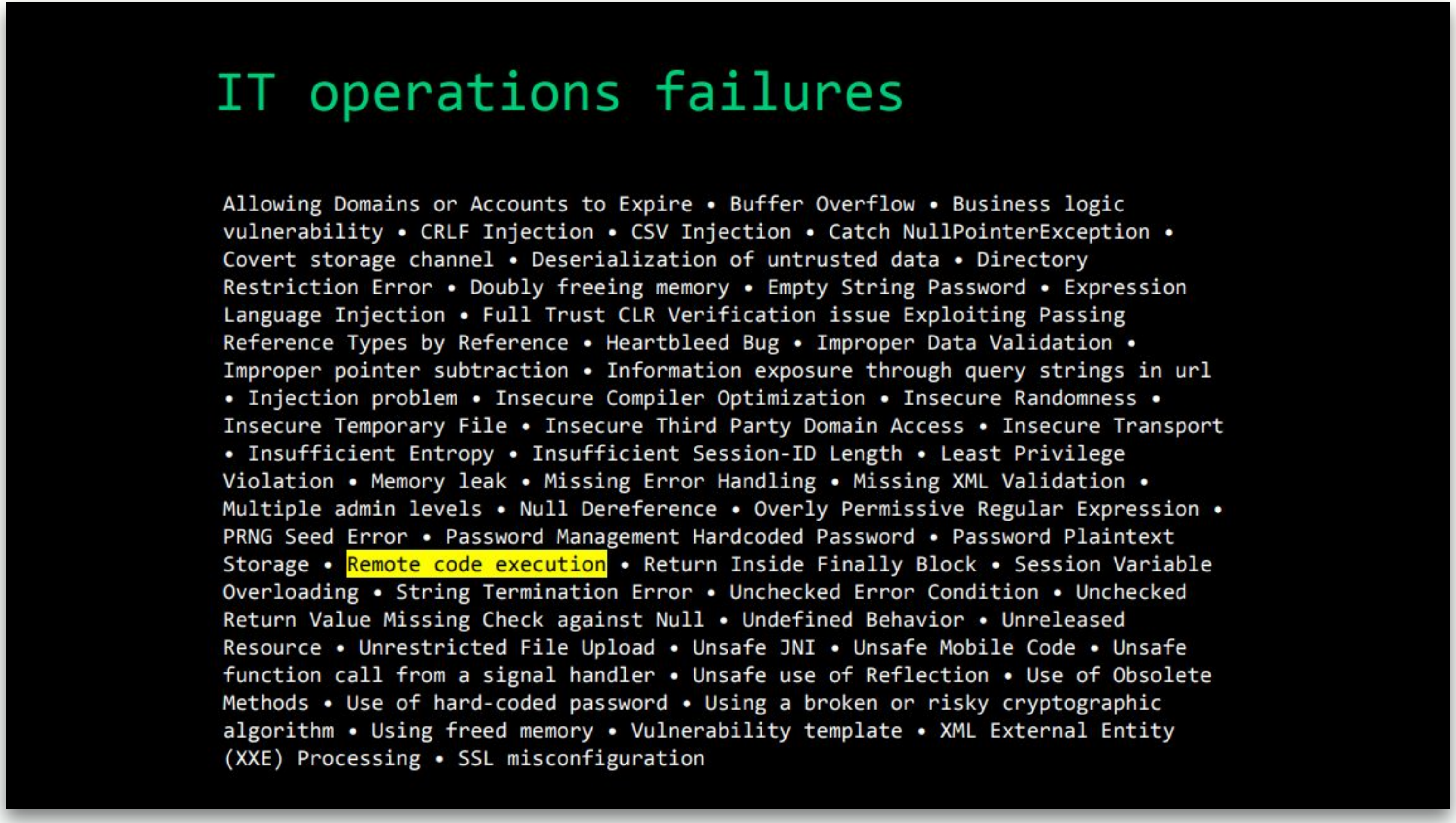
Secure your account

You are currently logging in with an ActivityInfo password. To improve the security of your account, we recommmend that you enable Single-Sign On.

