# Introduction

Use this document to refer to various notes regarding the application. This will include elements relating to the UI, plus the various API queries that have been used when ideating this concept

# Appearance

* Font = Lato
* Avatar = extracted from <https://graph.microsoft.com/v1.0/me/photo/$value> for the logged in user.

*Harris may know of a better way to do this*

* Iconography and Images in <https://teams.microsoft.com/_#/files/General?threadId=19%3A08CVHjyBnwukPmxUIokuWZcxsMeufDb6lW8sZ4MBR7w1%40thread.tacv2&ctx=channel&context=Assets&rootfolder=%252Fsites%252FBeCloudSafe%252FShared%2520Documents%252FGeneral%252FAssets>

# API Queries

## Number of Breached Email Accounts

1. Get all email accounts (“**mail”)** from <https://graph.microsoft.com/v1.0/users>
2. Check each email against HIBP via <https://haveibeenpwned.com/api/v3/breachedaccount/{mail}?truncateResponse=false>

(Not sure if there is a batch capability, or if there is a better query)

1. Count of mail addresses that have been breached

NB: Keep detail of breaches as that info is used in a different screen

## Microsoft Secure Score

1) Get “**currentScore”** value from

<https://graph.microsoft.com/v1.0/security/secureScores?$orderby=createDateTime&$top=1>

## Number of Breached Phone Numbers

1. Get all phone numbers (“**phoneNumber”**)from <https://graph.microsoft.com/v1.0/users>
2. Phone Number(s) needs to be converted to Country format. Ie: As an Australian phone number, 0434866666 needs to be input as +61434866666.

*Not sure if there is a field we can read to determine a user’s country*

1. Check each email against HIBP via <https://haveibeenpwned.com/api/v3/breachedaccount/{phoneNumber}?truncateResponse=false>

(Not sure if there is a batch capability, or if there is a better query)

1. Count of phone numbers that have been breached

NB Keep detail of breaches as that info is used in a different screen

## Number of Global Administrator Accounts

1. Get the “**count**” from controlName:“OneAdmin” section. From this query:

<https://graph.microsoft.com/v1.0/security/secureScores?$orderby=createDateTime&$top=1>

See example output below:

“controlCategory”: “Identity”,

“controlName”: “OneAdmin”,

“description”: “Having more than one global administrator helps if you are unable to fulfill the

needs or obligations of your organization. It’s important to have a delegate or an emergency

account someone from your team can access if necessary. It also allows admins the ability to

monitor each other for signs of a breach.”,

“score”: 1,

“implementationStatus”: “You currently have 6 global admins.”,

“**count**”: “6”,

“scoreInPercentage”: 100,

“IsApplicable”: “true”,

“controlState”: “active”,

“State”: “complete”,

“lastSynced”: “2021-09-22T00:00:00Z”

## Dormant Users

From https://graph.microsoft.com/beta/users?$select=displayName,userPrincipalName, mail, id, CreatedDateTime, signInActivity, UserType get a list of users (**displayName**) who have not logged in for more than 30 days using the

“signInActivity”: {

“lastSignInDateTime”: field.

If this field does not exist, the User can be ignored.

If the Today() - lastSignInDateTime > 30 Days then display the **displayName, lastSignInDateTime** (date only, ignore the time),& **Number of days since last signed in,** in descending order

## Percentage of Accounts using MFA

1. Get the “**scoreInPercentage**” from controlName “MFARegistrationV2” from this query:

<https://graph.microsoft.com/v1.0/security/secureScores?$orderby=createDateTime&$top=1>

See example output below:

“controlCategory”: “Identity”,

“controlName”: “MFARegistrationV2”,

“description”: “Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.”,

“score”: 3.7,

“implementationStatus”: “You have 7 out of 17 users registered and protected with MFA.”,

count”: “10”,

**“scoreInPercentage”: 41.17,**

“total”: “17”,

“IsApplicable”: “true”,

“controlState”: “active”,

“lastSynced”: “2021-09-22T00:00:00Z”