ActivityInfo

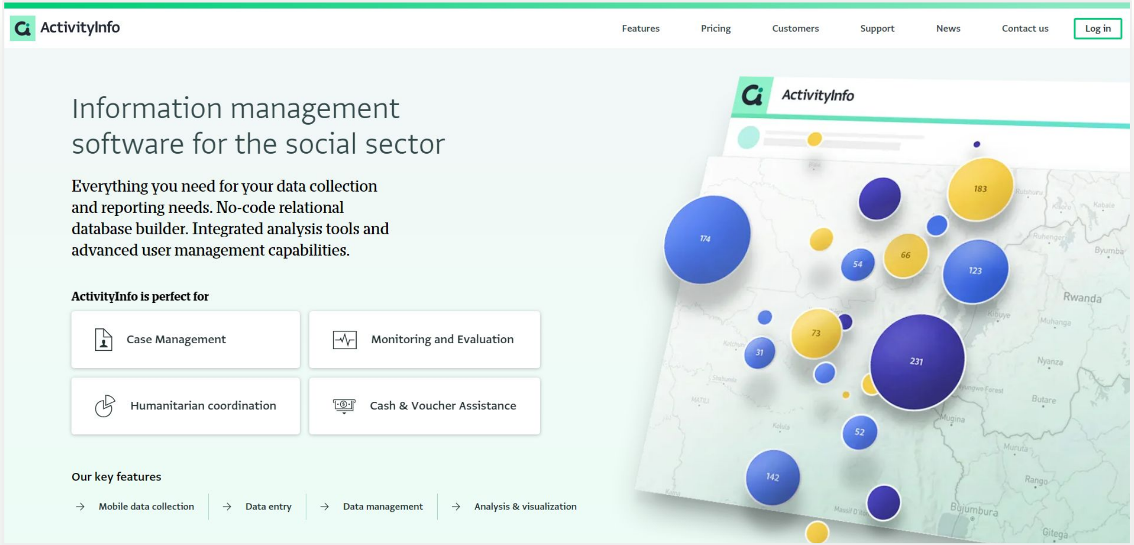
Keeping your M&E data secure

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 the social sector

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

Case Management
Monitoring and Evaluation
Humanitarian coordination
Cash & Voucher Assistance

Our key features

Outline

01 Emerging cyberthreats for NGOs

02 Best practices for your team

03 Best practices for configuring data access

04 Policies & Procedures

What is data security?

Confidentiality

Confidential data protected from exposure to unauthorized parties

Integrity

Prevention of unauthorized changes to your data

Availability

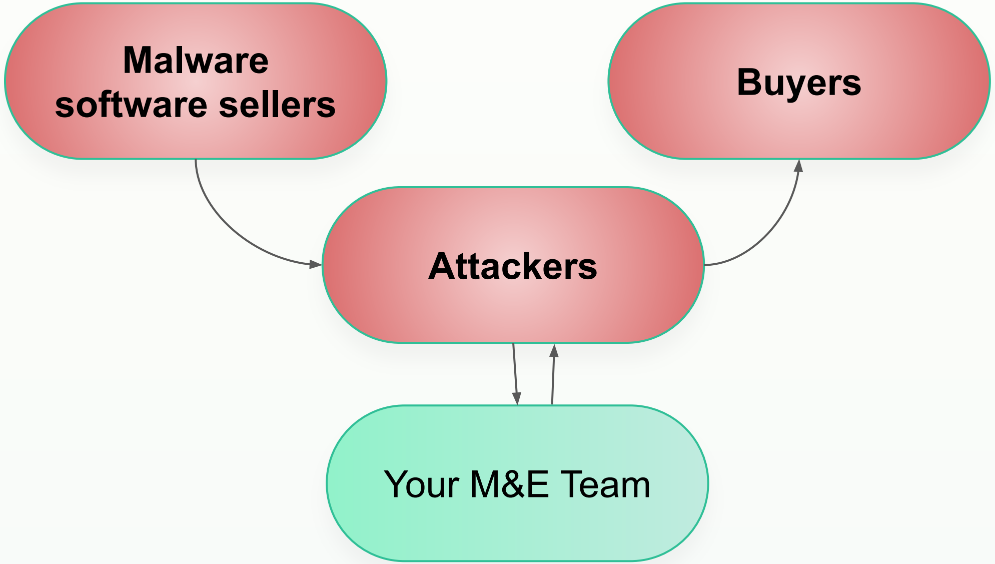
Ensuring data is available when needed to the parties who need it