ActivityInfo

03

IT Operations error



IT operations failures

Allowing Domains or Accounts to Expire • Buffer Overflow • Business logic vulnerability • CRLF Injection • CSV Injection • Catch NullPointerException • Covert storage channel • Deserialization of untrusted data • Directory Restriction Error • Doubly freeing memory • Empty String Password • Expression Language Injection • Full Trust CLR Verification issue Exploiting Passing Reference Types by Reference • Heartbleed Bug • Improper Data Validation • Improper pointer subtraction • Information exposure through query strings in url • Injection problem • Insecure Compiler Optimization • Insecure Randomness • Insecure Temporary File • Insecure Third Party Domain Access • Insecure Transport • Insufficient Entropy • Insufficient Session-ID Length • Least Privilege Violation • Memory leak • Missing Error Handling • Missing XML Validation • Multiple admin levels • Null Dereference • Overly Permissive Regular Expression • PRNG Seed Error • Password Management Hardcoded Password • Password Plaintext Storage • Remote code execution • Return Inside Finally Block • Session Variable Overloading • String Termination Error • Unchecked Error Condition • Unchecked Return Value Missing Check against Null • Undefined Behavior • Unreleased Resource • Unrestricted File Upload • Unsafe JNI • Unsafe Mobile Code • Unsafe function call from a signal handler • Unsafe use of Reflection • Use of Obsolete Methods • Use of hard-coded password • Using a broken or risky cryptographic algorithm • Using freed memory • Vulnerability template • XML External Entity (XXE) Processing • SSL misconfiguration

IT operations failures

400 GB of data was stolen from UN servers in 2019

Feb 2019: Alert for bug in Sharepoint published

July 2019: Attackers exploited this bug to gain access to UN systems.

The New Humanitarian

Dark Reading

IT operations failures

Personal data of 515,000 people

- **Sept 2021:** Alert for bug in ManageEngine published
- **Nov 2021:** Attackers exploited this bug to gain access to ICRC
- **Feb 2022:** Access discovered by ICRC

ActivityInfo

In-house vs outsourced

In house

Software running on servers your employees manage

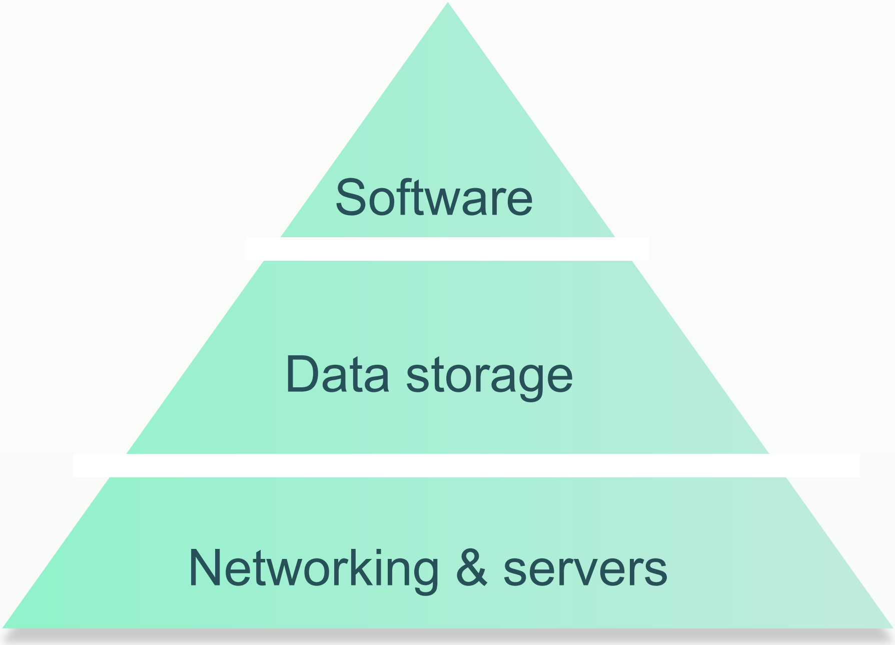
Resources?
Long-term budget for staff and software?
Expertise?
Focus?

