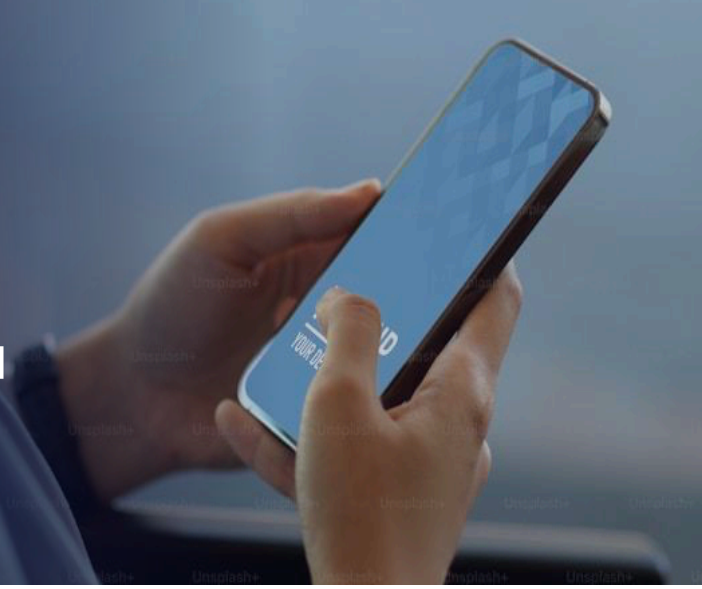
DeleteMe®

Top 5 Threats Powered By Exposed Employee Data



Your employees, from interns to the CEO and board, have their personal information all over the internet and it is creating risk.

The internet hosts an immense amount of personal data, including social media profiles, online purchases, medical records, and financial information. On average, DeleteMe will find and remove over 2300 pieces of this data for each individual over a two year period as new data is captured with every internet, cell phone, and application interaction. This vast accumulation of personal information poses significant risks to organizations such as identity theft, privacy breaches, and targeted cyberattacks.

2,389

Average # of exposed personal info ("PII") found on data brokers over a two year DeleteMe subscription

1. Spear Phishing
2. BEC (Business Email Compromise)
3. Doxing & Harassment
4. Identity Theft & Fraud Against Businesses
5. Privileged User Attacks

2 BEC (Business Email Compromise)

What is Business Email Compromise?

BEC is a type of cybercrime in which attackers impersonate n executive or CEO of a legitimate business. The goal of BEC is typically to trick employees or other business stakeholders into transferring money, providing sensitive information, or authorizing payments to the attackers' accounts.

1

Cybercriminals collect information and create profiles of executives and employee.

2

Using fake emails, messages, and texts, cybercriminals contact employees posing as executives and requesting urgent actions.

3

Employees are tricked and pressured into taking fraudulent or damaging actions

4

The employee unknowing transfers money, pays fictious bills or shares sensitive information with the criminal.

	2023	2022	2021	2020	2019
BEC Losses By Victims	$2,946,830,270	$2,742,354,049	$2,395,953,296	$1,866,642,107	$1,776,549,688
# of Complaints By Victims	21,489	21,832	19,954	19,369	23,775

FBI IC3 Internet Crime Report

BEC caused over $2.9 Billion worth of losses in 2023.

The BEC scam has been reported in all 50 states and 177 countries, with over 140 countries receiving fraudulent transfers. Based on the financial data reported to the IC3 , banks located in Hong Kong and China were the primary international destinations of fraudulent funds.

BEC attacks made up 10.6%, or more than 1 in 10, of social engineering attacks in 2023

BEC attacks grew by more than 50% between H2 2023 and H1 2024.

41% of customers were targeted by VEC attacks every week between January and June 2024.

DeleteMe®

1 Spear Phishing

What is Spear Fishing?

Spear phishing is a method attack that includes collecting significant personal information about the targets that is used to fool targets and defenders into believe the communications are real. Emails are the delivery method of choice with embedded or attached malware of links to malicious websites.

1

Attackers gather personal intel on individuals who are targets at the company

2

Using the intel, a personalized email is crafted to fool the recipient. The email may contain a malicious link or attachment.

3

The target receives the email and opens it, and believing it is real, mistakenly activates the malware.

4

The malware executes, compromising the user account or machine and gives the attacker access to the network

The Damage caused by Spear Phishing Attacks

Spear Phishing attacks can affect a company's finances and reputation and lead to regulatory fines. They can result in data breaches that can cost tens of millions of dollars. Here are some of the most costly incidents confirmed to be caused by spear phishing.

