

Welcome to this week's edition of Defuse News

A weekly briefing for people whose profile attracts attention.

Blocking is not assessing

Why filtering abuse away from a prominent person is not the same as knowing who is a danger to them

In August 2026 Luigi Mangione pleaded guilty to interstate stalking and cyberstalking resulting in death, over the killing of UnitedHealthcare's chief executive Brian Thompson in December 2024.

On the prosecutors' account he arrived in New York more than a week beforehand and conducted surveillance on locations Thompson used, including the area around his hotel and the venue hosting the company's investor conference.

He had never sent Thompson a threatening message and had no need to make contact at all. What he needed to know was where a chief executive would be on a particular morning, and a company that announces an investor conference has published half of that already.

It is a familiar shape. Across the research, only around one in ten of those who went on to harm a public figure had communicated a threat beforehand, to the target or to the authorities.

🛡️ What prominent people are told to do

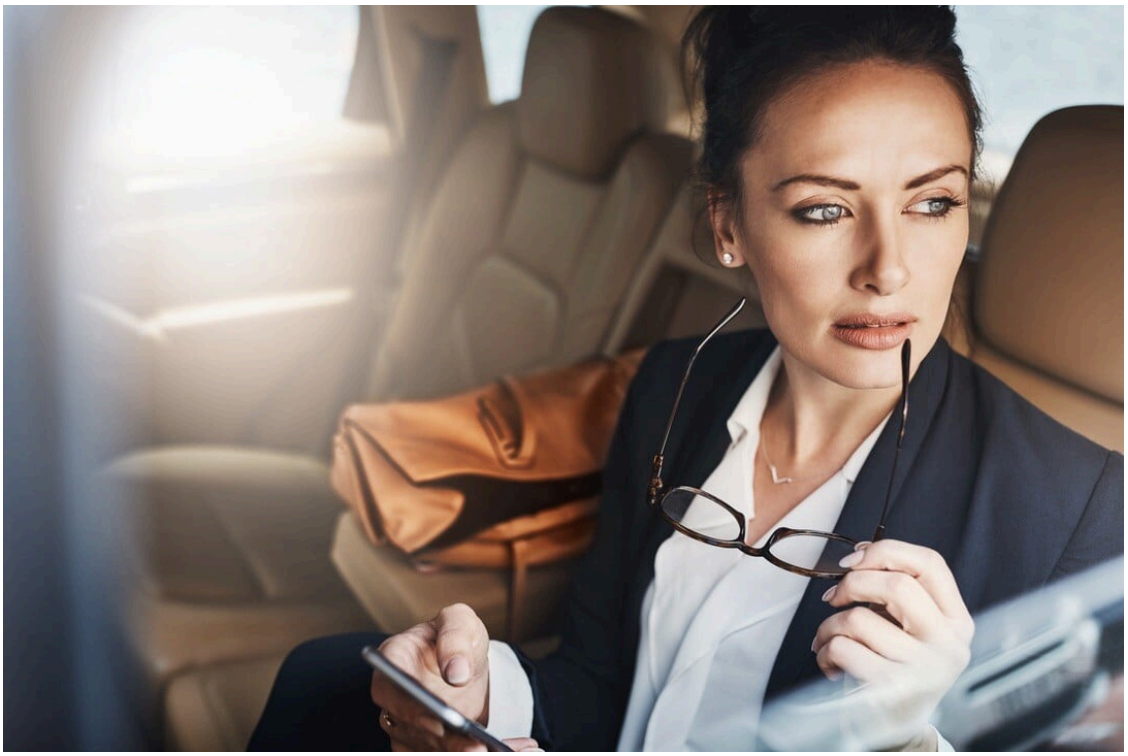
For years the standard advice to a prominent person has been the same, and it comes from serious people.

Do not rise to the bait. Block. Mute the notifications. Take a break. Report the worst cases to the police and send the lesser ones to the platform. The platforms have built the rest of it in: filtering that hides comments containing listed slurs, emojis or keywords before anybody sees them, and screening of notifications from unverified accounts.

For the purpose it was designed for, that advice is right. Amplification is real, and so is the harm to the person reading it.

But look at the sorting criterion. The worst cases. Worst by what measure? By how the words read — the one measure the research says has almost no bearing on what follows. Everything below that line is blocked, hidden or muted, and in most offices, nobody sees it again.

A system that blocks and never assesses may be adding to the risk rather than reducing it.