Outsourced

Software running on servers your vendors manage

Vendor reputation and/or certification?
Budget for recurring annual fees

Mitigation: IT operations failures - specialization



ActivityInfo

Google Cloud Datastore

Google Cloud

02

Insider attacks

Insider attacks

In 2005, a local NGO staff member was fired, and using his credentials, deleted all his NGO's reports in ActivityInfo.

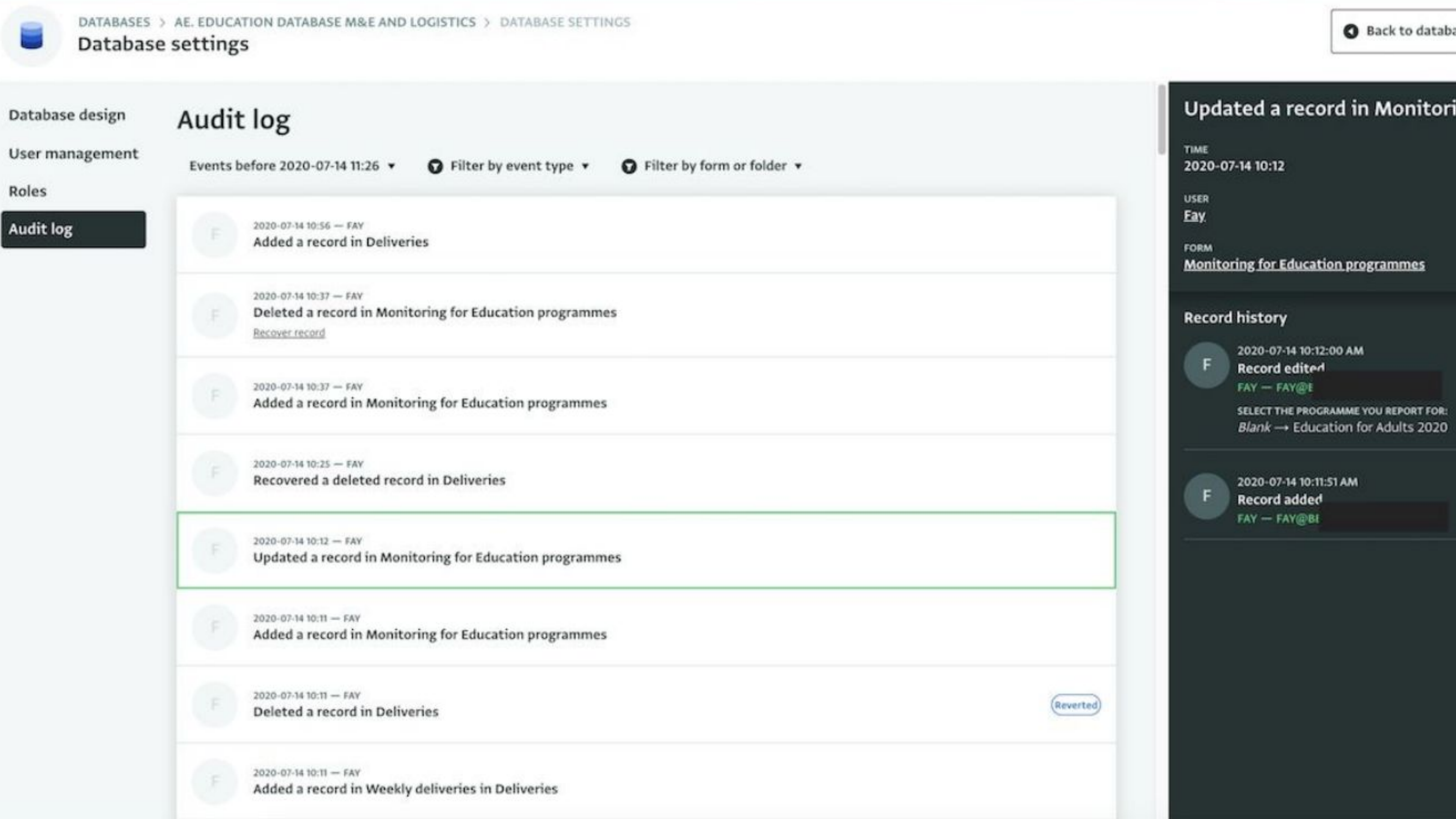
Insider attacks: what does it mean?