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

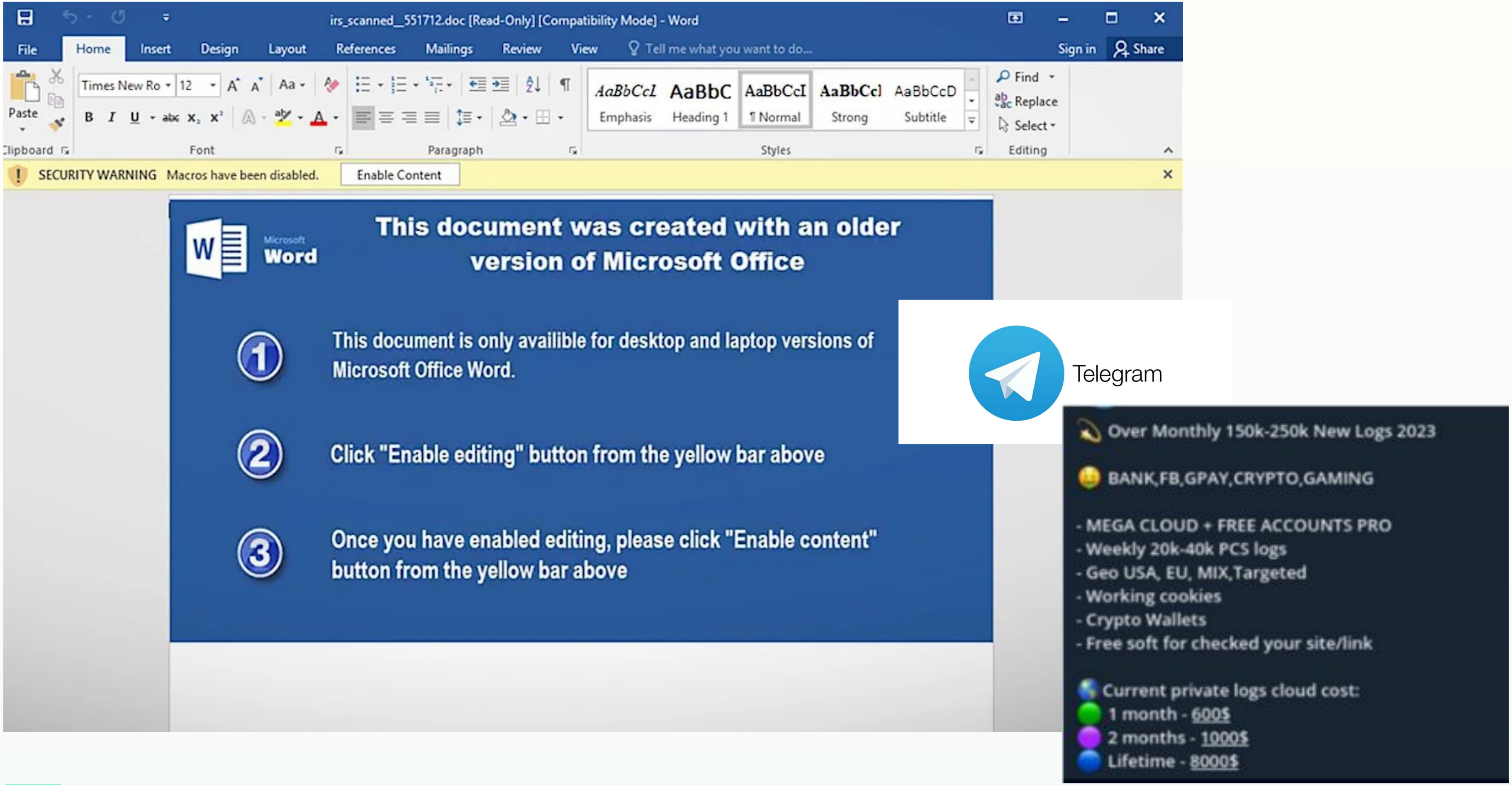
Emerging cyber threats

⚠ Rise of “infostealers"



ActivityInfo

Read more: https://flare.io/learn/resources/stealer-logs-and-corporate-access/



SECURITY WARNING Macros have been disabled.

This document was created with an older version of Microsoft Office

1. This document is only availible for desktop and laptop versions of Microsoft Office Word.
2. Click "Enable editing" button from the yellow bar above
3. Once you have enabled editing, please click "Enable content" button from the yellow bar above

Over Monthly 150k-250k New Logs 2023

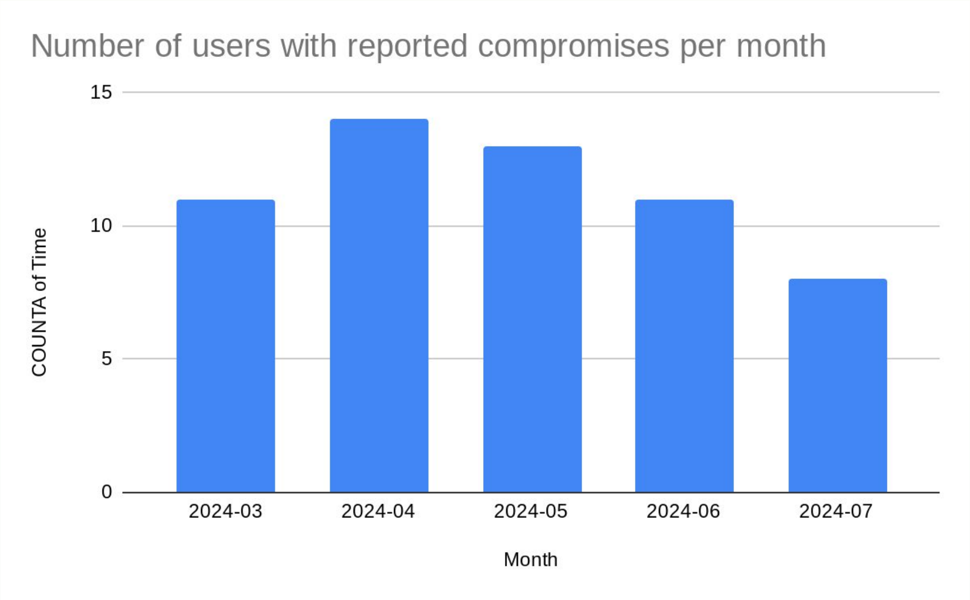
BANK,FB,GPAY,CRYPTO,GAMING

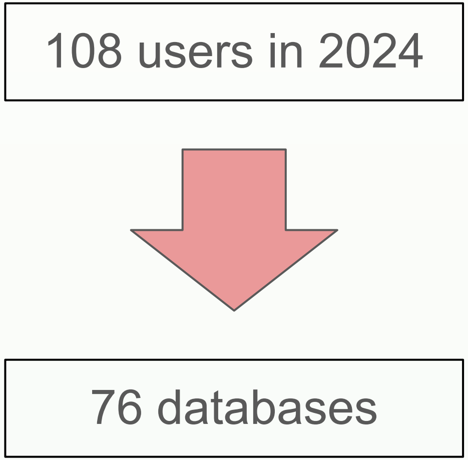
- MEGA CLOUD + FREE ACCOUNTS PRO
- Weekly 20k-40k PCS logs
- Geo USA, EU, MIX,Targeted
- Working cookies
- Crypto Wallets
- Free soft for checked your site/link

Current private logs cloud cost:
🟢 1 month - 600$
🟣 2 months - 1000$
🔵 Lifetime - 8000$