🔎 There is no single population to watch

Mangione was a stranger to Thompson. The British cases run the other way: in the attacks on Members of Parliament, all on the public record, the attacker came each time from the constituent population, a feature of that job and no rule about prominence.

Where the target is a private individual, threats are so common that, on the forensic psychologist Reid Meloy's calculation, they carry little predictive value on their own. One qualification is firm: all threats between intimate or former intimate partners must be taken seriously, and they rarely arrive through the channel automation watches.

Which is the point. You cannot pre-sort by who somebody is, any more than by how angry their language sounds. The employee let go last spring, the contractor in a payment dispute, the supporter who has written for two years and the stranger nobody has heard of are in the same pile until somebody competent reads it.

📂 Everything shared with us was assessed

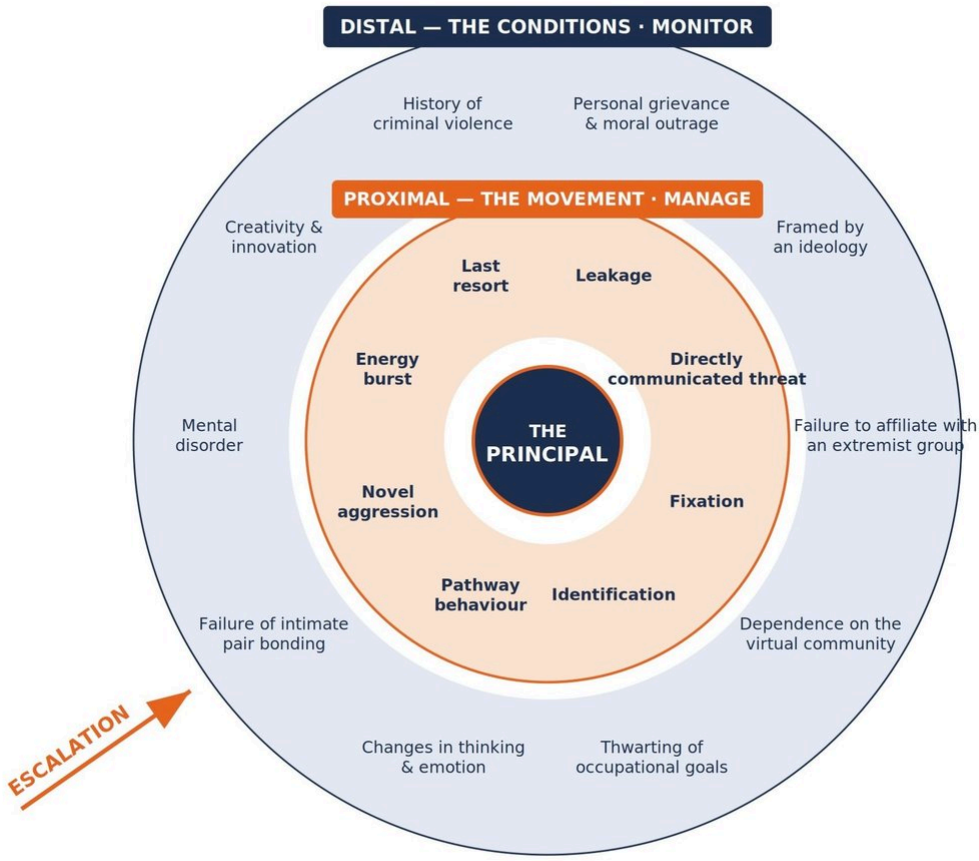
The practice we built inside Parliament was simple to state and demanding to run. Everything shared with us was assessed — not the abusive and threatening items picked out of the pile, but everything, because whether a communication is concerning is the conclusion of an assessment rather than the thing that qualifies it for one.

Three reasons, none about offensive language. A criminal offence may have been committed, and nobody will know unless somebody reads the message properly. Escalation is visible only across the set; it shows up as one author changing frequency, channel and subject over weeks. And the proximal warning signs are not common sense. They sit in plain sight, and they look odd, not frightening.

Meloy, writing with the former FBI behavioural analyst Mary Ellen O'Toole, identified the weak point, and it is not the technology. It is the untrained reader, who rationalises the odd message, minimises it or decides it was a joke.

Automation is that reader at scale, watching a channel where leakage (the communication to a third party of an intent to do harm) never appears at all.

