



The Risk to Employees from Exposed Personal Data (PII)

Cybersecurity isn't just about protecting systems, it's about protecting people.

Today, exposed personal information like names, addresses, emails, phone numbers, family ties, past employers, bar numbers, social media handles, is freely available on the open web and data broker sites. This data creates a blueprint for targeting your people in cyber and physical attacks.

The Threat Is Personal

| THREAT TYPE | HOW EXPOSED PII FUELS IT |
|--|--|
| Phishing & Social Engineering | Attackers personalize messages using employee names, roles, org charts, and recent activity to increase click-through and compromise rates. |
| Account Takeovers | Publicly known usernames, breached passwords, and personal identifiers are used to bypass MFA or reset credentials. |
| Business Email Compromise | Scammers impersonate executives or vendors using org-specific context to trick employees into wiring funds or sharing data. |
| Doxing & Harassment | Adversaries weaponize home addresses, phone numbers, and family info to intimidate, shame, or silence targets—especially in media, legal, and public-sector roles. |
| Physical Threats | Personal details found online are used to stalk, confront, or threaten employees at home or in public. |



The Stats Tell the Story

88%

of web app breaches involve stolen credentials
(Verizon DBIR, 2025)

69%

of BEC attacks rely on targeted spear-phishing
(GreatHorn, 2021)

36%

of doxing victims face real-world physical
threats (Statista, 2022)

+ 1 million

identity theft reports filed with the FTC in 2024
alone

*If attackers **can** see your people, they **can** reach your people.*

What Security Leaders Can Do

- ✓ **Scan for Exposed Data** – Proactively identify what PII is available on the open web about high-risk employees.
- ✓ **Remove It at Scale** – Automate opt-outs and removals from data broker sites.
- ✓ **Reduce Social Engineering Risk** – Limit attacker visibility into your workforce hierarchy and personal life details.
- ✓ **Protect Key Roles First** – Focus on execs, public-facing staff, legal/comms, and high-value targets.

DeleteMe helps organizations reduce human-targeted risk by removing employees' personal data from the open web and data broker sites—at scale.

Want to see your organization's risk exposure?

[Schedule a Free Exposure Assessment →](#)

