CYBER PATH
POLICE & ACADEMIA
TALENT HORIZONS

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Individual Internet Discovery
Alison Marks

Services Provided:	Individual Internet Discovery
Created for:	Alison Marks
Report Submitted:	03/01/2026
Student Assessor:	Alex Thomas

Contents

Your Assessment

Thank you for entrusting our team at Cyber PATH to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Assessment Information	
Service completed	Individual Internet Discovery
Assessment Completed By	Lindsey Thomas
Date Completed	14/12/2025
Overseen By	Cyber PATH Student Supervisors. Savva Pistolas & Nathan Watson

Executive Summary

The executive summary identifies the key findings of the report ahead of the technical section and provides an understanding of the content of the report. This section is followed by a Risk Summary which categorises these findings into high-risk, moderate-risk, and low-risk. The technical report follows, which evidence discoveries in a way that is repeatable. The remediation and recommendation section then succinctly suggests means of removing identified information from the respective sources.

The subject is Alison Marks. She has recently been appointed to a new role as the manager of and is in [redacted] charge of a large number of employees. She expressed some concern that existing employees were likely to search her name online. Alison requested an online investigation into her digital footprint in order to summarise what content about her was available online. Upon conclusion of the investigation, it is clear that there were no high-risk findings to the reputation or safety of the subject. There was however a great deal of information about the subject available, of which the subject can grade the relevant to her own reputation. These are summarised as follows.

Email breach – The subject's personal email was found online, and when checked it was found to have been part of a data breach relating to a company called. [redacted] In. [redacted] 2020, the [redacted] suffered a data breach which exposed over. [redacted] unique email addresses. The breach also exposed the names of users, password hashes and the titles of converted documents. Hashing is a mathematical process that creates a fixed length string of letters and numbers to securely store and compare passwords in a database – so that companies do not store the exact passwords of users. When these hashes are leaked, they can be compared with the hashes of simple password hashes to see if they are identical – if they are then they can be safely assumed to be the same password. This means that non-unique or reused passwords are at risk when the hashes are leaked.

There was a plethora of content available on the internet regarding the. [redacted] and [redacted] that the subject was a part of. Using the [redacted] and exploring the [redacted] yielded photos of the subject engaging in re-enactment social events and competitions, as well as connecting the assessment team with a series of internet communities hosted on Discord that led to further images of the subject.

The website [redacted] has public facing pictures and screenshots from its weekly games that can be accessed. The subject is viewable in some of these photos, and these images are referenced by the community discord server.

The subject has a clear media presence, with interview videos available on [redacted], alongside multiple uploads of podcast and radio appearances.

Risk Summary

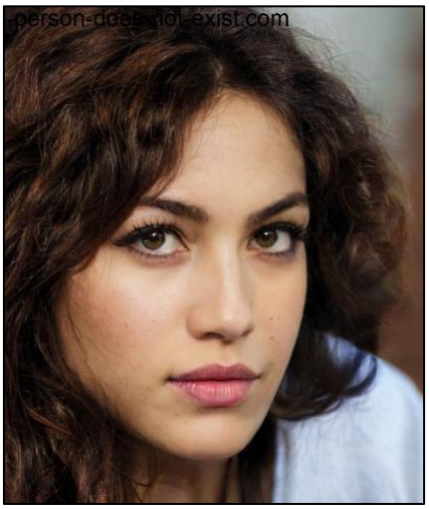
The following table presents a summary of the risks identified throughout the assessment. It can be interpreted based on the colour and order of information. Red = important and yellow=attention required. Blue= will likely not pose an ongoing threat but is worth your attention in determining if further action is required.

Summary of High-Risk Findings	
0	There were no findings that constituted a high-risk finding.

