Optery

Personal Data Removal: A Core Cybersecurity Measure

Why data broker removal is a must-have for organizations

The Overlooked Cybersecurity Risk

Personal data exposure is the biggest cyber threat to organizations today. It enables the most successful attack vectors: social engineering and the use of compromised credentials. Despite this reality, many companies continue to overlook a major security risk—vast amounts of employee personal data readily available on data broker sites.

Attackers use this information for reconnaissance and to target employees with phishing, vishing, smishing, business email compromise (BEC), and other vectors. Proactively removing exposed employee data is critical for reducing the volume of such attacks.

Today's Attackers Exploit Exposed PII

While companies should continue to invest in infrastructure and awareness training, these reactive measures by themselves have proven to be insufficient in stemming the tide of PII-based attacks, which remain the top source of organizational breaches.

Evidence From Industry Reports:

Phishing, smishing, and BEC were the most commonly reported attack vectors in breach notices from privately owned businesses in 2024. For publicly traded companies, **credential stuffing** was the most cited attack vector. (Identity Theft Resource Center 2024 Data Breach Report)

Phishing attacks surged in Operational Technology (OT) environments, rising from **49% to 76% year-over-year**, with **BEC affecting nearly two-thirds of organizations**. (2024 State of Operational Technology and Cybersecurity Report)

Valid Accounts was the most common successful attack technique across federal, state, local, and private sector infrastructure, responsible for **41% of successful attacks. Cracking password hashes succeeded in 89% of USCG assessments for Domain Administrator access**. Spear-phishing was the second most common successful attack technique. (CISA & USCG FY23 Risk and Vulnerability Assessment Report)

How Attackers Use Data Broker Information

Reconnaissance and target selection for social engineering

Data broker sites make it easy for attackers to gather intelligence, identify targets, and launch social engineering attacks, and threat actors are taking advantage of this.

Black Basta ransomware gang’s use of data brokers

The recently leaked Black Basta chat logs reveal how modern ransomware groups operate—using employee info from data broker sites for reconnaissance and to facilitate social engineering campaigns. The leaks show that members of the group leveraged data from data brokers ZoomInfo and RocketReach to assess a company’s financial status and identify employees to target. After gathering intelligence on potential victims, the group deployed phishing emails, fake download links, and other social engineering tactics.

Scatter Swine and the 0ktapus campaign

The use of data brokers by Black Basta isn’t an isolated case. For instance, threat intelligence from Okta Security has previously indicated that the cybercriminal group Scatter Swine harvests mobile phone numbers from data brokers that link phone numbers to employees at specific organizations. This info was used during the infamous 0ktapus campaign for mass smishing attacks, compromising nearly 10,000 credentials across 130 organizations.

These examples highlight the serious and ongoing security risk posed by data brokers. Companies must consider data broker exposure as a key component of their attack surface and actively work to reduce it to prevent being targeted.

Without easy access to employee PII, it is much more difficult for attackers to identify victims and carry out social engineering campaigns. As an expert OSINT hunter recently told us, “If the data isn’t out there on an individual, the bad actor is going to move on to the next person.”

2 Data brokers help facilitate credential-based attacks

Beyond social engineering, data brokers help facilitate credential compromise. With the data broker profiles of employees at their disposal, attackers can not only launch targeted email, voice, and messaging scams, they can also cross-reference a target’s email with breach repositories to find their password hashes. These can then be cracked and tested on company systems.

Ethical hacker Rachel Tobac demonstrated how easy this is to do when she hacked CNN Tech Reporter Donie O’Sullivan using his own leaked passwords. After obtaining his contact info, readily available through data brokers, within just 30 seconds she was able to find 13 of O’Sullivan’s plaintext passwords, hashes, and password hints from data breach repository sites. Using a rainbow table and the password cracking tool Hashcat, she cracked Donie’s password hashes to demonstrate how easily attackers use such methods to break into accounts.

Removing employee and executive personal data from data broker sites disrupts this process, making it significantly harder for attackers to find and crack valid credentials. Organizations that prioritize data broker removal are thus much less likely to be targeted with BEC, credential stuffing, and account takeover attempts.

Prioritizing Personal Data Removal for High-Risk Roles

Historically, enterprise cybersecurity teams have focused PII removal efforts solely on executives. The traditional assumption is that executives are the most attractive targets for cyber attackers, and, being the public faces of the company, PII removal also serves to protect them from physical threats. While this protection for executives is crucial, threat actors today are targeting a wide range of employees, from contractors to senior leadership and everyone in between. Limiting the exercise of personal data removal to executives leaves a wide security gap across the remainder of the organization.

Certain roles within an organization are prime targets for cyber threats due to their access to sensitive systems, financial accounts, and critical company data, and should be prioritized for personal data removal.