COMPANY	LOSS	TARGET
Anthem Insurance	$100 Million, $16m in fines, 80 million records	IT Administrators and Support Teams
Crelan (Belgium Bank)	Over $70M	Employees Targets
E .ON (UK Energy)	$250K in Fraud	CEO Targeted
UK Mersyrail	Over $10M	CEO email to employees
ARUP Energy	$25M	Employees in Finance Targets
Google/Facebook	Over $100M	Finance Dept

Human Failings

82%

Of data breaches involve human error (Verizon 2024)

68%

Of employees were victims of social engineering or other non-malicious human element (Verizon 2024)

31%

Of successful cyberattacks utilize stolen credentials that all attackers to bypass most existing cyber defenses (Verizon 2024)

3 Doxing & Harassment

What is Doxing?

When someone's personal information is published online including home address, work location, emails, phone numbers, social media accounts and more. In 90% of cases the publishers intent is to harm the person. Doxing can start for many different reasons, here are the most common.

1. Breakup or end of relationship/friendship
2. Data breach or PII date found on the internet
3. Active on discussion boards, chats or online communities
4. Chatting or texting with an unknown user – someone usually targeting you.

Doxing is widespread

Around 4 percent of Americans – an estimated 11 million people – report that they've personally been victims of doxing attacks, while 62% of those individuals personally knew someone who experienced doxing SafeHome.org

6 Common Reasons Why People Dox

- To threaten or blackmail
- For personal publicity
- Out of revenge or anger
- Collective bullying
- To embarrass or bring shame
- Belief in social justice

Doxing Data by the Numbers

Of the types of personally identifying information shared during doxing incidents:

90% Of doxed files included the victim's address

60% Included the victim's cell phone

53% Included the victim's email address

40% Included the victim's IP address

25% Of severe Harassment Takes Place in Doxing Victims

4 Impersonation & Fraud

What is business identity theft?

Identity theft is the act of illegally obtaining and using someone else's personal information, typically for financial gain. Business related identity theft occurs when criminals assume the identities of business owners, officers, employees, partners or customers to fraudulently obtain cash, credit, and loans, leaving the victimized business with the debts.

1

Cybercriminals collect information and create profiles of employees, partner and customer employees

2

Using fake emails, messages, phone calls and texts, cybercriminals contact the company posing as a trusted employee, partner or customer.

3

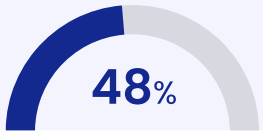
The company is tricked into sharing sensitive data, offering loans or credit and even making false payments.

4

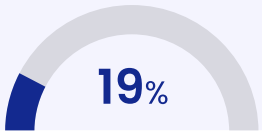
The cybercriminal disappear with the funds, and it often takes companies weeks and even months to discover the loss.

FTC: 5.39 million reports in 2023

Fraud

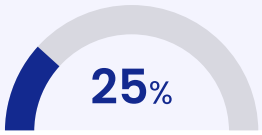


Identity Theft



Credit Card Fraud

Payment, Social Media, Online Shopping fraud



Top Five Types of Identity Theft Affecting Business, 2023

TYPE OF IDENTITY THEFT	NUMBER OF REPORTS	PERCENT OF TOTAL
Credit card fraud-new accounts	381,122	42%
Miscellaneous identity theft (2)	279,221	30,7%
Bank fraud-new accounts	84,335	9,3%
Governament benefits fraud-applied for/received	82,419	9,1%
Loan fraud-business/personal loan	81,342	9%
Total	**908,439**	**100%**

(1) Consumers can report multiple types of identity theft. In 2023, 15 percent of identity theft reports included more than one type of identity theft.
(2) Includes online shopping and payment account fraud, email and social media fraud, and medical services, insurance and securities account fraud, and other identity theft.
Source: Federal Trade Commission, Consumer Sentinel Network.

5 Privileged User Attacks

What are Privileged user attacks?

Certain people in an organization have the critical access (privileged users) needed to enable cybercriminals to easily bypass and organizations cyber defenses. These include IT staff, software developers and even help desk staff. We have broken out this attack vector from Spear phishing because it has played a critical role in recent compromises.

1

Cybercriminals collect information and create profiles critical staff with privilege network or IT system access

2

Using social engineering-based attacks via email, text and phone, they begin communicating with the target

3

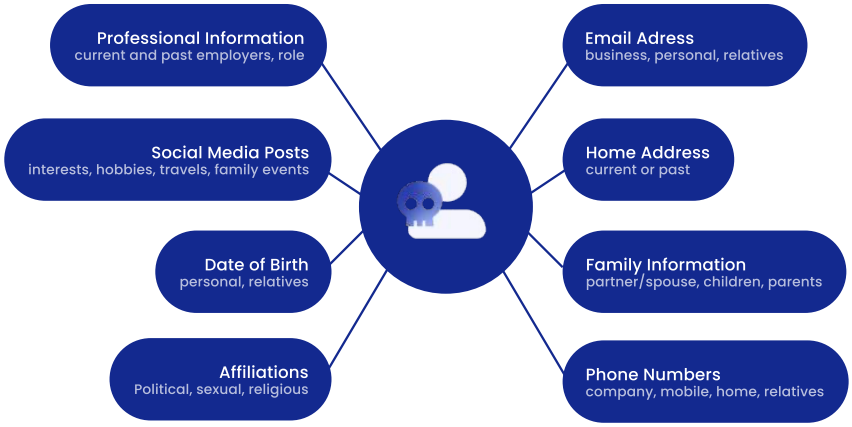
The target employee mistakenly clicks on or shares information with the cybercriminal that allows them to compromise systems