Summary of Moderate-Risk Findings	
1	The subject's personal email – Alison.marks@gmail.com is linked to a data breach involving [redacted] Files relating to this breach can still be accessed online.
2	Images relating to the subject and [redacted] were found online on multiple websites as well as Facebook. These images can be found in the technical section below.
3	Alison Marks name and [redacted] found in leaked file online. Data relates to [redacted] in a database that has a large number of personal email addresses of members – indicating a possibility for a breach of other information the subject may have shared with this organisation.
4	Potential addresses and phone numbers found in [redacted] but not verified as Alison Marks address: [redacted]

Summary of Low-Risk Findings	
5	[redacted] meetings that the subject attended are viewable online. These are images attached in the technical section.
6	Media relating to Alison Marks professional and academic life – Interviews, videos – Listed in the technical section.

Technical Report

Name	**Alison Marks**	
Alias/es	[redacted]	
Sex	Female	
Unique Identifiers	None	
Associated Addresses	[redacted]	
Email	Alisonmark56s@gmail.com	
Telephone:	[redacted]	
Links	[redacted]	
LinkedIn	[redacted]	
Facebook	[redacted]	
Skype	[redacted]	

Work and experience history

The subject has shared their work and volunteering history on LinkedIn, alongside their educational history and publications. It is possible to view this timeline without connecting to the subject and so it should be considered freely available.

Work History

Title	Organisation	Dates of work
[redacted] Manager	[redacted]	Aug-[redacted] – Present
[redacted] Manager, [redacted]	[redacted]	Sep-[redacted] – Dec-[redacted]
[redacted] Officer	[redacted]	Oct-[redacted] – Aug-[redacted]
[redacted] Manager	[redacted]	Jan-[redacted] – Oct-[redacted]
[redacted] &	[redacted]	Jul-[redacted] – Aug-[redacted]
Coordinator	[redacted]	[redacted]
[redacted]ation officer	[redacted]	Jul-[redacted] – Aug-[redacted]
Att[redacted] Service Supervisor	[redacted]	Feb-[redacted] – Jul-[redacted] Feb- – Nov-

Volunteering

Title	Organisation	Dates of work
[redacted] Volunteer	[redacted]	Oct-[redacted] – Oct-[redacted]
[redacted]	[redacted]	Oct-[redacted] – Jan-[redacted]
Volunteer	[redacted]	Sep-[redacted] – Sep-[redacted]

Publications

Title	Publisher	Date Published
[redacted]	[redacted]	Feb [redacted]
[redacted]	[redacted]	Sep [redacted]
[redacted]	[redacted]	Jan [redacted]

Human Verification of Subject

Determining the subject's identity required human verification. Although the team could assume the identity of the subject due to the widespread number of results relating to a "Alison Marks" working at [redacted] verification of the assumed identity was confirmed by a member of the assessment team that had previously interacted with the subject.

Alias Identification

[redacted]

Aliases are fictitious names that either a person or group use for a particular purpose. Determining someone's alias is critical in finding information relating to a subject, especially in an online context.

Throughout the assessment, two methods to determine the subject's alias were discovered.

The subject's public Facebook profile listed a[redacted] next to their legal name as seen in Figure 1. This confirms further references to the alias.