- Threats from within your own company
- Difficult to deal with
- Motivations include:
  - Personal gain
  - Emotional reaction

Mitigation: Insider attacks

- ✓ Narrow user permissions
- ✓ Data-loss prevention measures
- ✓ Never share passwords!

ActivityInfo


DATABASES > AE. EDUCATION DATABASE M&E AND LOGISTICS > DATABASE SETTINGS
Database settings
Back to databa
Database design
User management
Roles
Audit log
Events before 2020-07-14 11:26 ▾
Filter by event type ▾
Filter by form or folder ▾

Audit log

2020-07-14 10:56 — FAY
Added a record in Deliveries

2020-07-14 10:37 — FAY
Deleted a record in Monitoring for Education programmes
Recover record

2020-07-14 10:37 — FAY
Added a record in Monitoring for Education programmes

2020-07-14 10:25 — FAY
Recovered a deleted record in Deliveries

2020-07-14 10:12 — FAY
Updated a record in Monitoring for Education programmes

2020-07-14 10:11 — FAY
Added a record in Monitoring for Education programmes

2020-07-14 10:11 — FAY
Deleted a record in Deliveries
Reverted

2020-07-14 10:11 — FAY
Added a record in Weekly deliveries in Deliveries

Updated a record in Monitori

TIME
2020-07-14 10:12

USER
Fay

FORM
Monitoring for Education programmes

Record history

2020-07-14 10:12:00 AM
Record edited
FAY — FAY@E[redacted]
SELECT THE PROGRAMME YOU REPORT FOR:
Blank → Education for Adults 2020

2020-07-14 10:11:51 AM
Record added
FAY — FAY@BI[redacted]

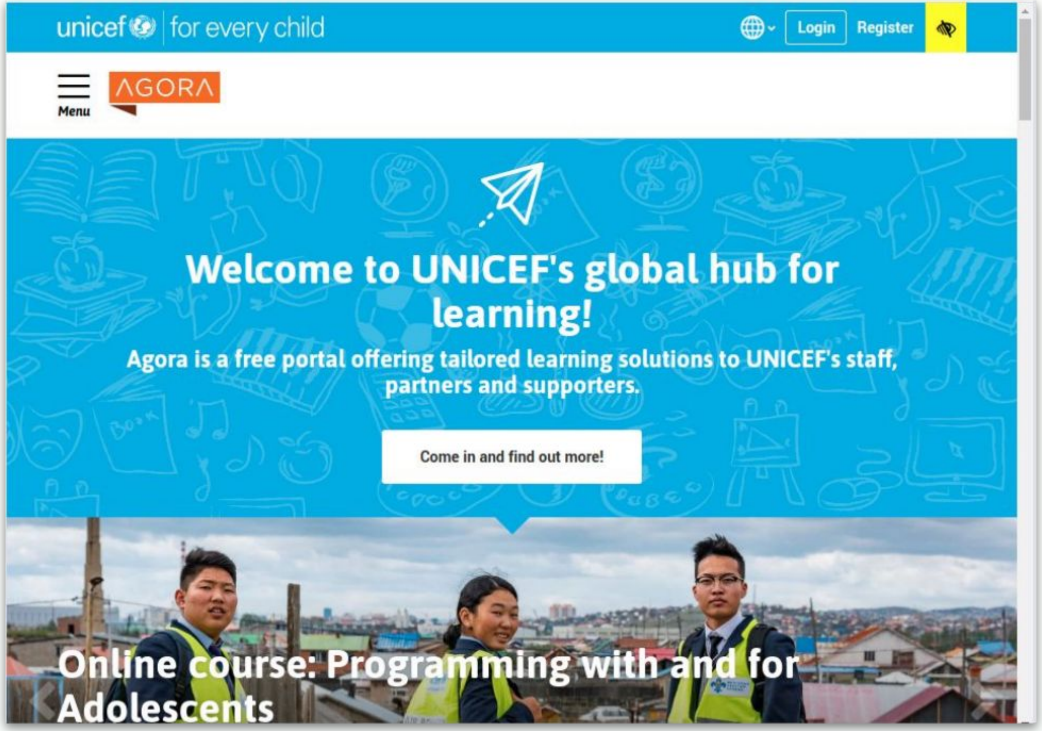
01

User error

User error

“An email holding the private data of 8,253 users enrolled onto courses on immunisation went out to around 20,000 Agora users in late August [2019]”

