Data Breaches: your casual end of year security problem

Adam Black

All companies are fictitious

Are we too casual about data protection?

Could a link to vulnerable data be sitting in your email inbox?

End of year holidays

Ferry trip to Zoo

2 hours south (Kiama)

Holiday security

Door locked?

What about the windows?

Holiday security

Camera website data leak

URLs

URL: **https://comics.com/cat?mask**

what do you look at?

- a: the comic
- b: read “https://comics.com”
- c: read “cat” (path)
- d: read “mask” (query parameter)

Case study

End of financial year

- Tax summary

Case study

From: stationary@starkIndustries.com 

Title: Your Tax Summary

Download:
https://starkIndustries.com/files/1401271.pdf

Case study

https://starkIndustries.com/files/1401271.pdf

1271.pdf:

Dear Adam Black,
This year you purchased:

- 1 Iron pen $2

Delivered to: 1 purple way

Case study

https://starkIndustries.com/files/140**1271**.pdf

1271.pdf:

Dear Adam Black,
This year you purchased:

- 1 Iron pen $2

Delivered to: 1 purple way

1270.pdf: 

Dear Shrek,
This year you purchased:

- 100 Miniature toy donkeys $1,000
- 1 Swamp decoration kit $100

Delivered to: Shrek's Swamp

Case study

Remediation

1271.pdf:

This link is currently unavailable.
We will send you another email.
Sorry for the inconvenience.

The problem

Sensitive data accessible via guessable URL

(Insecure Direct Object Reference Vulnerability)

Is it vulnerable?

Car insurance renewal:

https://insurance.com.au/payment?member=1024019&postcode=2000

Option 1

Bruce Wayne

Car: Batmobile
Registration: 1 bat
Insurance cost: $2000
Expiry: 8 November

Is it vulnerable? YES

Car insurance renewal:

https://insurance.com.au/payment?member=1024019&postcode=2000

Option 1

Bruce Wayne

Car: Batmobile
Registration: 1 bat
Insurance cost: $2000
Expiry: 8 November

Reporting issue

Response:

Option 1

Bruce Wayne

Car: Batmobile
Registration: 1 bat
Insurance cost: $2000
Expiry: 8 November

Is it a concern?

Option 1

Bruce Wayne

Car: Batmobile
Registration: 1 bat
Insurance cost: $2000
Expiry: 8 November

Option 2

Member: 3033019
Car: DeLorean time machine
Insurance cost: $1000
Expiry: 8 January

Is it vulnerable?

Tax invoice:

https://linkmonitor.com/a-ltbktzjthtjinh

Is it vulnerable? YES

https://linkmonitor.com/a-ltbktzjthtjinh

a-ltbktzjthtjin**h =** my tax invoice

a-ltbktzjthtjin**i =** company facebook page

a-ltbktzjthtjin**a =** someone else’s tax invoice

Is it vulnerable?

Find my order

Order number (required):

10182102

Billing email address (required):

Find my order

Is it vulnerable? Very Likely

Find my order

Order number (required):

10182102

Billing email address (required):

Find my order

Is it vulnerable?

https://vision.com.au/s/9e1b4366-d59e-43e6-9059-fecc2cb79b99

UUID (128 bits)