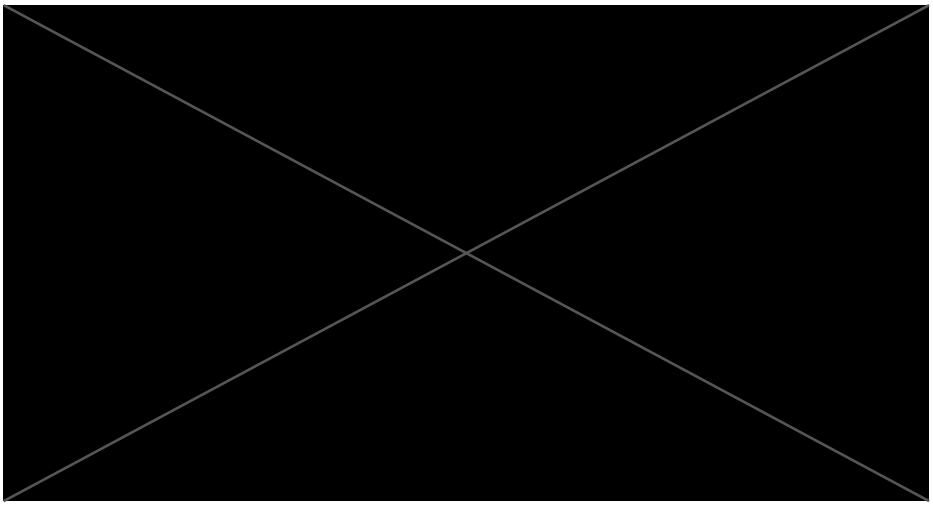


Figure 1: Subject's Public Facebook Profile.

[redacted] and Community

The subject's interest and knowledge around [redacted] is clear, and this section aims to cover the exposure of information about the subject relating to [redacted]

[redacted]

Google dorking is the process of using logical operators to filter for specific web results. Using this technique in unison with the subject's full name revealed that [redacted] Within one of these files, a record of the subject's name and alias can be found (see Figure 2). This further validates the information found on the subject's Facebook page and also identifies them as a member of . There are countless other full names – and most disclose their personal emails. There is discussion in the [redacted]

[redacted]

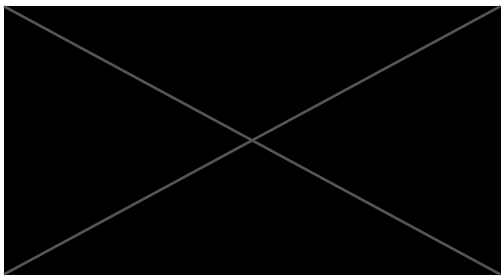


Figure 2: [redacted] File Dump

[redacted]

Searching for instances of the name [redacted] across [redacted] sites and resources quickly surfaced her [redacted] and [redacted] is worthwhile noting that this [redacted] (Viewable in Figure 3) can be associated with the subjects given name and reliably image searched.

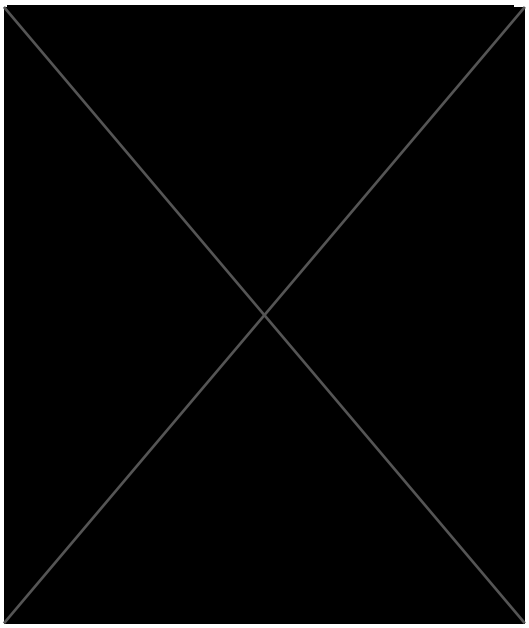


Figure 3 - [redacted]

[redacted]

[redacted]

Another Google Dorking search of the subject's alias, [redacted], revealed an image of the subject [redacted] in at [redacted] in 2016 as seen in Figure 4.