Escalation is movement from the outer ring towards the inner one, and towards the person in the middle.



Indicators from the TRAP-18 — Dr J. Reid Meloy (Meloy & Gill, 2016). **www.defuseglobal.com**

⚠️ Where the risk comes back

Blocking removes a channel you could see. It does not remove the person. Where contact goes next — a new account, an intermediary, the switchboard, a request for a meeting — is somewhere nobody is watching.

The writer Chelsea Cain told Amnesty International that deleting her account was the point things escalated.

It changes what the office believes, too. When the abuse stops appearing, the principal believes it has stopped and the team believes it is covered. That is an absence of

information mistaken for reassurance.

None of which means the principal should read it. But filtered is not the same as deleted, and away from the principal is not the same as away from everybody.

Three questions worth asking of any system in use

1. Triage, or delete? Filtered material should be retained and searchable, not discarded at the point of blocking.

2. Who actually reads it? Every flagged message, and by someone trained in behavioural threat assessment and management.

3. One author, over time. Can it follow the same person across platforms, and does it register approach: a request for a meeting, contact with staff or family, knowledge of a movement never made public?

Threat rests on intent and capability. An alarming message proves neither, and silence proves nothing at all, least of all silence you have manufactured yourself.

Prevention not Prediction.

One of the British cases ended with a sentence rather than a funeral. In 2017 a man told a meeting in a pub what he intended to do. Somebody present passed it on, and it reached the team I ran, The Parliamentary Liaison and Investigation Team, third-hand and unsolicited.

Much that arrived by that route was not genuine. This was assessed as a genuine threat, and the investigation was initiated on that basis. He was sentenced at the Central Criminal Court in London in May 2019 to life with a minimum of twenty years, having researched his target's movements and never written to her.

Volume arrives, most of it amounting to nothing, and the only way to find the item that matters is to look at all of it.

Click here to email us with any concerns about abuse and threats you are receiving.



🎧 On the podcast: True Wealth

Success changes a person's threat profile long before anybody has decided to do anything about it. More visibility. More personal detail sitting in public view. Routines and movements that are easier to work out than they were a year ago. And attention that is difficult to read — some of it warm, some of it odd, some of it worth a second look.

Personal security tends to get considered after something has happened. Guards, gates and cameras have their place, but they are one part of a response and not the whole of it.

I joined Anthony Ng Monica and Fintan Costello on True Wealth to talk about how wealthy individuals and families can think more clearly about their own safety.

The conversation covers:
🔎 How privacy and personal exposure change risk
🧠 Why behaviour matters when you are assessing a concern
🛡️ Where physical security actually fits
📋 What to do if you believe you are under threat

The aim throughout is prevention: identifying what matters early and taking measured action before a concern becomes a crisis.

My thanks to Anthony and Fintan for the invitation.

📅 **Tuesday 22 September** 🕛 **12.30pm BST**

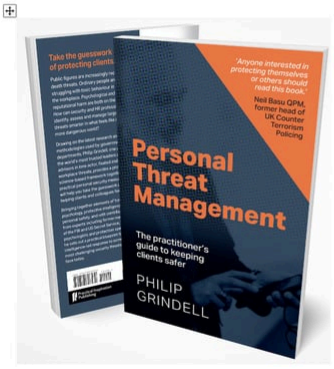
🎧 **All podcast platforms**

Listen on Apple Podcasts.

Listen on Spotify

From the author of this newsletter

Personal Threat Management



The practitioner's guide to keeping clients safer

The book is about judgement rather than equipment. How to tell the difference between somebody who is frightening and somebody who is dangerous. How to read behaviour as it changes over time, instead of counting incidents one by one. And what should happen next at each stage.

It is written for the people whose work includes keeping somebody else safe: family offices, chiefs of staff, lawyers, HR teams and security leads. It draws on the methods used by government threat assessment units, with contributions from former FBI and US Secret Service specialists, psychologists and protection practitioners.

"Anyone interested in protecting themselves or others should read this book."

Neil Basu QPM, former head of UK Counter Terrorism Policing

"A significant resource to anyone involved in helping others feel safer."

Kim Leadbeater, Member of Parliament for Spen Valley

Click here to purchase your copy



If anything in this newsletter has caused you to think, you may benefit from our help.

