Ensuring Privacy and Security in the Digital Age

Data privacy is no longer a luxury; it is a necessity. With the exponential growth of our digital footprints and the lack of uniform privacy protection, businesses must protect their employees' and customers personal information or face the daunting threat of successful spear phishing, identity theft, fraud, doxing, harassment, and even threats of physical attacks, the results of which can have devastating consequences for individuals and organizations.

The Current Landscape of Data Privacy

In today's digital age, personal information is easily accessible online. A multitude of entities , including governments, financial institutions, retail companies, healthcare providers and insurance companies, social media, technology and communications companies, and data brokers, collect and sell personal data, offering easy access to cybercriminals. Organizations must take proactive measures to protect their employees' privacy and mitigate the risk of cyber-attacks.

Challenges Faced by Businesses

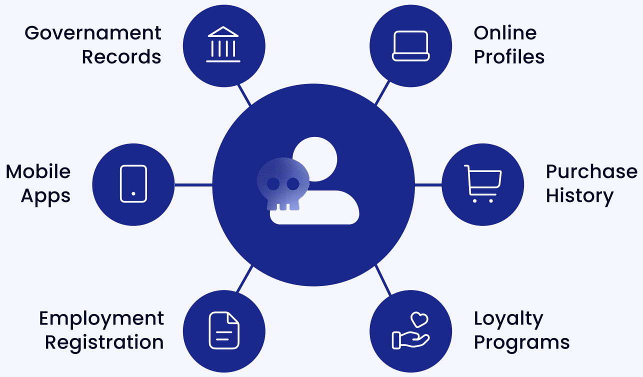
- Spear Phishing: Tailored phishing attacks exploit personal data to deceive employees, suppliers, and customers, leading to security breaches.
- Theft and Fraud: Employee and consumer identity impersonation or theft is used to trick and deceive an organization into money transfers that can cost hundreds of thousands of dollars.
- Harassment and Abuse: From board room to the data that is gathered from the Internet and used to harass, threaten, and even physically attack individuals.

Your Executives and Manager are Prime Targets

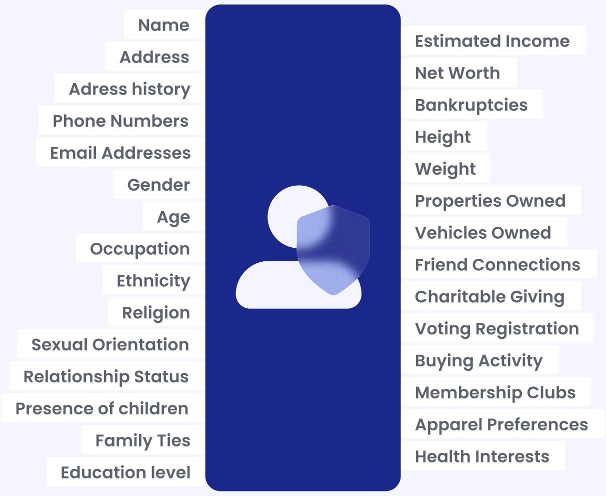
Executives and managers are prime targets for attacks, including cyber-attacks, fraud, impersonation, intimidation, and harassment. Their access to sensitive information, influence within the organization, and significant public presence make them a primary target. Protecting their personal data is crucial to safeguarding the company's overall security.

Examples of cybercriminals impersonating an individual close to the executive (friend, family, coworker, boss) to commit fraud or identity theft are all too common. The C-suite is more at risk from social engineering and targeted phishing attacks because threat actors can use stolen confidential data to make their communications more convincing.

How PII is captured



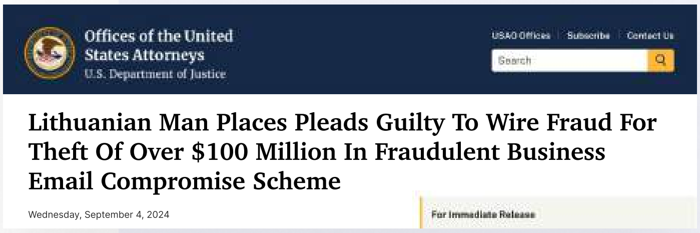
What type of data are collected



Headlines social attacks

Business Email Compromise (BEC) is another type of social engineering attack that executives and managers must be cautious of. While spear or whale phishing targets high-level executives, BEC attacks involve impersonating them. In these attacks, lower-level employees might receive a fake or spoofed email that appears to be from an executive. According to IC3 research, BEC attacks have caused more financial damage from cybercrime than ransomware.