- ☑ **Executives & Board Members** – Targets for cyber and physical threats due to high-profile status and privileged access to sensitive company data. Their assistants and family members are also at risk.
- ☑ **IT & Security Staff**– Control access to core systems, making them top targets for attackers looking to infiltrate networks or impersonate IT support.
- ☑ **Administrators** – Manage CRM, HR, and financial systems, giving attackers a direct path to sensitive employee and business data.
- ☑ **Engineers & R&D Teams** – Handle proprietary technology and trade secrets, making them targets for industrial espionage and IP theft.
- ☑ **HR & Finance Teams** – Process PII, payroll, and financial transactions, putting them at high risk for fraud and identity-based attacks.
- ☑ **Legal & Compliance Teams** – Manage confidential legal documents, contracts, and regulatory data, making them valuable targets for cybercriminals.
- ☑ **Vendor & Supply Chain Managers** – Serve as a bridge to external partners, making them attractive for supply chain attacks and vendor impersonation schemes.
- ☑ **Long-Term Employees** – Have more exposed personal data online due to years of professional presence, leading to an increased risk for social engineering and credential compromise.

Prioritizing the removal of personal data for these roles significantly reduces an organization's attack surface and enhances overall security. It's important to adapt personal data removal prioritization based on your organization's specific context and structure. Different companies may assign varying risk levels to different roles depending on their operational dynamics. Regularly assess whom to prioritize to ensure that your cybersecurity efforts are effectively focused on protecting the most vulnerable and critical roles within your organization.

Assessing Your Organization’s Exposure

Optery provides free scans to help organizations identify where their employees' personal data is exposed. Businesses can also sign up for a free Optery for Business account and get up to 10 free employee basic accounts to assess your exposure and conduct self-service removals. For automated employee personal data monitoring and removal at scale, visit Optery’s pricing page to instantly calculate the costs based on your needs.

Why Optery is the Industry Leader in Personal Data Removal

Patented search technology

Optery employs award-winning search technology, including patented and proprietary search technologies, enhanced with advanced anti-bot detection, sophisticated AI matching algorithms for discovery, and consistent monitoring through monthly automated searches, making it the most sophisticated data broker scanning software available today. We far surpass Google and competitors in uncovering user profiles, averaging ~100 profiles per user, including ~50 profiles missed by competitors.

> “I tested [Optery] out and it caught nearly 50 more [profiles] than what I had already cleared out with DeleteMe.”
>
> **Devin Coldewey**, TechCrunch Journalist

Unlimited data broker coverage

Our coverage spans 610+ data brokers, plus an unlimited number of additional data brokers via our Custom Removals feature, and we are continuously expanding.

Transparent reporting

Optery is the only personal data removal service that provides detailed before and after exposure and removal reports, complete with screenshots and links to results, to demonstrate the effectiveness of our service. Our Removals Report has no peers in the market and is provided quarterly.

> “Open the report and prepare to be amazed. Optery doesn’t just search on the personal information you supplied. It uses data found in data broker profiles to recursively expand its reach ... Unlike any other product I’ve seen, Optery doesn’t just state that your data was found, like IDX Complete. It also doesn’t simply list the found data items, like DeleteMe. Rather, the report presents you with a screenshot of your actual profile data on the site.”
>
> **Neil Rubenking**, Lead Analyst for Security at PCMag.com

Effective and comprehensive data removal

Optery leverages a sophisticated 'humans + machines' approach to data removal, combining the best of automation with the added precision of manual reviews and handling of edge cases. This is further enhanced by the utilization of Limited Power of Attorney (LPOA) and Authorized Agent Requests, ensuring an effective and comprehensive data removal process from hundreds of sites.

Our strategy surpasses competitors who rely solely on manual methods or outdated technology (which is slow and error-prone), or those depending entirely on automated processes with limited scope (focusing only on the easiest-to-opt-out-of sites).

> “Wiping your digital footprint by yourself really isn’t possible without help. There are just too many data brokers out there. Optery offers the best consumer data deletion service in my opinion, and I research the space closely.”
>
> **Jeff Jockisch**, Data Privacy Expert

Enterprise-grade capabilities

Optery’s enterprise-grade capabilities include SSO/SCIM/SAML integration, SOC 2 Type 2 attestation, and a business administrator dashboard.

We offer transparent, flexible pricing plans tailored to various organizational needs, allowing companies to calculate costs instantly on our pricing page based on their requirements.