“This was an inadvertent data leak caused by an error when an internal user ran a report...”



unicef for every child

Login Register

Menu

ΛGORΛ

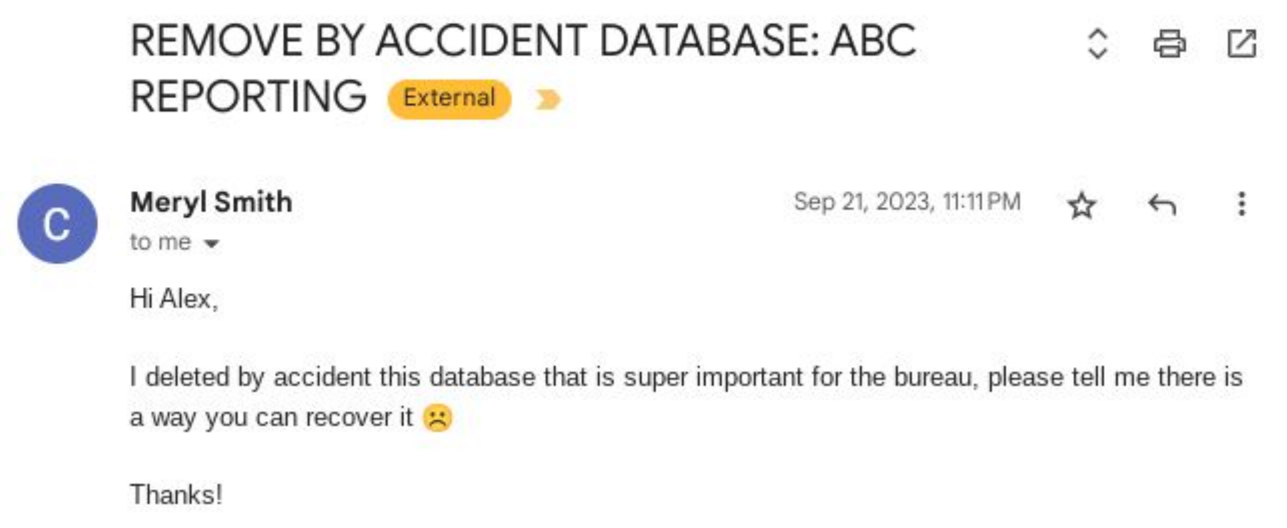
Welcome to UNICEF's global hub for learning!

Agora is a free portal offering tailored learning solutions to UNICEF's staff, partners and supporters.

Come in and find out more!

Online course: Programming with and for Adolescents

User error



REMOVE BY ACCIDENT DATABASE: ABC REPORTING

Meryl Smith

to me

Sep 21, 2023, 11:11 PM

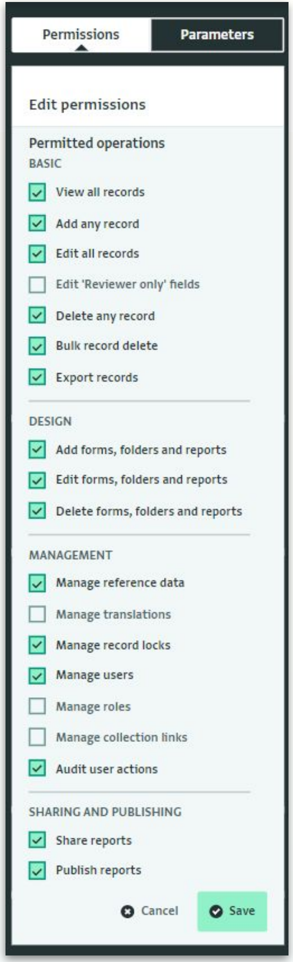
Hi Alex,

I deleted by accident this database that is super important for the bureau, please tell me there is a way you can recover it ☹

Thanks!

