OSINT Reconnaissance:

-by Arpit and Kush

-presented by *ideathon loosers*

Exposing your digital footprint before attackers do.

Core OSINT Techniques

Six Ways Attackers Find You Online

Image Reversal

Tools like Cleanup.pictures and Yandex identify where your photos appear online, revealing location data and associations.

Social Mapping

Google operators (site:instagram.com intext:username) expose all public posts, comments, and tagged content linking to your profile.

Document Harvesting

Filetype searches ("name" filetype:pdf OR docx OR xlsx) surface resumes, court records, and official documents containing personal details.

Facial Recognition

FaceCheck.id links your photo to thousands of indexed images, building visual profiles across the web.

Breach Mapping

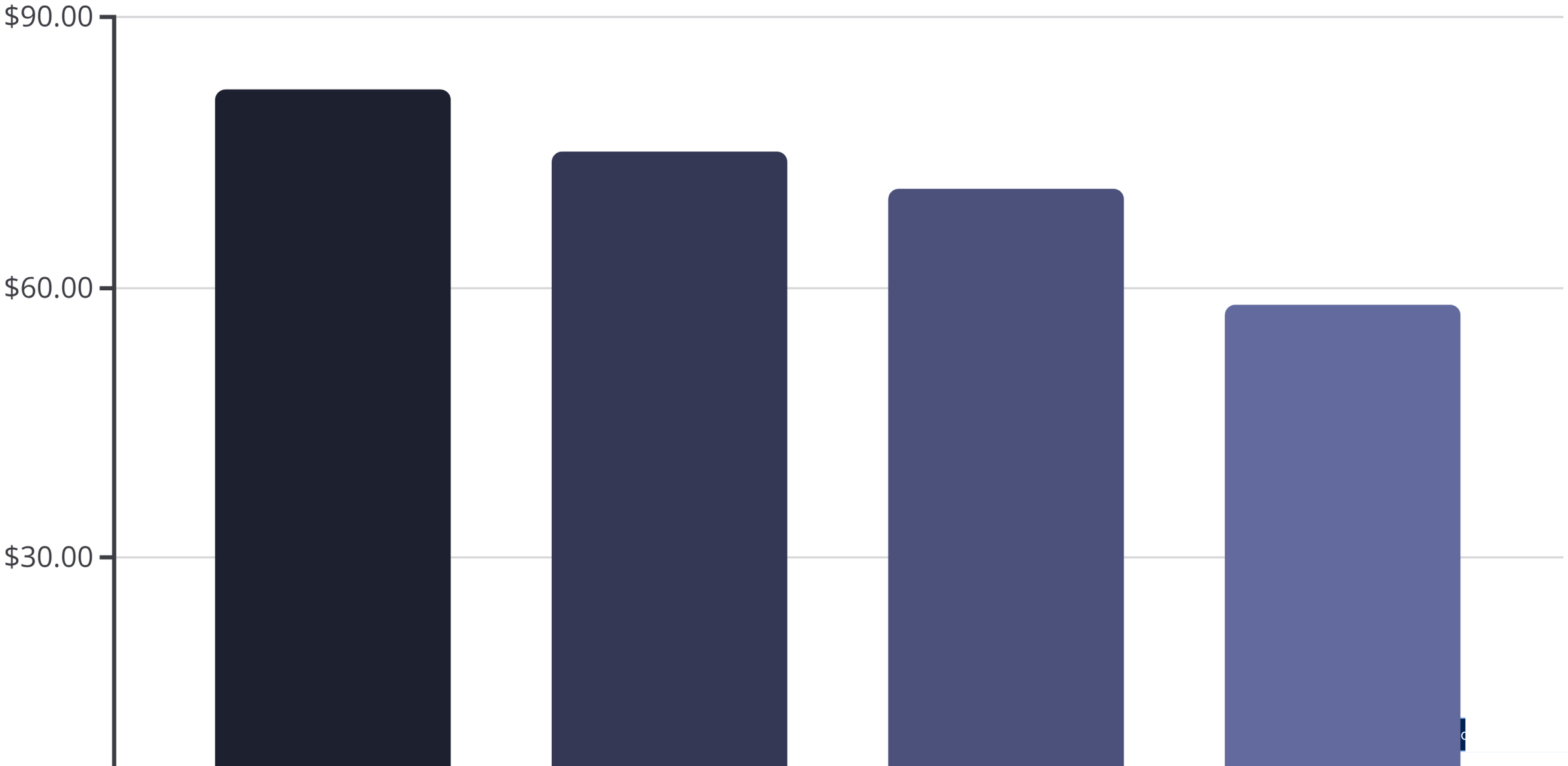
HaveIBeenPwned reveals if your email appears in past breaches, exposing linked accounts and credentials.