ActivityInfo

Impact on NGOs and M&E

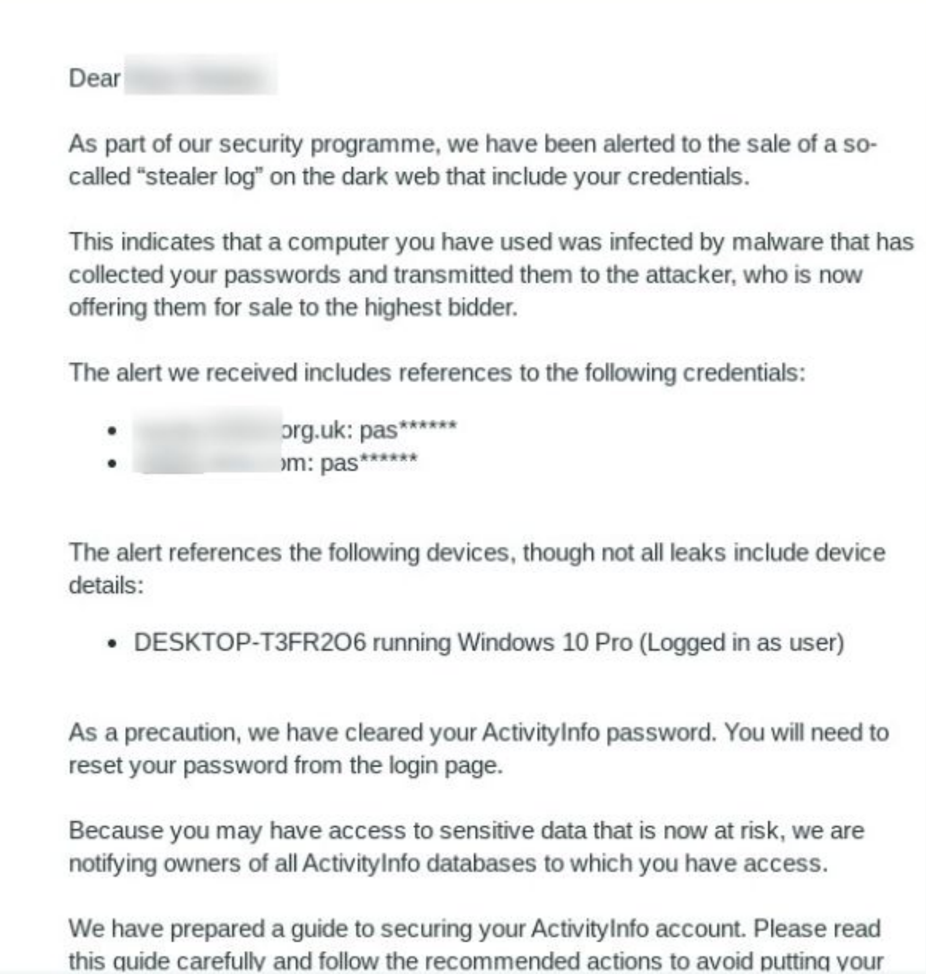




108 users in 2024

76 databases

Source: ActivityInfo user accounts (as of 2024-09-07)



Dear [redacted]

As part of our security programme, we have been alerted to the sale of a so-called “stealer log” on the dark web that include your credentials.

This indicates that a computer you have used was infected by malware that has collected your passwords and transmitted them to the attacker, who is now offering them for sale to the highest bidder.

The alert we received includes references to the following credentials:

- [redacted]org.uk: pas******
- [redacted]om: pas******

The alert references the following devices, though not all leaks include device details:

- DESKTOP-T3FR2O6 running Windows 10 Pro (Logged in as user)

As a precaution, we have cleared your ActivityInfo password. You will need to reset your password from the login page.

Because you may have access to sensitive data that is now at risk, we are notifying owners of all ActivityInfo databases to which you have access.

We have prepared a guide to securing your ActivityInfo account. Please read this guide carefully and follow the recommended actions to avoid putting your

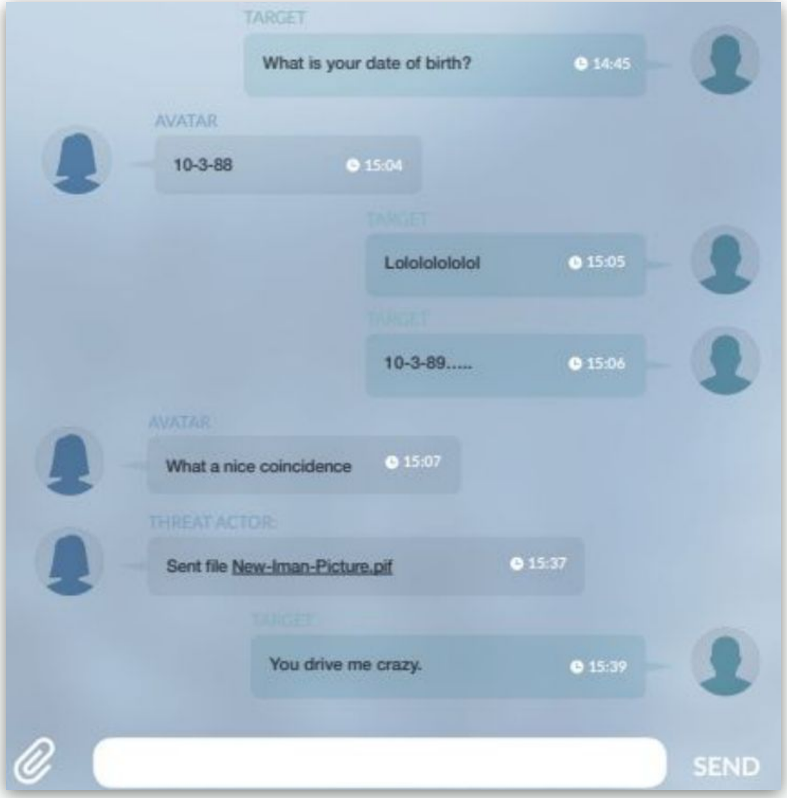
⚠ Insider attacks

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

Parties to conflict

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

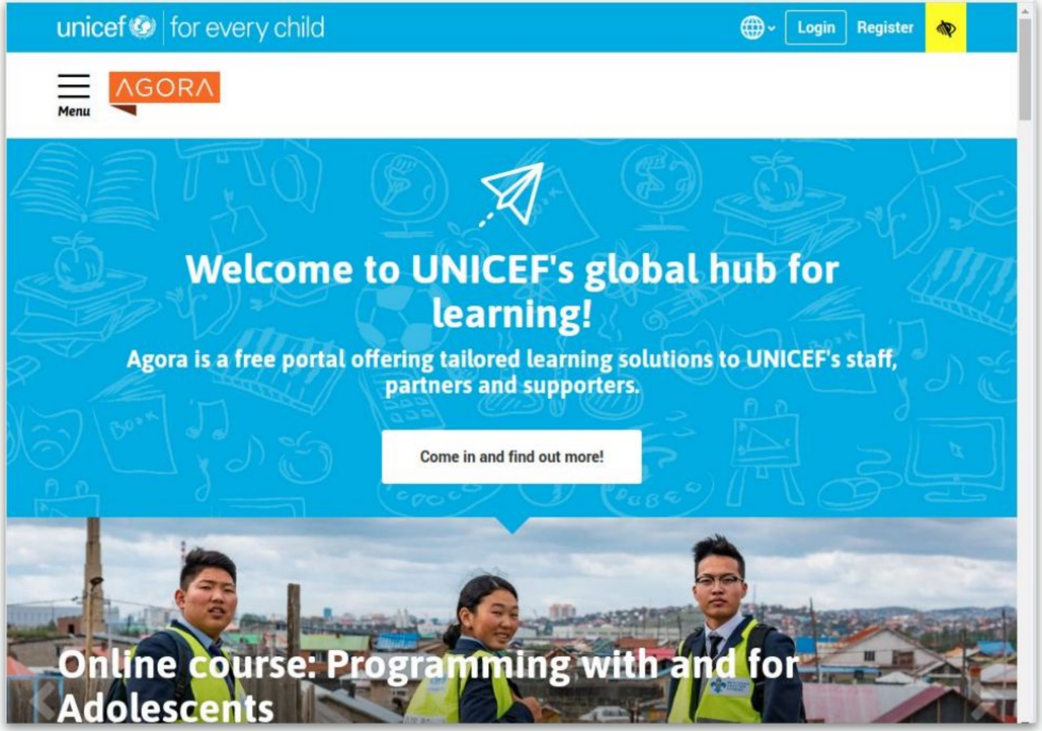
THREAT ACTOR:
Sent file New-Iman-Picture.pif 15:37

TARGET
You drive me crazy. 15:39

⚠ Human 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...”