Mitigation: User error

- Narrow user permissions
- Consider whether users really the need the ability to Edit or Delete.
- For sensitive data, be careful with Export and Publish permissions.



Edit permissions

Permitted operations

BASIC

- ☑ View all records
- ☑ Add any record
- ☑ Edit all records
- □ Edit 'Reviewer only' fields
- ☑ Delete any record
- ☑ Bulk record delete
- ☑ Export records

DESIGN

- ☑ Add forms, folders and reports
- ☑ Edit forms, folders and reports
- ☑ Delete forms, folders and reports

MANAGEMENT

- ☑ Manage reference data
- □ Manage translations
- ☑ Manage record locks
- ☑ Manage users
- □ Manage roles
- □ Manage collection links
- ☑ Audit user actions

SHARING AND PUBLISHING

- ☑ Share reports
- ☑ Publish reports

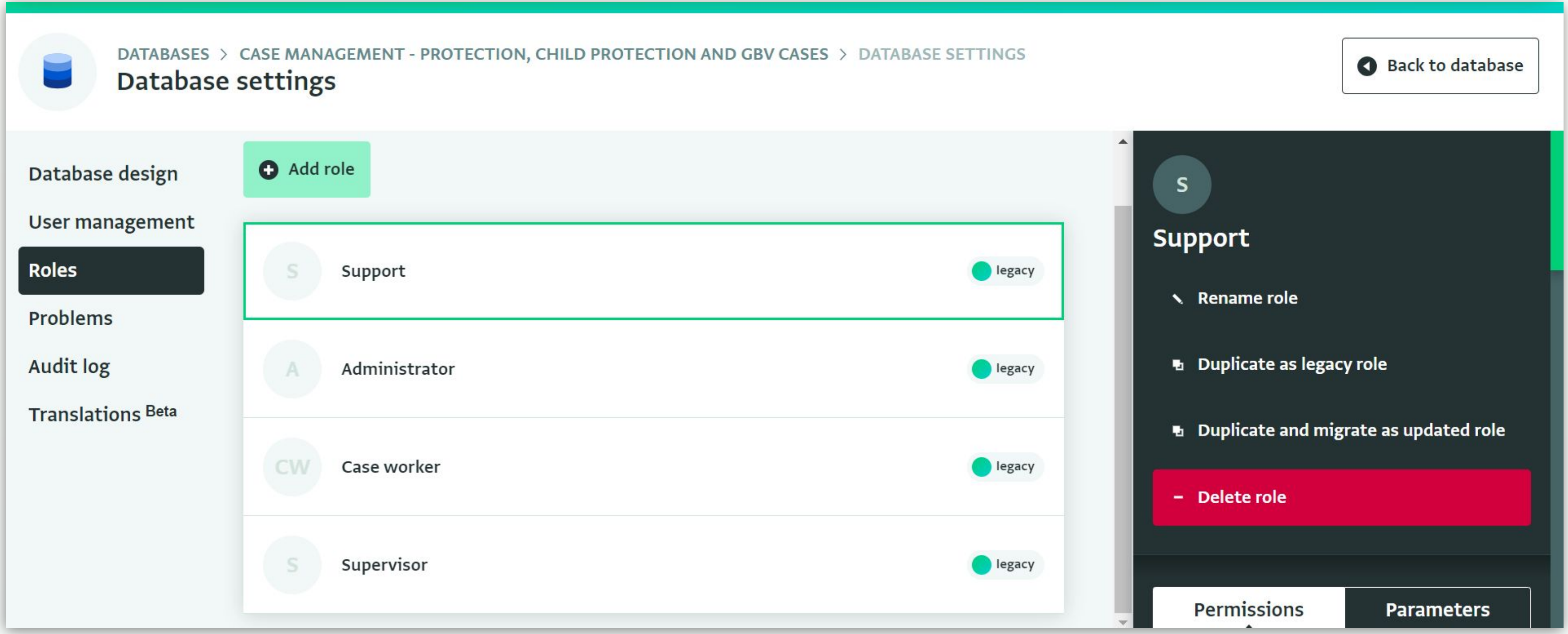
Narrow user permissions

We analysed each of our customers, and between

40 - 75% of users

granted administrative privileges are not using them!