Username Tracking

InstantUsername.com catalogs every website where your username exists, creating a complete account inventory.

Why OSINT Reconnaissance Matters

Attackers combine OSINT data with social engineering tactics to enable breaches, fraud, and targeted attacks. The threat is both widespread and severe.

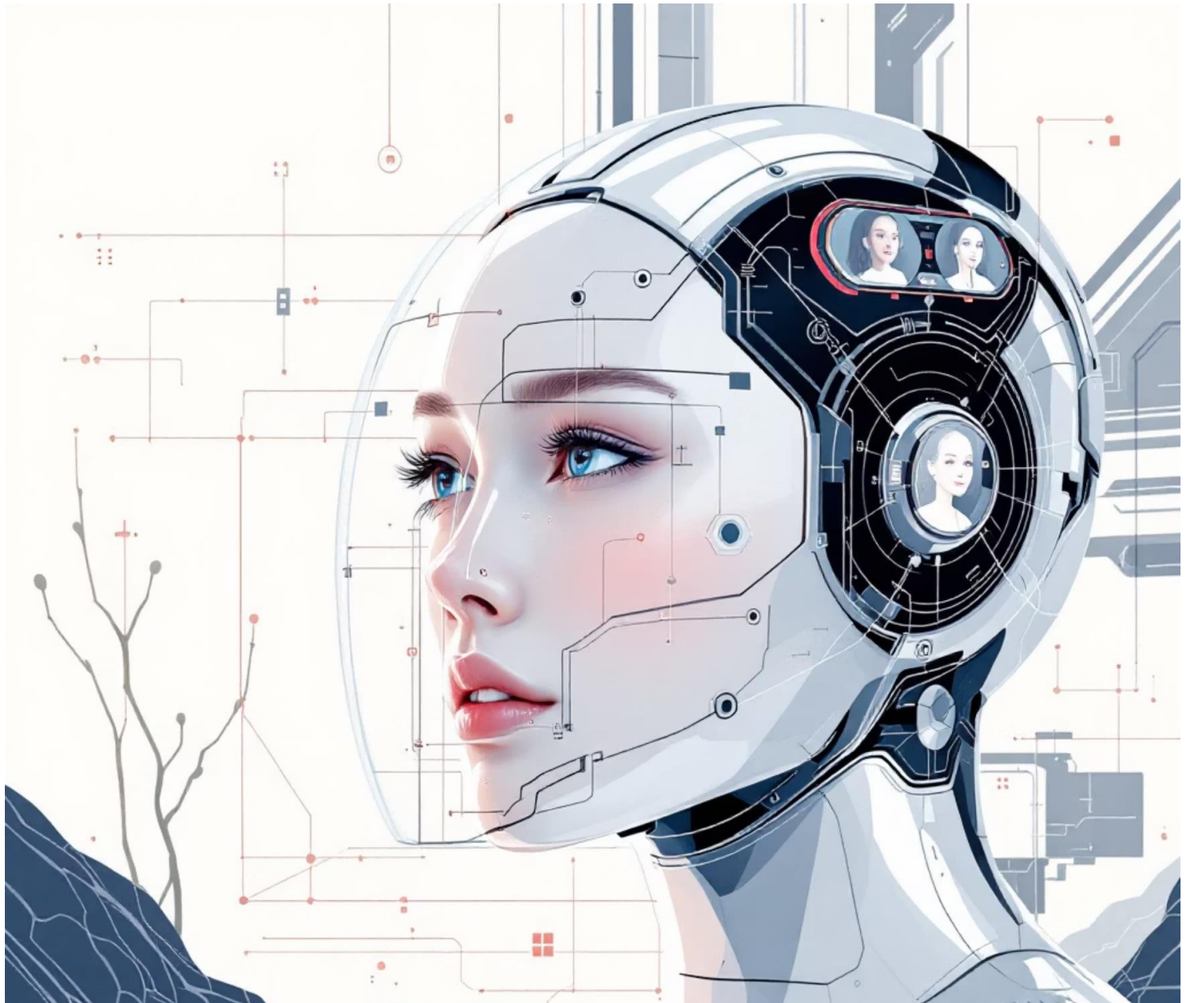


The Scale of Profiling

Billions of Images, Millions of Profiles

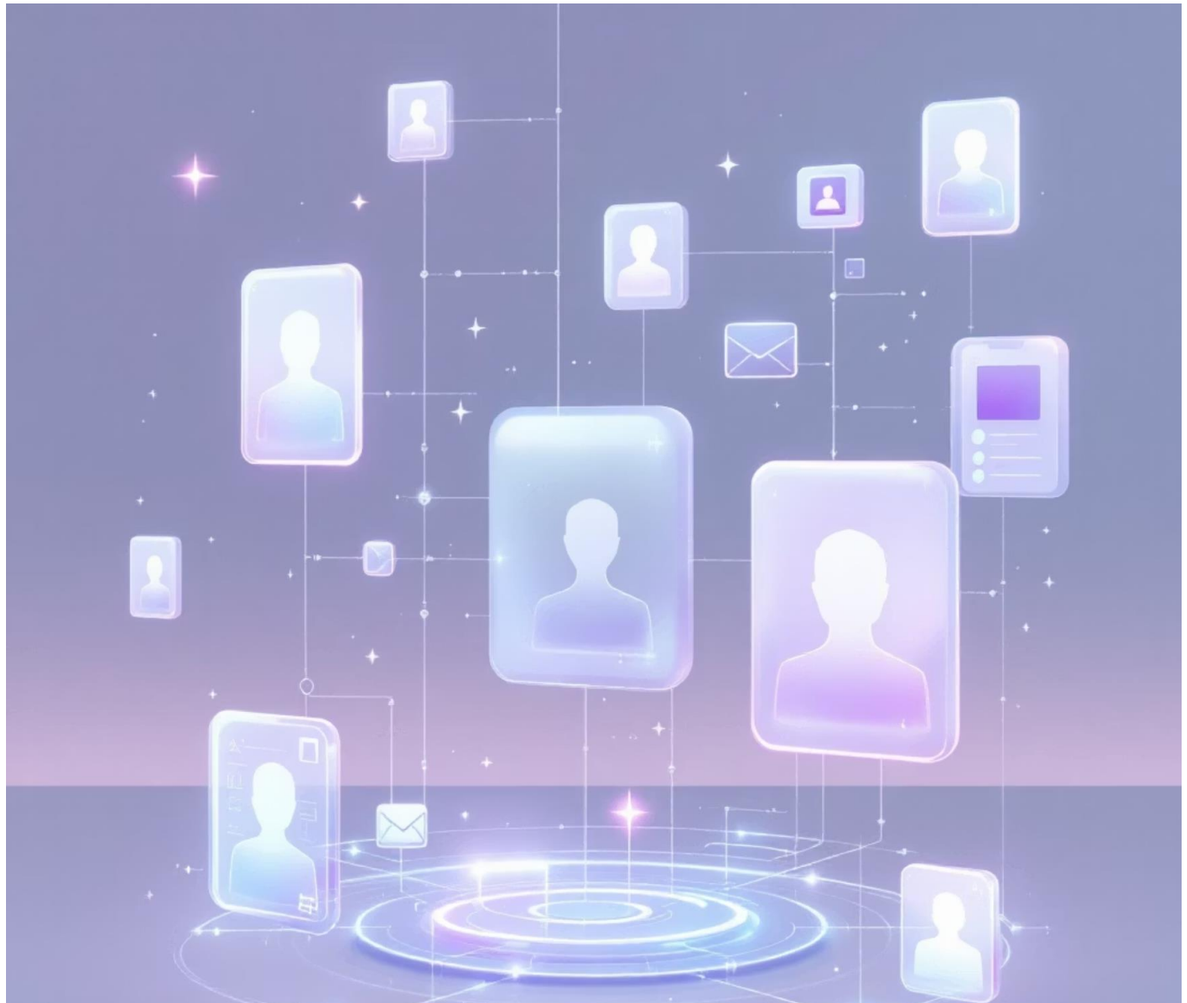
Face-Recognition Infrastructure

Companies have invested approximately **$8.83 billion in 2025** to build facial recognition databases. Clearview AI alone reported access to billions of indexed images and faced multi-country fines for unauthorized scraping.



The Exposure Risk

Every public photo, document, and social post becomes searchable metadata. A single high-resolution profile picture can be indexed by dozens of facial recognition systems within hours. Your online presence is permanent, searchable, and weaponizable.



Defense Strategies

Seven Practical Steps to Reduce Your Digital Footprint

Scan Your Exposure

Use reverse-image checkers and document searches to audit what's publicly available in your name. Prioritize removal of high-risk documents first.

Secure Document Sharing