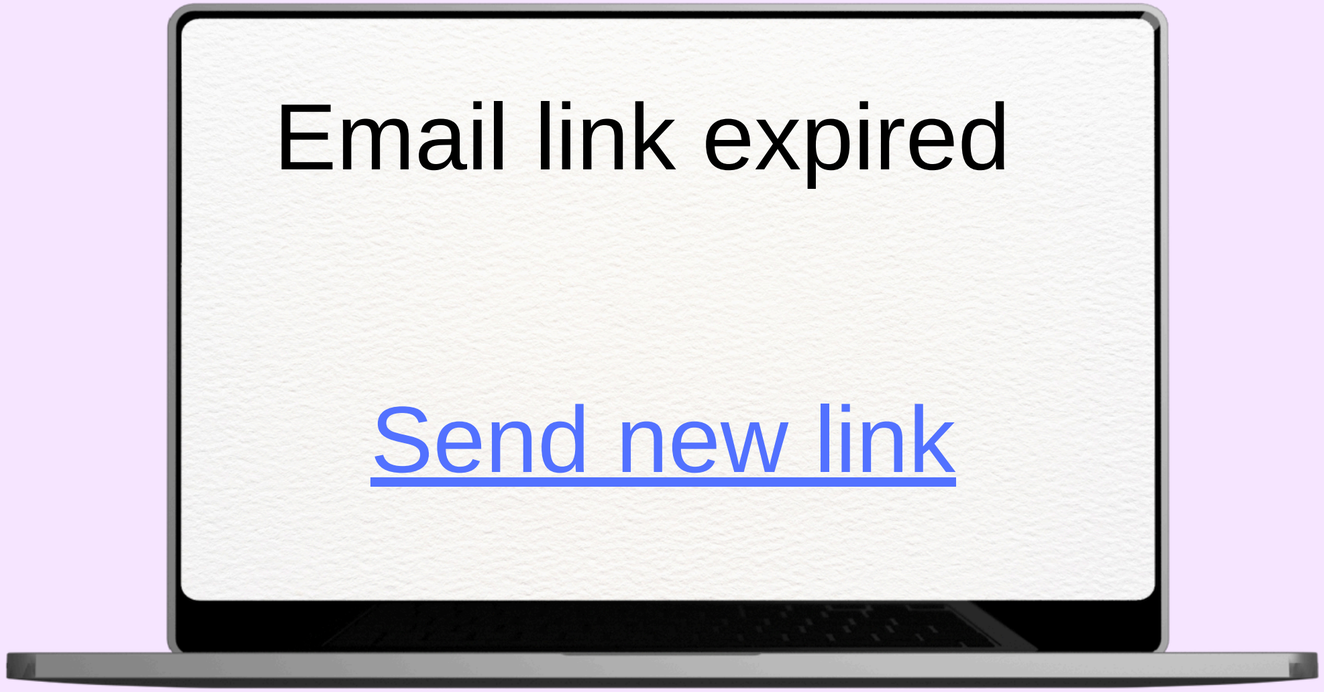
Is it vulnerable? NO

https://vision.com.au/s/9e1b4366-d59e-43e6-9059-fecc2cb79b99

UUID (128 bits)

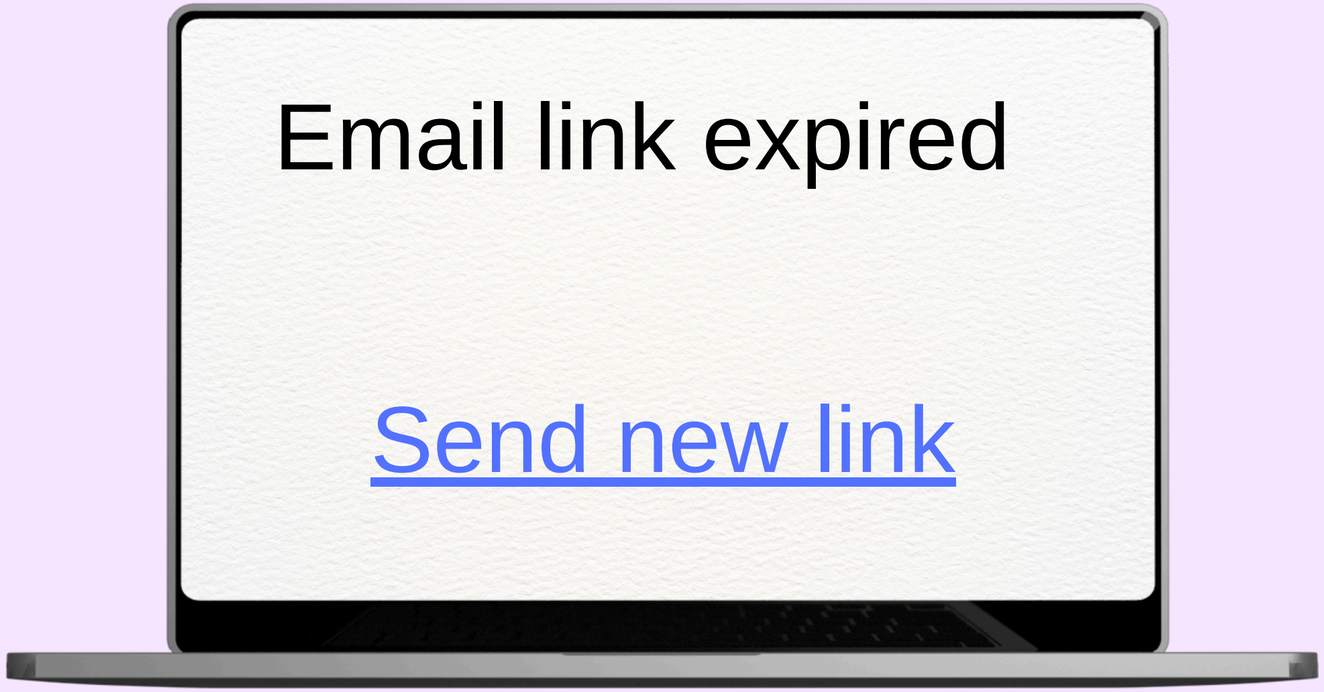
Is it vulnerable?

https://sign.com/email?a=48d66189-c5a8-4586-a222-203c64406a45&b=1f10a386-8f60-4112-82bb-2ac0f7986151



Is it vulnerable? NO

https://sign.com/email?a=48d66189-c5a8-4586-a222-203c64406a45&b=1f10a386-8f60-4112-82bb-2ac0f7986151



Best practices

Prefer non-enumerable ids

e.g. UUID 128 bits

626c9c60-d040-4d65-a007-b96a50820b71

Best practices

Ensure adequate authentication and authorization controls.

- Link expiry
- Login

Best practices

Rate Limiting

Potentially: Verify not a bot

Summary

Inspire you to:

- review URLs

Holiday tips

- Lock your windows
- Pack:
  - Towel
  - The Hitchhiker's Guide