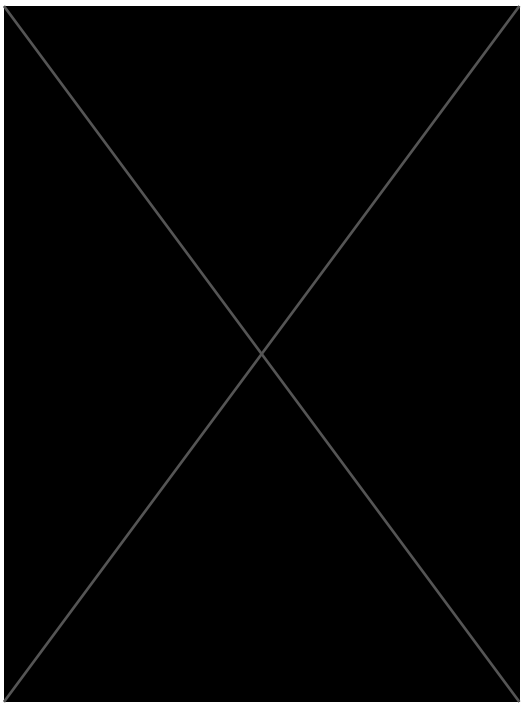


Figure 4: The subject at

– 2009

Another search of the subject's alias also revealed the results of a 200 competition, as seen in Figure 5. This also revealed details such as the subject's and being and , respectively.

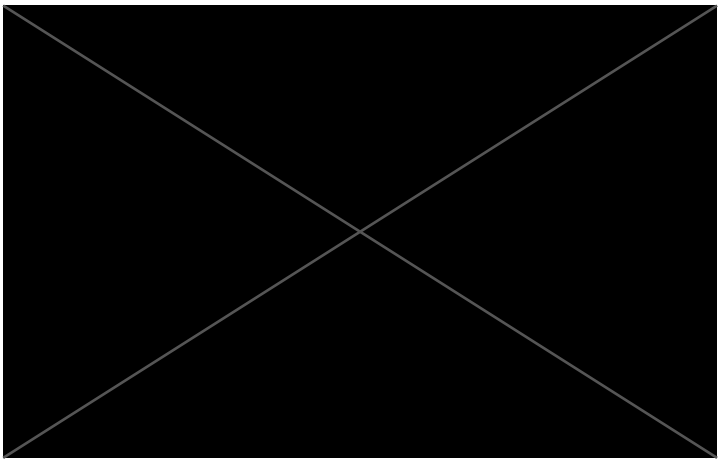


Figure 5: Scores

Event

The subject shared congratulations with participants in an event she attended, and photos of the event are available on Facebook. This can be seen in Figure 6.