Narrow roles



DATABASES > CASE MANAGEMENT - PROTECTION, CHILD PROTECTION AND GBV CASES > DATABASE SETTINGS

Database settings

Back to database

S	Support	legacy
A	Administrator	legacy
CW	Case worker	legacy
S	Supervisor	legacy

ActivityInfo

00

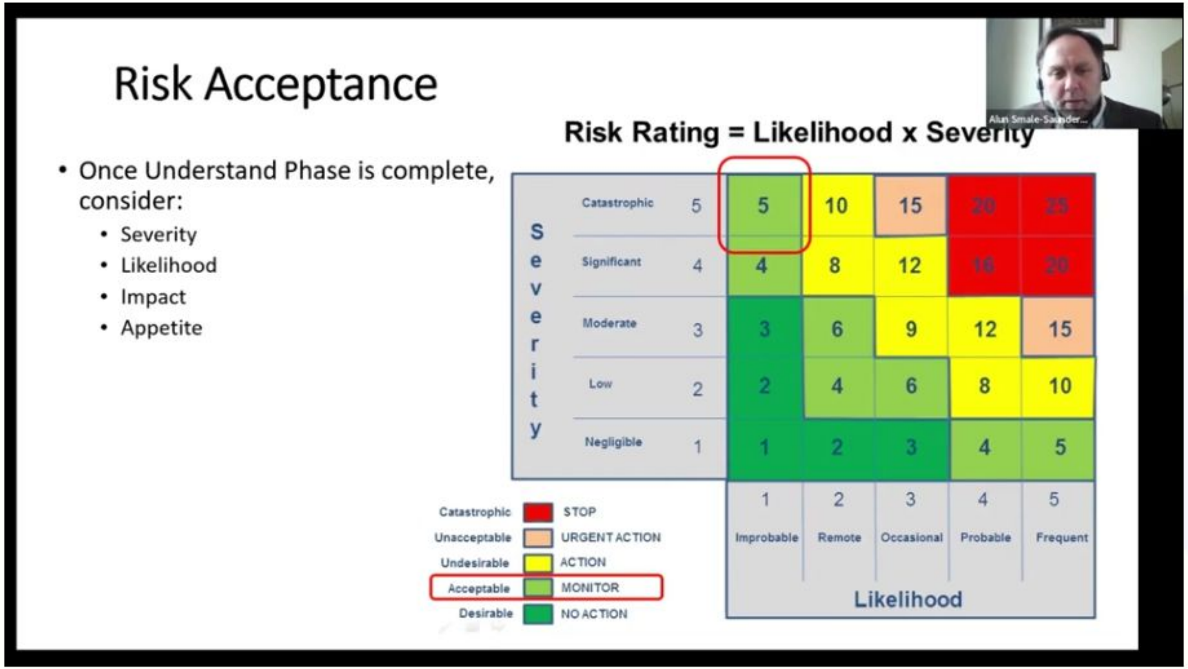
Device Security

Device Security: Minimums

- ✓ Screen lock on all devices
- ✓ Encrypted hard drive / phone
- ✓ Anti-Virus for Windows Machines

ActivityInfo

Device security in the field



Risk Acceptance

- Once Understand Phase is complete, consider:
  - Severity
  - Likelihood
  - Impact
  - Appetite

Risk Rating = Likelihood x Severity

Severity						
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5
		1	2	3	4	5
		Improbable	Remote	Occasional	Probable	Frequent
		Likelihood				

Catastrophic	🟥	STOP
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

Risk-management: we can do this!

✓ NGOs have lots of experience with risk management

✓ We need to view data security through the same lens:

- What are the risks?
- How much risk do we accept?
- How do we mitigate risks?

ActivityInfo

Questions?

Follow us:

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