Never publish resumes or sensitive documents with your full name on public platforms. Use private sharing links, anonymized filenames, and privacy-focused upload services.

Redact Personal Affiliations

Avoid publishing exact graduation years, university names, or locations. Use safer phrasing or consider removing affiliation details entirely from public profiles.

Lower Photo Resolution

Avoid uploading high-resolution pictures on public platforms. Compress images and strip EXIF metadata containing geolocation, camera model, and timestamps.

Strengthen Authentication

Enable two-factor authentication on all accounts. Use unique, complex passwords across different platforms to prevent credential stuffing attacks.

Monitor Breaches

Subscribe to breach monitoring services. Schedule regular checks (monthly or quarterly) to detect if your email appears in newly disclosed breaches.

Privacy Education

Develop awareness habits. Before posting locations, high-resolution photos, or personal milestones, pause and assess the risk to your security posture.

Proposed Solution

Public Surface Scanner: An Integrated Defense Platform

A web-based tool that audits your OSINT exposure and provides actionable remediation steps.

1

Risk Dashboard

Input your name, email, or username. Output includes: count of public documents, reverse-image matches, geotagged posts, username reuse map, and breach database hits.

2

EXIF Stripper

Automatically removes metadata from images before sharing, eliminating location data and device information.

3

Attacker Simulator

Shows users an anonymized mock profile of what attackers see—compiled name, workplaces, locations, and photos—making abstract risk tangible for non-technical audiences.

Feasibility: Leverages existing open-source APIs and freely available data (Google Dorks, HaveIBeenPwned, FaceCheck). Minimal infrastructure costs. Scales from individual dashboards to enterprise/university deployments and third-party APIs.

Impact & Outcomes

Building a Culture of Digital Privacy

Personal Exposure Score

Users receive a clear metric showing how much of their data is publicly visible and specific action steps to reduce their footprint.

Public Awareness

Turns complex OSINT concepts into interactive, educational experiences. Non-technical users understand privacy risks and how reconnaissance enables breaches.

Institutional Training

Schools, companies, and government agencies deploy the tool to train employees on online safety, reducing phishing, identity theft, and social engineering attack success rates.