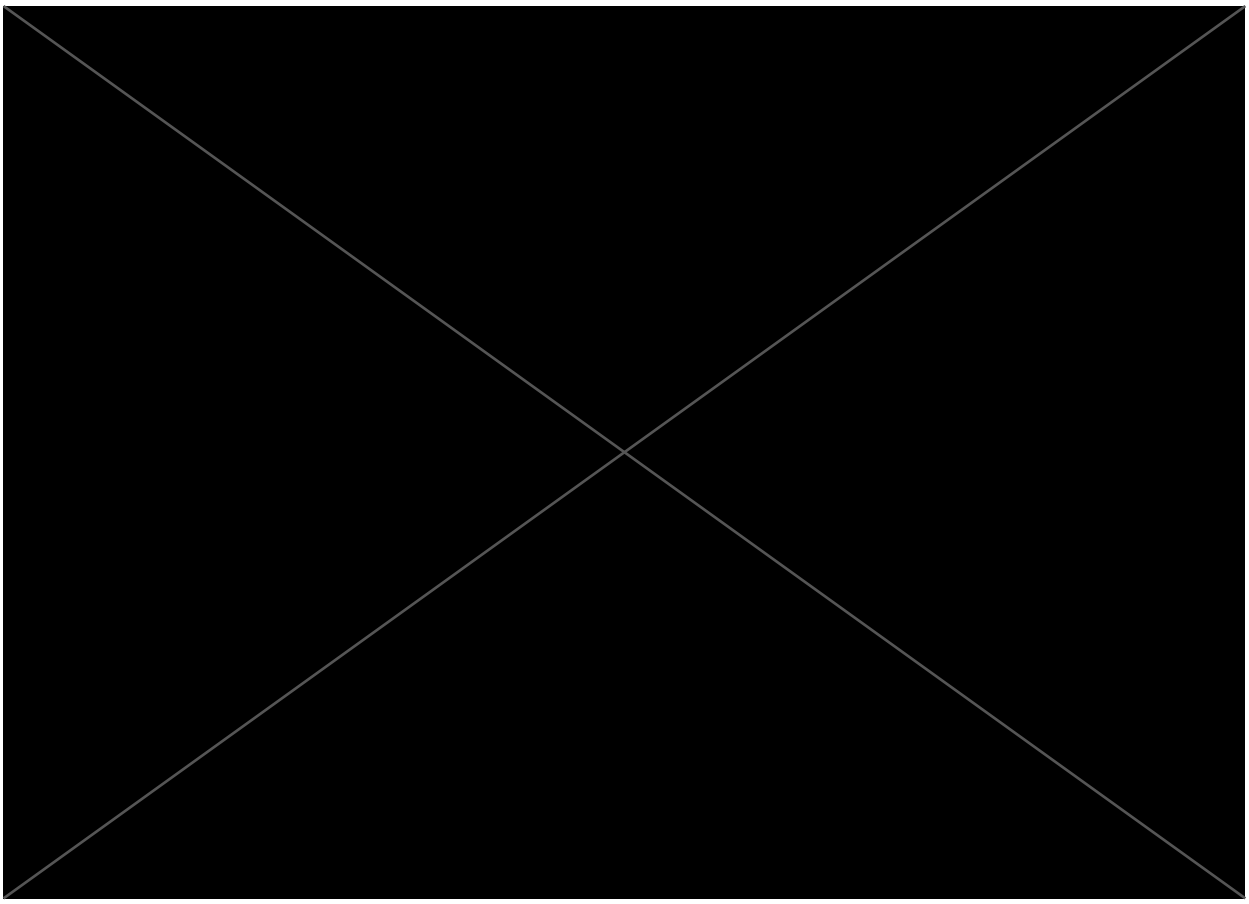
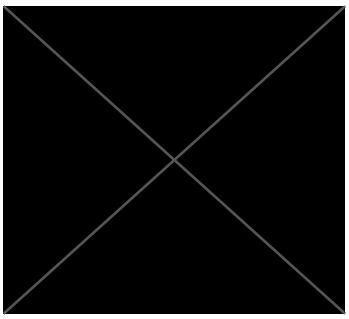
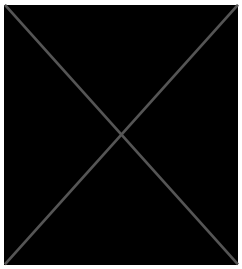
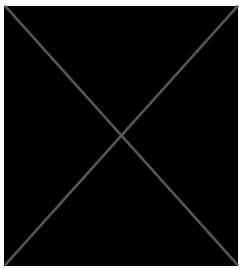
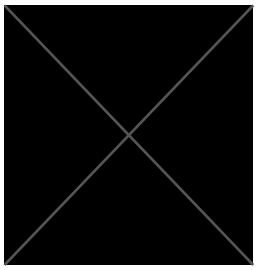


Figure 6 - An event hosted by the [redacted].

Discord Servers

Multiple discord servers were seen in the background of the [redacted] image, with some of those identified and searched by the assessment team. There were additional servers that were enumerated from within the named examples, but they are not mentioned as they are not relevant. If the subject does have a discord account, it was not identified.

Server Logo & Name	Server Description	Discord Link
	This server uses [redacted]. It is assumed to be a private discord server for university students.	N/A
	This is the central discord server for [redacted] and has been advertised as such on their website.	[redacted] – found through old link on their website https://discord.com[redacted]
	A [redacted] that the subject has been a confirmed participant of. The discord link is available on multiple Facebook posts by the [redacted]	[redacted] -= found through [redacted] page https://discord.gg[redacted]
	A community discord for members of [redacted] to communicate.	https://discord.gg[redacted]

Internet Investigation

Media Presence and Professional Profile

The subject's diverse set of roles in [redacted] knowledge has generated opportunities for mixed media appearances. These are easily discoverable and disclose the subject's voice and likeness. They are detailed here.