Welcome to UNICEF's global hub for learning!

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

Online course: Programming with and for Adolescents

Understanding threats

- ⚠ Rise of “infostealers”
- ⚠ Insider attacks
- ⚠ Parties to conflict
- ⚠ Human error

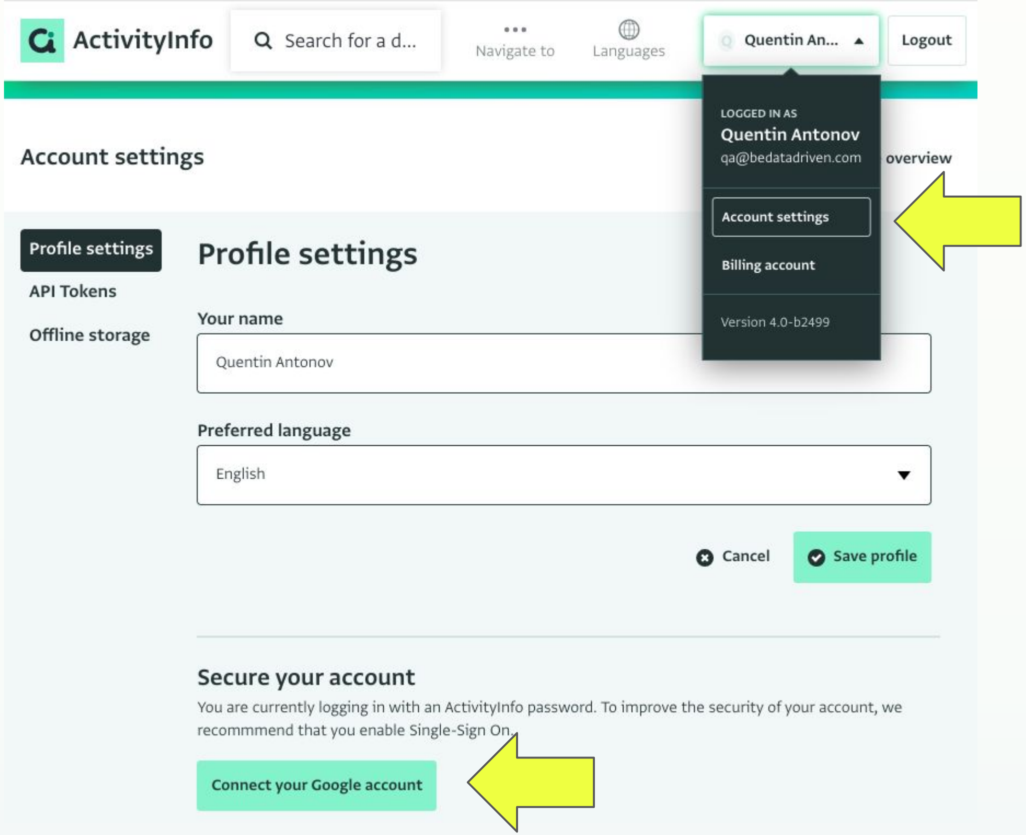
Best practices

BASIC cyber hygiene

- ✓ Enable 2FA everywhere you can
- ✓ Use a password manager everywhere else
- ✓ Anti-virus and anti-malware
- ✓ Hard disk encryption
- ✓ Lockscreen

https://www.activityinfo.org/support/docs/user-account/securing-your-activityinfo-account.html

Enabling SSO in ActivityInfo



Account settings

Profile settings

Your name

Quentin Antonov

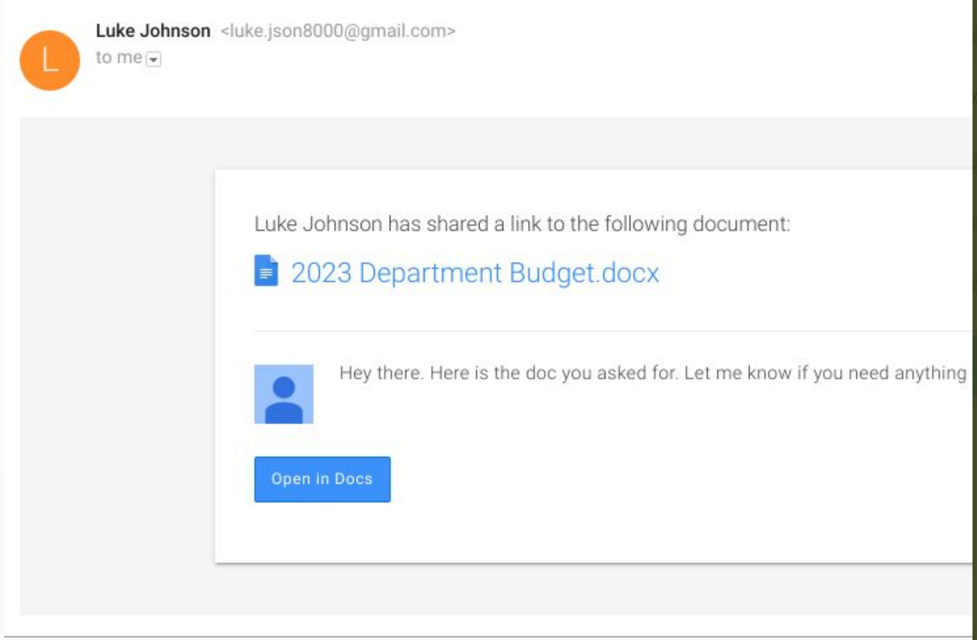
Preferred language

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.