Contact us at info@defuseglobal.com

Defuse Ltd, 124 City Road, Old Street, London EC1V 2NX, United Kingdom, +44 02072930932

Unsubscribe Manage preferences

Chat

- New Chat

Search

Close modal

The data of AITOPIA isn't real-time. WebAccess Feature combines the intelligence of AITOPIA with realtime web information, allowing GPT to handle real-time information-related questions more effectively. Upgrade to gain this feature, and worry no more about outdated information!

Upgrade Now

Page Content

The Target May Not Be Who You Think It Ishttps://25099926.hubspotpreview-eu1.com/_hcms/preview/email/424460136646?portalId=25099926&preview_key=MgeWinfN&_preview=true&from_buffer=false&hsPreviewerApp=email

Summarize

Get a brief overview of the main points and key takeaways



AITOPIA
This week's edition of Defuse News focuses on the idea that the perceived target of attention or risk may not be the true target. It highlights various patterns in personal risk, including behavioral threats and unwanted attention. Key insights include how easily individuals can be found online, the fact that the person attracting attention is often not the only one at risk, and the need for broader awareness among those surrounding high-profile individuals. The piece emphasizes that those most capable of noticing potential risks are often not part of the security team. Overall, it serves as a guide for individuals and families on managing personal privacy and safety proactively.

Compare with GPT-6 Astra

Stop generating



AITOPIA

Vision

Close modal

Upload an image to easily get intelligent explanations and extract text from your images.

Supported image types are JPEG and PNG
Drag your Image here or click to upload
Or

Take a screenshot

Upload File

Close modal

Upload a PDF, Word, Excel, or PowerPoint file to easily get intelligent summaries and answers for your documents.

Supported file types are PDF, Word, Excel, and PowerPoint

Drag your file here or click to upload

Ask me anything...

Group Chat Web Access



00:00

10 Upgrade

Free Plan

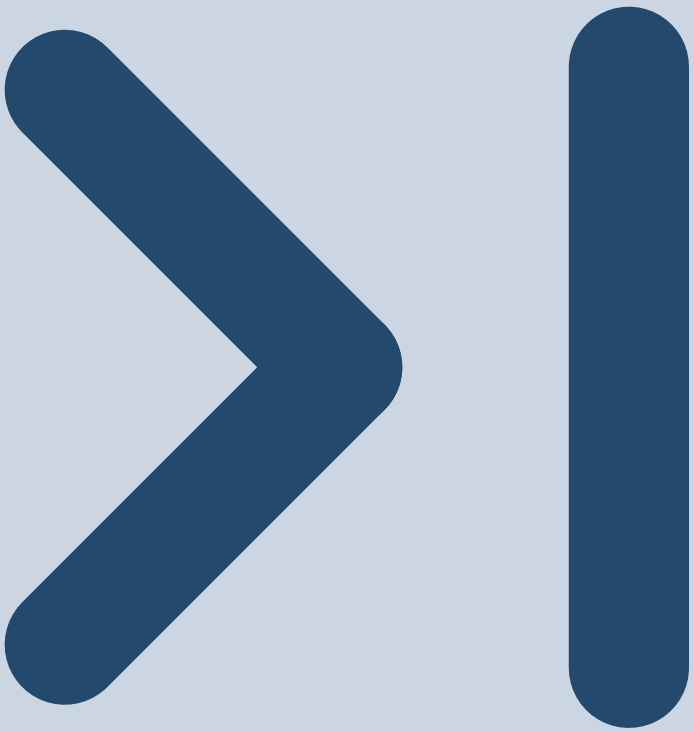
10

Upgrade

Fast Text
10
AITOPIA, GPT-6 Luna, GPT-4o Mini, GPT-5 Mini, GPT-4.1 Mini, Claude 3.5 Haiku, Grok 3 Mini, Claude 4.5 Haiku, Gemini 3 Flash, Gemini 2.0 Flash, Gemini 2.5 Flash, Gemini 2.5 Flash-Lite, Gemini 3.1 Flash-Lite, Llama 3.3 70B, Llama 4 Maverick, Llama 4 Scout, GPT Image 1 Mini, GPT Image 1.5, SDXL v1.0, DeepSeek V3