Audio Interview [redacted] FM

[redacted]

An interview was conducted by [redacted] FM' that spoke to the subject in the capacity of the regional [redacted] of the [redacted] It is available on their website and on Spotify, the former visible in Figure 7.

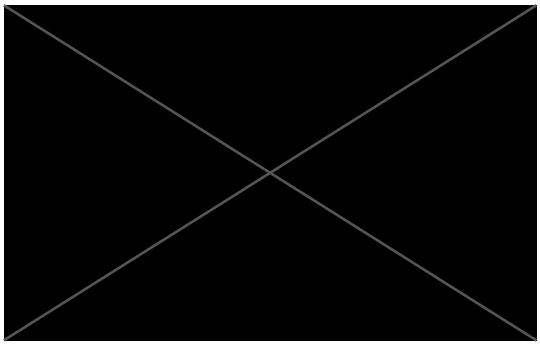


Figure 7 - The web page of [redacted] FM', hosting an audio interview with the subject. It is also available on Spotify.

Video Interview – [redacted] Domain

[redacted]

A video of an interview with the subject was uploaded under the title [redacted] by a user called [redacted]. The subject advocates for the protection of [redacted] a [redacted] A capture of the vimeo page that hosts the video can be seen in Figure 8.

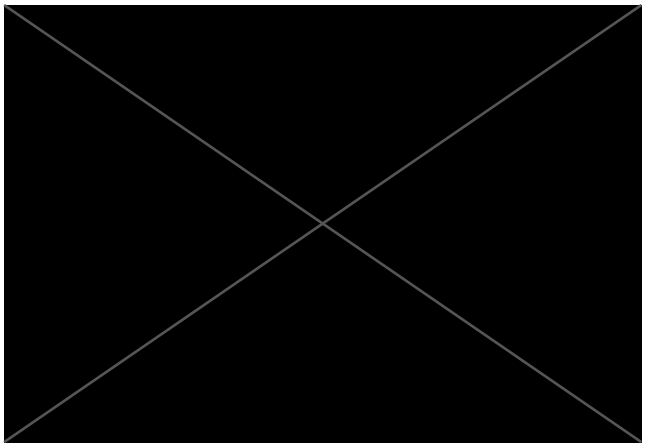


Figure 8 - A still from the video interview conducted with the subject.

[redacted] Hosted Images

[redacted]

A facial recognition search of the subject returned results relating to an [redacted] event hosted on a Zoom call (Shown in Figure 9 through to Figure 11). These calls were participated in by a range of people including the subject. The file names suggested that the first meeting took place in September of [redacted] and that the other two in December of [redacted]. These dates and file extensions/numbers can be manipulated to search through the public facing images that are hosted on the site, and as such photos of all the zoom calls are available, and the site provides a 'sitemap' that shares all the images on the website.

These pictures revealed the full names and faces of a lot of people in the shared circles of the subject. These people of interest could be identified almost exclusively through [redacted] – Also known as [redacted] via [redacted] Facebook account. The account had no settings configured for privacy and was entirely public facing. It was possible to identify discord and Facebook accounts for near enough everyone in these images. The subject's discord could not be identified.