Social Engineering

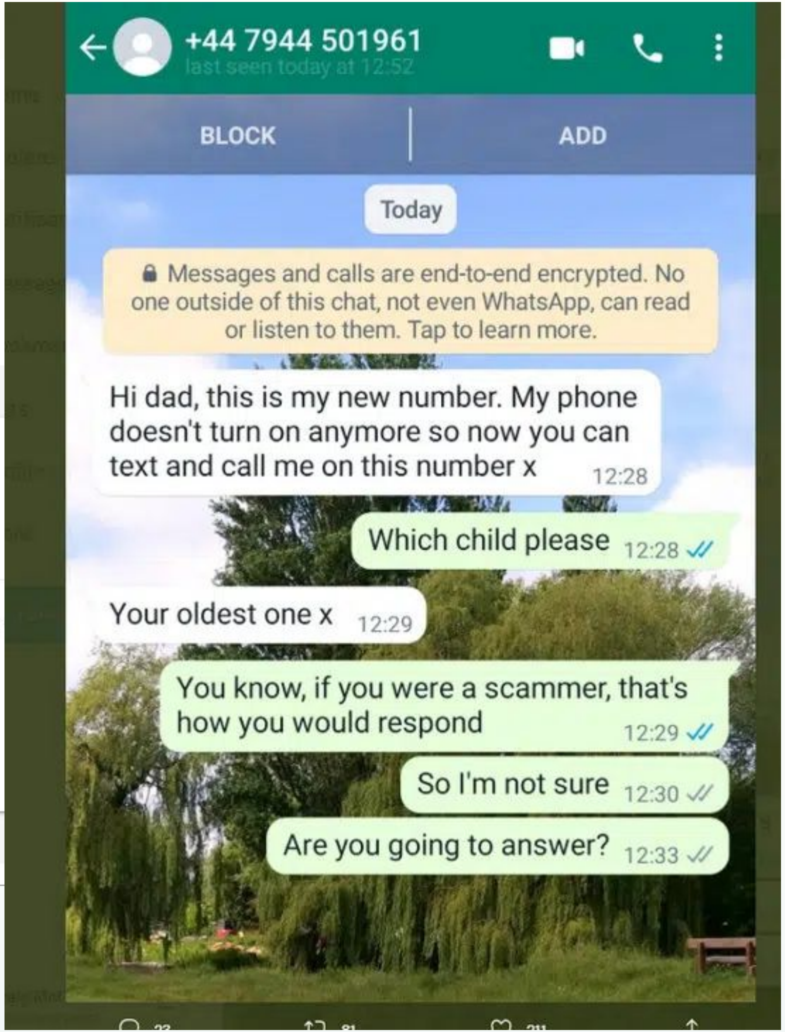


Luke Johnson <luke.json8000@gmail.com>
to me

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



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

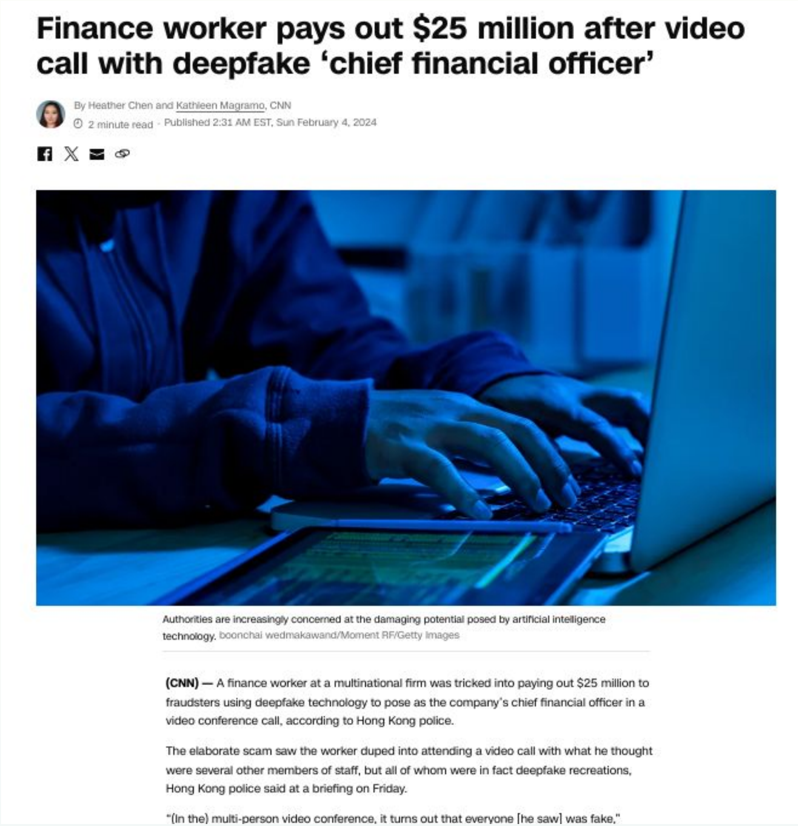
Your oldest one x 12:29

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

Generative AI amplifies these risks



Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

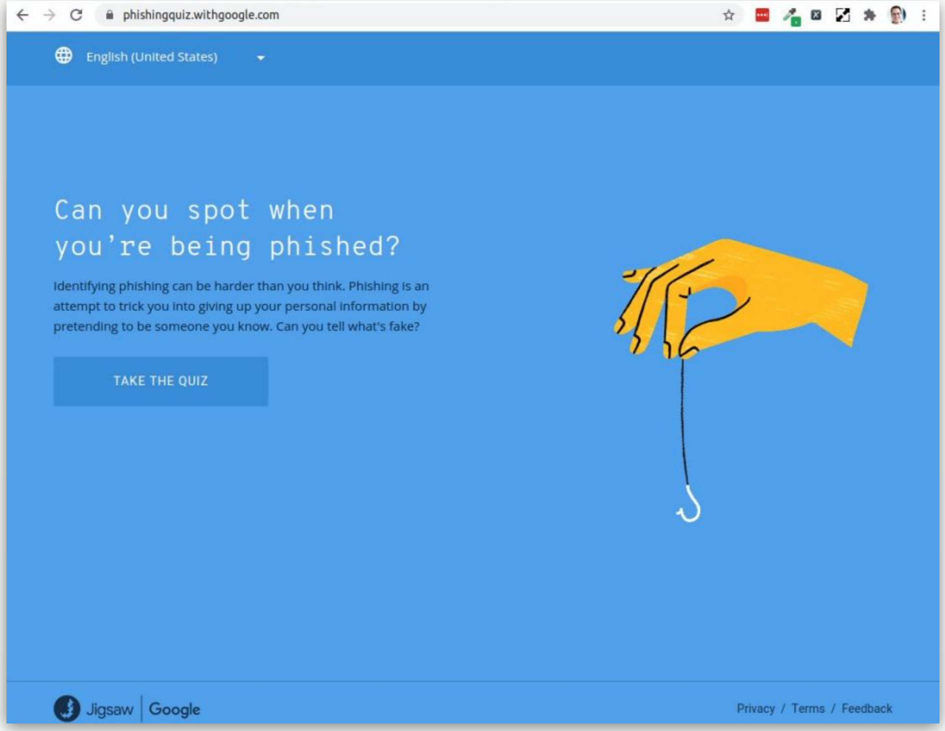
The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

"(In the) multi-person video conference, it turns out that everyone [he saw] was fake,"