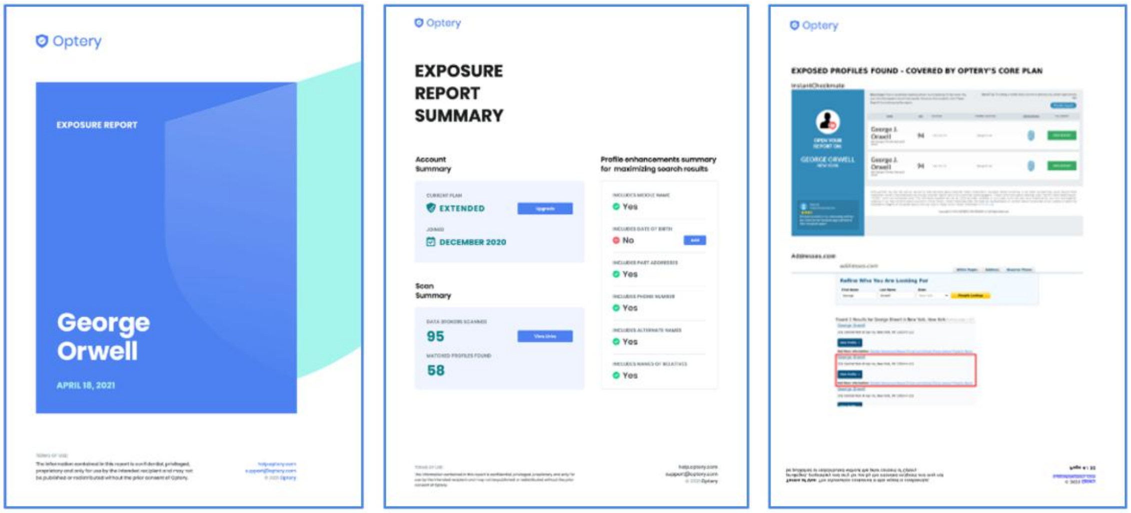
Industry recognition

Optery was awarded "Editors' Choice" by PCMag.com as the most outstanding product in the personal data removal category in 2022, 2023, 2024, and 2025, received Fast Company’s Next Big Things in Tech award for security and privacy in 2023, was named winner in the Employee Privacy Protection, Attack Surface Management, and Digital Footprint Management categories of the 2024 and 2025 Cybersecurity Excellence Awards, and received the Top InfoSec Innovator Award for Attack Surface Management by Cyber Defense Magazine in 2024.

PII Removal Proactively Protects Against Today’s Top Attack Vectors

Personal data removal has become a must-have security measure for organizations. Today’s most successful attack vectors rely on publicly available employee information, and data brokers are a primary source of this data. Organizations that proactively remove exposed employee and executive data from data brokers can significantly reduce their attack surface, prevent targeted phishing and credential-based attacks, and minimize their risk of a breach.

Get started with a free scan today



Optery

EXPOSURE REPORT

George Orwell

APRIL 18, 2021

Optery

EXPOSURE REPORT SUMMARY

Account Summary

CURRENT PLAN
EXTENDED

JOINED
DECEMBER 2020

Scan Summary

DATA BROKERS SCANNED
95

MATCHED PROFILES FOUND
58

Profile enhancements summary for maximizing search results

INCLUDES MIDDLE NAME
Yes

INCLUDES DATE OF BIRTH
No

INCLUDES PAST ADDRESSES
Yes

INCLUDES PHONE NUMBER
Yes

INCLUDES ALTERNATE NAMES
Yes

INCLUDES NAMES OF RELATIVES
Yes

Optery

EXPOSED PROFILES FOUND - COVERED BY OPTERY'S CORE PLAN

InstantCheckmate

GEORGE ORWELL

Addresses.com

Optery

About Optery

Optery is the first company to offer a free report with dozens of screenshots showing where your personal information is being posted by hundreds of data brokers online, and the first to offer IT teams a completely self-service platform for finding and removing employee personal information from the web. Optery subscription plans automatically remove customers from these sites, clearing your home address, phone number, email, and other personal information from the Internet at scale. The service provides users with a proactive defense against escalating PII-based threats such as phishing and other social engineering attacks, ransomware, credential theft, identity fraud, doxxing, and harassment. Optery has completed its AICPA SOC 2, Type II security attestation, and distinguishes itself with unparalleled search technology, data removal automation, visual evidence-based before-and-after reporting, data broker coverage, and API integration options. Optery was awarded “Editors’ Choice” by PCMag.com as the most outstanding product in the personal data removal category in 2022, 2023, 2024, and 2025, was named winner in the Employee Privacy Protection, Attack Surface Management, and Digital Footprint Management categories of the 2024 and 2025 Cybersecurity Excellence Awards, received the Top InfoSec Innovator Award for Attack Surface Management by Cyber Defense Magazine in 2024, and received Fast Company’s Next Big Things in Tech award for security and privacy in 2023. Hundreds of thousands of people and hundreds of businesses use Optery to prevent attacks and keep their personal information off the Internet.