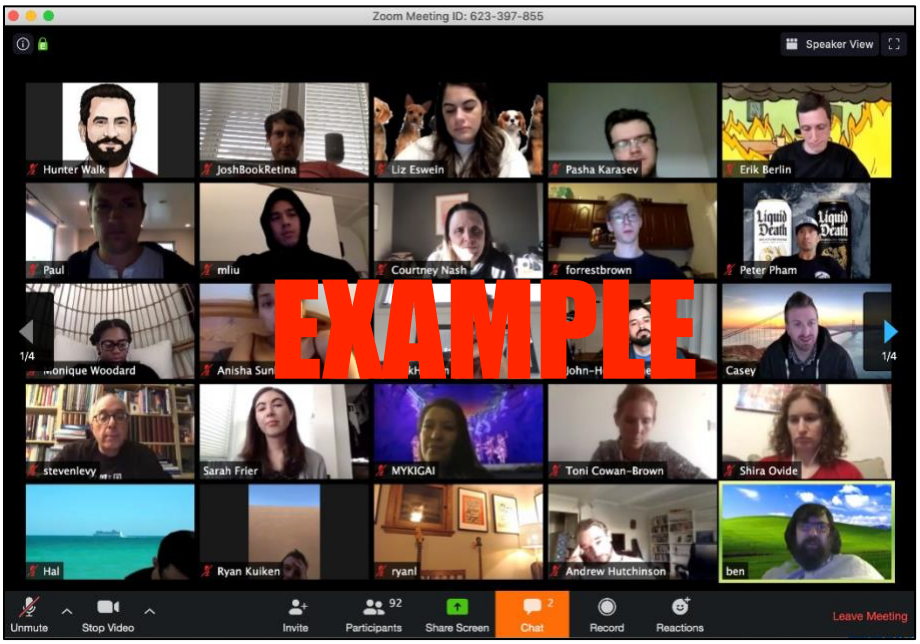


Figure 9: [redacted] Zoom call screenshot #1

Figure 10 - [redacted] Zoom call screenshot #2

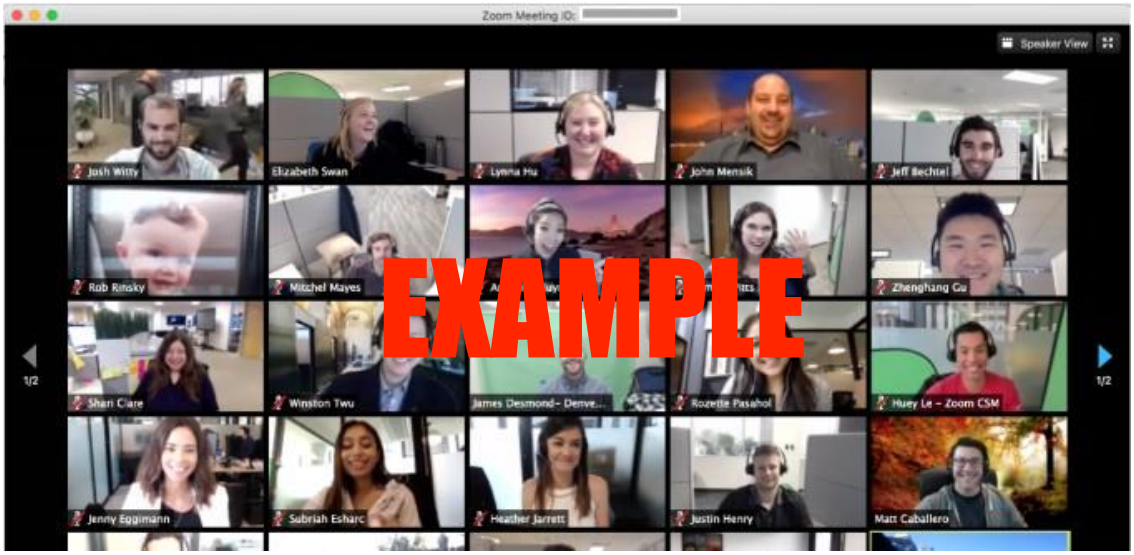


Figure 11 - [redacted] Zoom call screenshot #3

Facebook Enumeration

Exploring the Facebook account belonging to a connection of the subject's revealed three similar photos of the subject, an example of which is attached in Figure 12.