Social Engineering Resistance

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

https://phishingquiz.withgoogle.com/

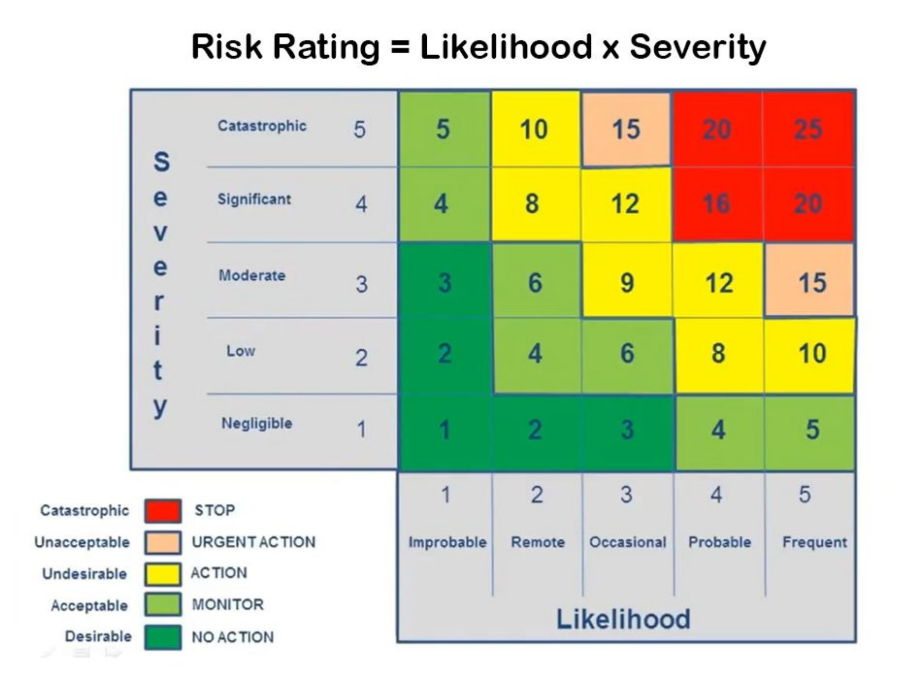


Can you spot when you’re being phished?

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?

Physical security in the field

- ✓ Determine risk acceptance
- ✓ Plan ahead
- ✓ Identify risks
- ✓ Go/No Go



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

https://www.activityinfo.org/support/webinars/2023-03-16-device-security-in-the-field.html

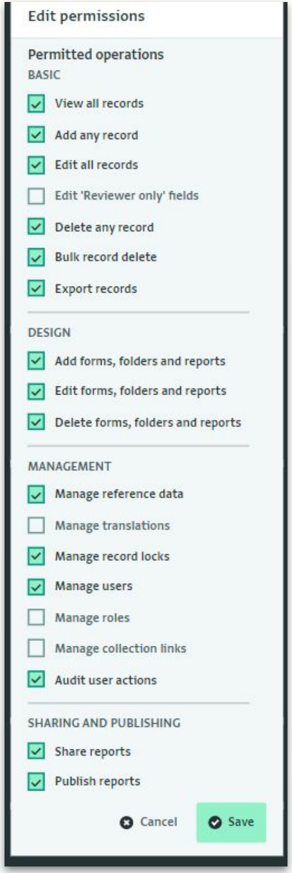
Best practices for configuring data access

Least privilege

Best practices for designing roles

Design roles with **narrow** user permissions

- Employ the Principle of Least Privilege as a rule
- To maintain integrity: consider whether users really the need the ability to **Edit** or **Delete**
- To protect sensitive data: be careful with **Export** and **Publish** permissions
- Grant **User Management** operations selectively



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

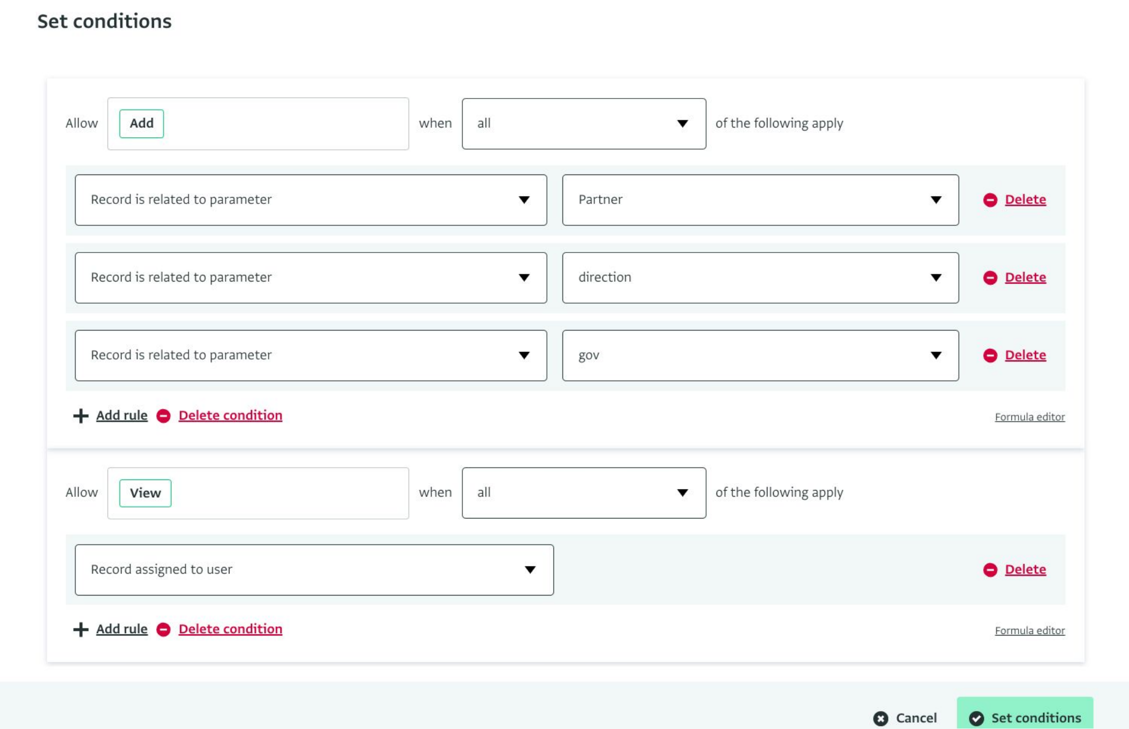
MANAGEMENT

☑ 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

Record-level permissions



Set conditions

Allow **Add** when all ▼ of the following apply

- Record is related to parameter ▼ — Partner ▼ — Delete
- Record is related to parameter ▼ — direction ▼ — Delete
- Record is related to parameter ▼ — gov ▼ — Delete