Advanced Text
1
GPT-6 Astra, GPT-5.6 Luna, GPT-5.1, GPT-5.5, GPT-5.6 Sol, GPT-5.6 Terra, GPT-5.4, GPT-5, GPT-4o, GPT-5.2, GPT-4.1, o1 Mini, o3 Mini, o4 Mini, Grok 4.3, Claude Sonnet 5, Grok 3, Claude Opus 5, Claude 3.5 Sonnet, Claude 4.5 Sonnet, Claude 4.5 Opus, Claude Opus 4.8, Gemini 1.5 Pro, Gemini 2.5 Pro, Gemini 3 Pro Preview, Gemini 3.1 Pro, Gemini 3.5 Flash, Llama 3.1 405B, GPT Image 2, Nano Banana, Nano Banana 2, SD3, SD3 Large Turbo, DeepSeek R1

Agent
0
Invite Friends to get more credits

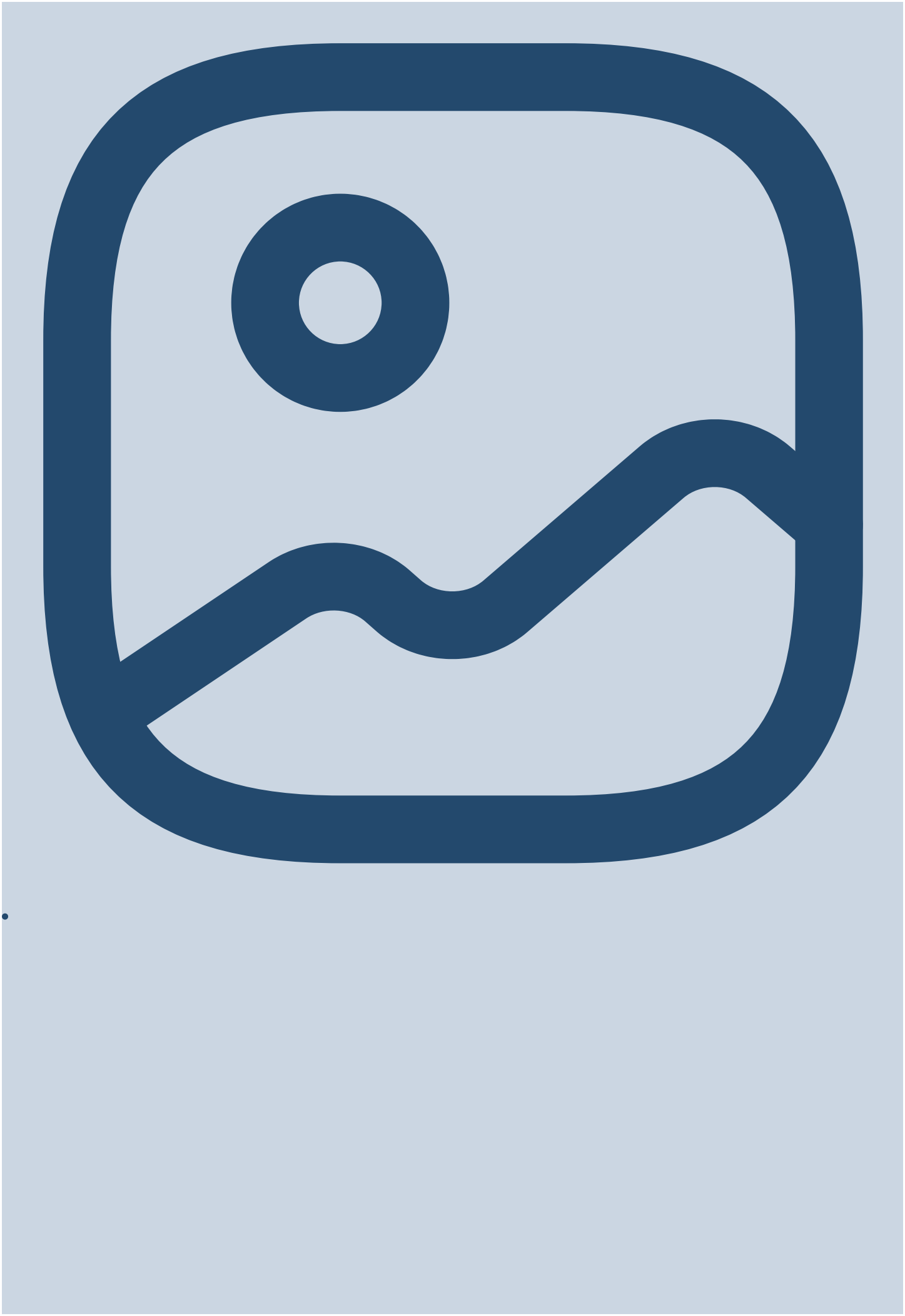










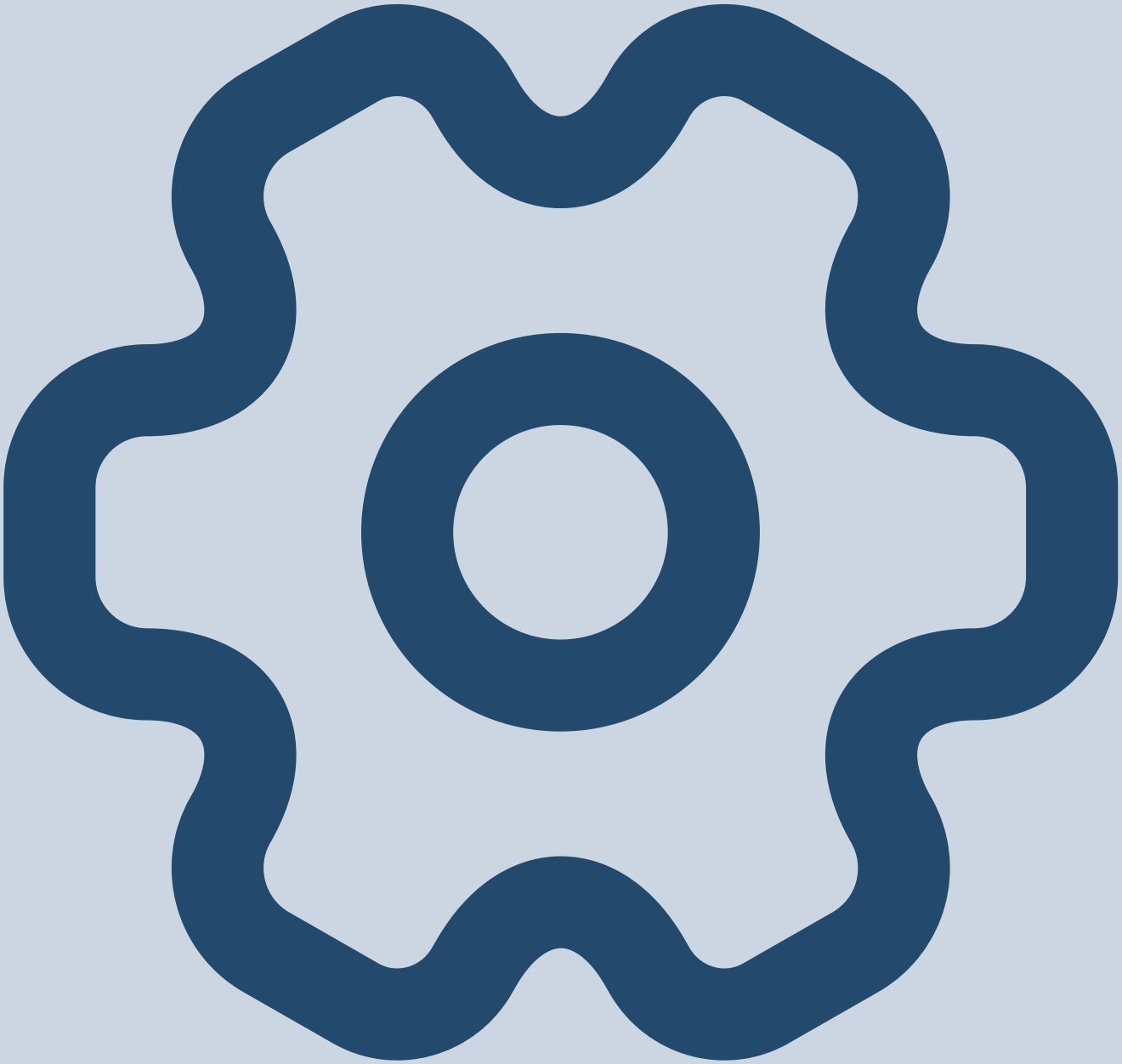














Log in as a user

What's New



How to use



Feedback

Invite & Earn

Close modal

Earn 5 Fast credits & 1 Advanced credit for both of you and your friend.Earn more when you refer more!



Refer your friend with an Invitation link



Your friends sign up



They install extension & login. You both earn credits!

Copy Invitation Link

Check Invitation Records

x



- 