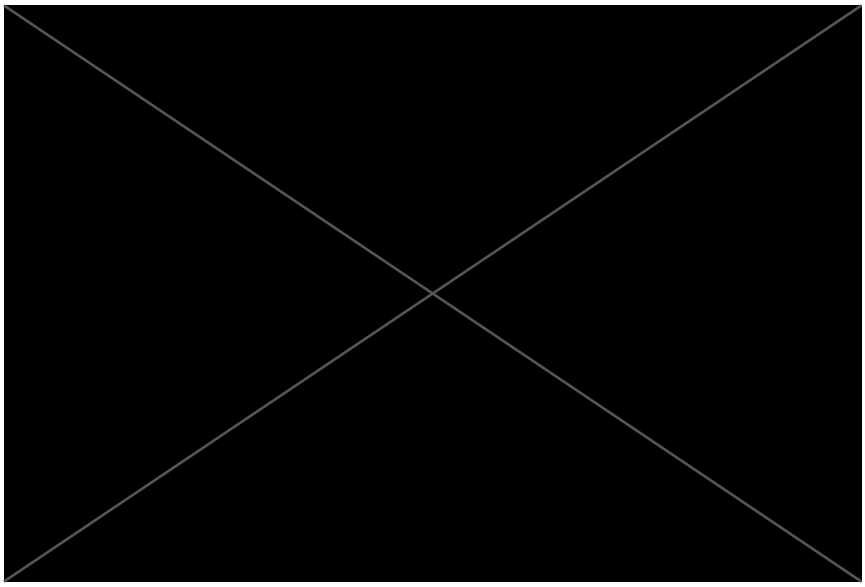


Figure 12 - A photo of surrounded by people one being identifiable as the subject.

Email Breach –

https://haveibeenpwned.com/

The website 'haveibeenpwned' allows a user to anonymously search if their phone number or email address has been involved in a data breach.

A breach is an incident in which data has been exposed to the public by an individual or group with bad intent. These breaches often reveal personal information relating to details submitted by users to the affected company/organisation.

Figure 13 shows a breach involving the subject's email address (alisonmarks@gmail.com) from the haveibeenpwned website.

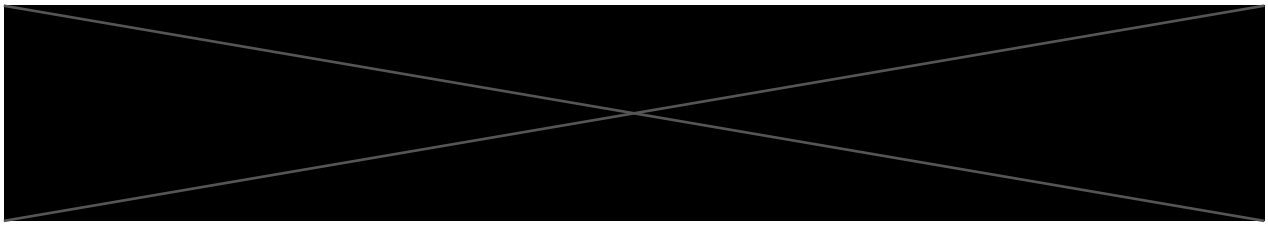


Figure 13: data breach

Remediation & Recommendations

This section of the report details the actions that could be taken to address the points of information that have been collated in the report. The recommendations made are only on how to reduce the available information that can be collated on the subject – and are not an evaluation on the potential harm to the reputation or security of the subject.

In addressing the [redacted] breach, the subject should identify all passwords that were used with the breached email and assess if they are used for current accounts. It is also worth signing up for 'haveibeenpwned' with their currently used email to guarantee that the subject is informed of future breaches as and when they happen.

The photos and information that relates to the subject in the context of [redacted] is two pronged in origin. The first and clearest appearance is on the subjects Facebook page – added as an alternative name or alias. The second is in the available data as leaked by the [redacted] domain, as visible in Figure 2. The former can be remedied by the subject, and the latter by contacting the domain web master for [redacted] to request these folders be made unavailable. This is something that the Cyber PATH team can help facilitate if there is interest.

The photos available on [redacted] Facebook page are public facing. The total enumeration of the people identified in the [redacted] was facilitated by [redacted] Facebook page that had no restrictions on what unknown users could search for. If interested in removing access to them, the subject should request directly that [redacted] alter the privacy settings of the image or their Facebook profile.

The [redacted] photos are hosted publicly and are reliably discoverable. A request could be made to remove the images or remove the subject's presence within them. This is something that Cyber PATH team can help facilitate if there is interest.