Allow **View** when all ▼ of the following apply

- Record assigned to user ▼ — Delete

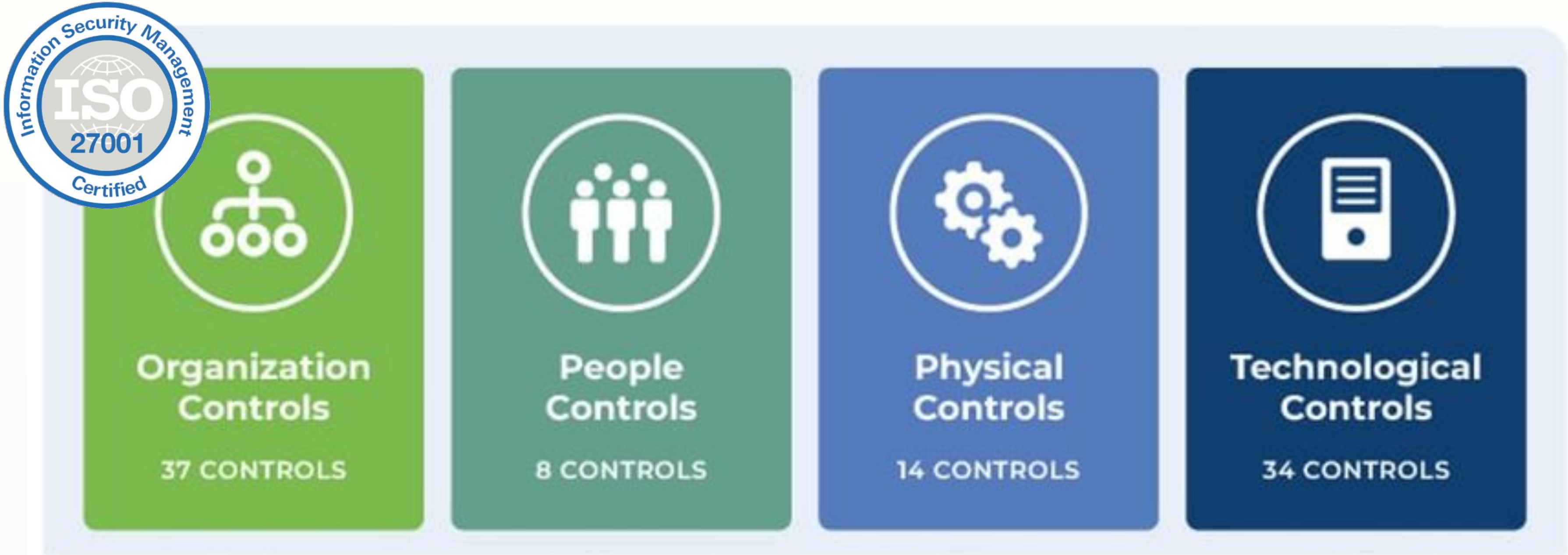
ActivityInfo

Policies & Procedures

An information security management system (ISMS)
is a set of policies and procedures for systematically managing an organization's sensitive data.

The goal of an ISMS is to minimize risk and ensure operational continuity by proactively limiting the impact of a security breach.

Information Security Management
ISO
27001
Certified



Organization Controls

37 CONTROLS

People Controls

8 CONTROLS

Physical Controls

14 CONTROLS

Technological Controls

34 CONTROLS

- Policies
- Roles and responsanilities
- Access rights
- Information labeling
- ...

- Terms and conditions of employment
- Security training
- Remote working
- Disciplinary process
- ...

- Physical security perimeters
- Physical entry
- Cabling security
- Equipements maintenance
- ...

- User endpoint devices
- Configuration management
- Data masking
- Data leakage prevention
- ...

“Quick win” controls

- Data inventory map
- Access reviews

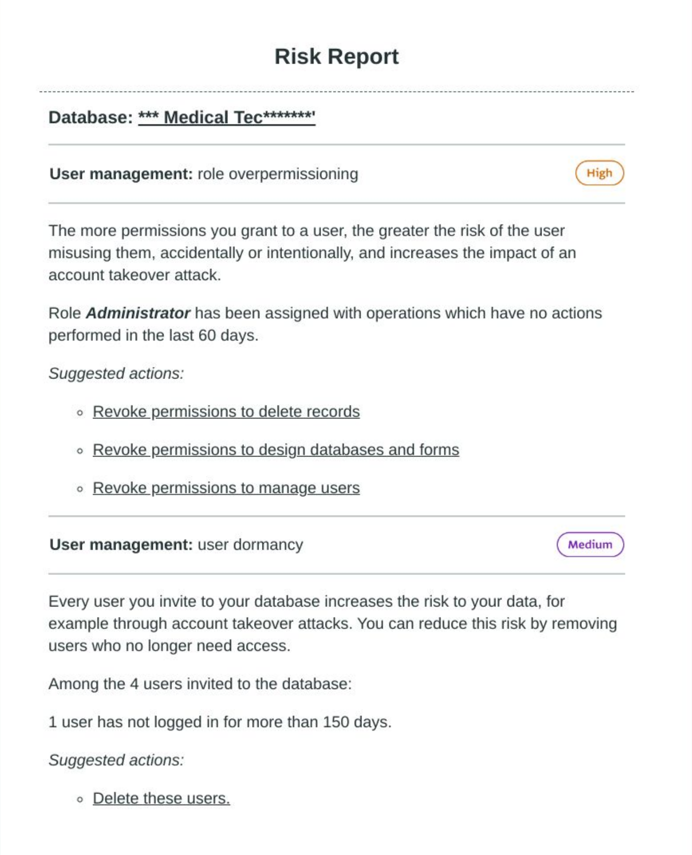
Data inventory map

- Spreadsheet with a list of all data you collect and retain
- Personally-identifiable information?
- Where/with whom is it stored?
- Shared?

Access reviews

- Pick a frequency: monthly, quarterly
- Put an hour in your calendar to review permissions in all of your M&E systems
- *Optional*: track the number of corrections you have to make each time.

Weekly risk report



Risk Report

Database: *** Medical Tec*******'

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 ***Administrator*** 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
- Revoke permissions to manage users

User management: user dormancy Medium

Every user you invite to your database increases the risk to your data, for example through account takeover attacks. You can reduce this risk by removing users who no longer need access.

Among the 4 users invited to the database:

1 user has not logged in for more than 150 days.

Suggested actions:

- Delete these users.

ActivityInfo

Thank you!