4

With the literal keys to the kingdom, attackers bypass existing defenses and access sensitive information to implement fraud, ransomware or supply chain attacks

Bypassing millions of dollars of defenses in seconds

The average Fortune 500 company spends about $1.6 million on cybersecurity each Year. They employ about 30K IT staff each and average another 14K in software engineering. Each one of those privileged users have hundreds of pieces of PII data easily available on the internet and cybercriminals know just how to find and use it.



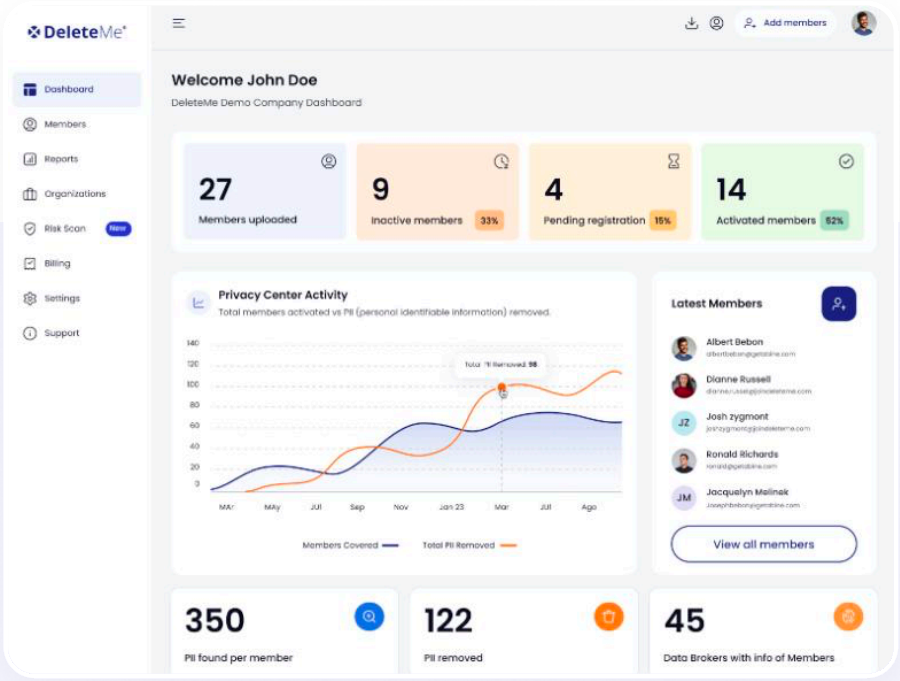
ORGANIZATION	TARGETED EMPLOYEE	COST
RSA	IT Staff, ID Sys Engineers	$66.3M + (China used to steal military tech)
Sony Pictures	Privileges Admins	$ 171M
Robin Hood Trading	Customer Support Staff	$ 20M
Rock Star Games	IT Staff (slack)	$ 6M+
Circle CI	IT Admin/Auth Sys	$ 300K

DeleteMe Quickly Identifies & Continuously Removes Workforce Personal Information

DeleteMe reduces the risk of employee and executive personal data exposure by finding, removing, and monitoring employee personal information from numerous online and offline sources. DeleteMe is a proven privacy service with unparalleled quality and flexibility that combines a unique blend of privacy advisors, process automation, and advanced scanning/matching technology.

- Ongoing scanning and proactive removal of exposed employees' personal information
- Regular reporting that shows exposed data and removal status for each employee
- Dedicated privacy advisors to work with employees and executives
- Dedicated customer expertise and program rollout support that ensures success

Trusted by 20% of the Fortune 500 and dozens of federal and state agencies, DeleteMe delivers a highly effective, continuous service that proactively removes personal information across hundreds of websites, providing a robust shield against potential threats.



A Human Centric Approach to Privacy Protection and Cybersecurity

1. **Employees, Executives, and Board Members Complete a Quick Sign-Up**
2. **DeleteMe Scans for Exposed Information**
3. **Opt-Out and Removal Requests Begin**
4. **Initial Privacy Report Shared and Ongoing Reporting Initiated**
5. **DeleteMe Provides Continuous Privacy Protection and Service All Year**