ActivityInfo is an all in one Information Management Software

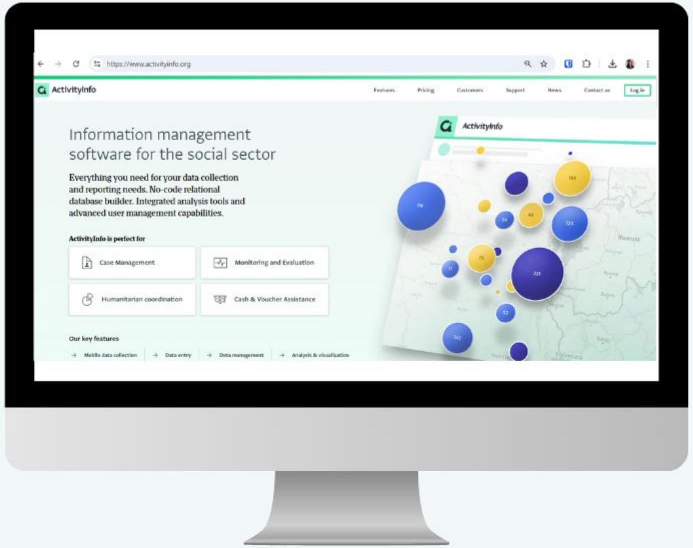
Humanitarian Operations

Development Operations

Data collection

Data management

Data Analysis & Visualization



Information management software for the social sector

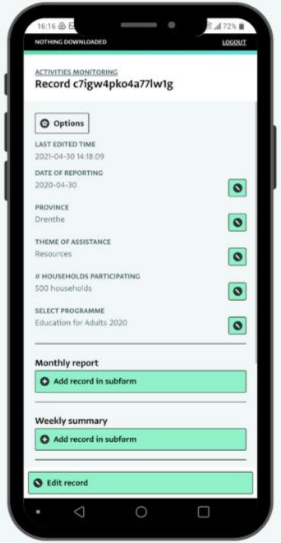
Everything you need for your data collection and reporting needs. No-code relational database builder. Integrated analysis tools and advanced user management capabilities.

ActivityInfo is perfect for

- Case Management
- Monitoring and Evaluation
- Humanitarian coordination
- Cash & Voucher Assistance

Our key features

→ Mobile data collection | → Data entry | → Data management | → Analysis & visualization



ACTIVITIES MONITORING

Record c7igw4pko4a77lw1g

Options

LAST EDITED TIME
2021-04-30 14:18:09

DATE OF REPORTING
2020-04-30

PROVINCE
Drenthe

THEME OF ASSISTANCE
Resources

HOUSEHOLDS PARTICIPATING
500 households

SELECT PROGRAMME
Education for Adults 2020

Monthly report

Add record in subform

Weekly summary

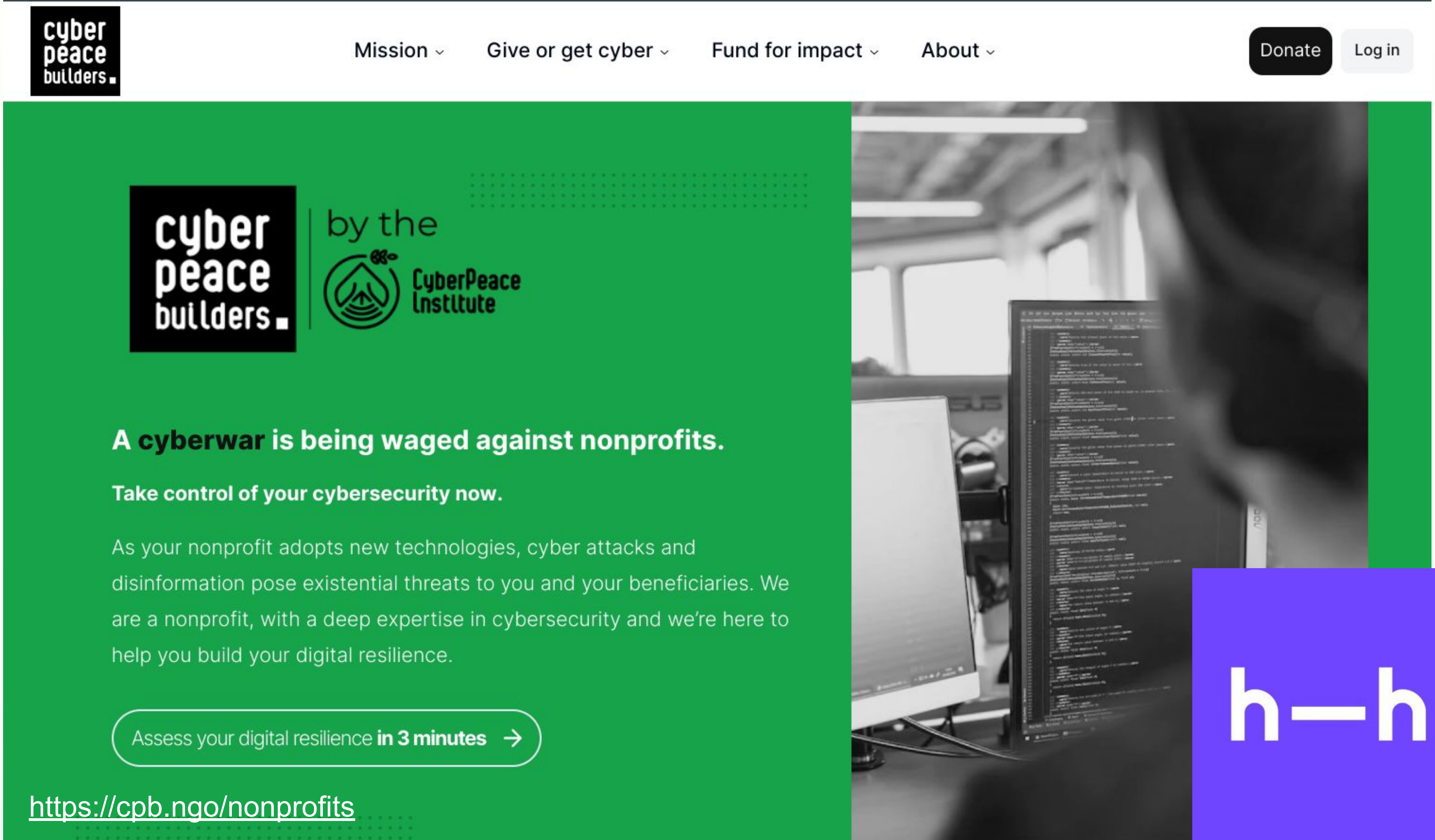
Add record in subform

Edit record

Contact us for a demo or more information about using ActivityInfo

https://www.activityinfo.org/about/contact.html

Brendan O’Neill
Commercial Director



A **cyberwar** is being waged against nonprofits.

Take control of your cybersecurity now.

As your nonprofit adopts new technologies, cyber attacks and disinformation pose existential threats to you and your beneficiaries. We are a nonprofit, with a deep expertise in cybersecurity and we're here to help you build your digital resilience.

https://cpb.ngo/nonprofits

Questions?

Follow us:

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

Upcoming webinars

OCT 24

ActivityInfo for Monitoring & Evaluation [Arabic]

NOV 13

ActivityInfo, One Platform for the Complete Global Program Data Lifecycle

NOV 21

Data privacy laws in Monitoring and Evaluation