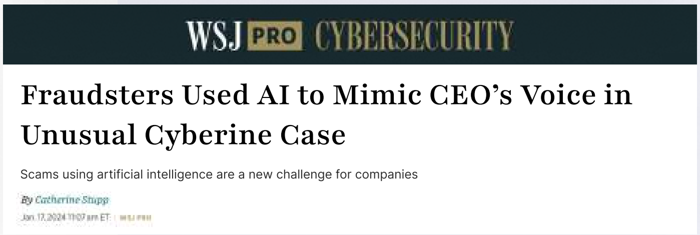
In 2023, BEC resulted in $2.9 billion in losses for victims. Doxing, the malicious practice of publicly revealing private or identifying information about an individual, poses significant risks to executive and employee personal safety and privacy. Doxing can lead to harassment, threats, identity theft, financial fraud, and severe emotional distress.


Offices of the United States Attorneys
U.S. Department of Justice
USAO Offices
Subscribe
Contact Us
Search

Lithuanian Man Places Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme

Wednesday, September 4, 2024

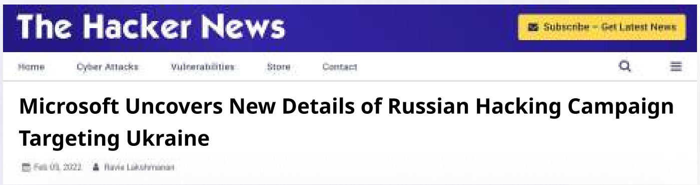
For Immediate Release



Fraudsters Used AI to Mimic CEO's Voice in Unusual Cyberine Case

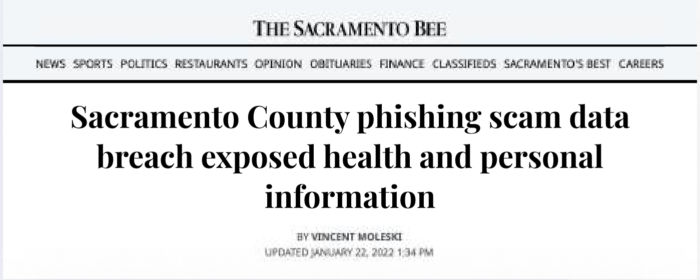
Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp
Jan 17, 2024 11:07 am ET | WSJ PRO



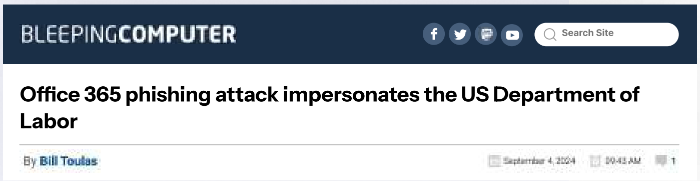
Microsoft Uncovers New Details of Russian Hacking Campaign Targeting Ukraine

Feb 03, 2022 · Ravie Lakshmanan


THE SACRAMENTO BEE
NEWS SPORTS POLITICS RESTAURANTS OPINION OBITUARIES FINANCE CLASSIFIEDS SACRAMENTO'S BEST CAREERS

Sacramento County phishing scam data breach exposed health and personal information

BY VINCENT MOLESKI
UPDATED JANUARY 22, 2022 1:34 PM



Office 365 phishing attack impersonates the US Department of Labor

By Bill Toulas · September 4, 2024 · 09:43 AM · 1

From IT to Admins, Threat Actors Moving Beyond Executives

Threat actors understand that IT admins, engineers, QA and design teams, customer service and help desk staff, executive admins, and other critical personnel with access to sensitive data are primary targets for social engineering and cyber attacks. Publicly available data gives threat actors the upper hand in deceiving security awareness-trained employees, and the greater access created by compromising a high-value employee increases the likelihood of defeating cyber defenses. Attacking help desk staff to bypass MFA and other defenses has grown exponentially in 2024, with the American Hospital Association warning its members in January of 2024 (1), a dire security alert from the US Department of Health in April (2), and a Mandiant special report released in June (3).

"Mandiant has observed UNC3944 in multiple engagements leveraging social engineering techniques against corporate help desks to gain initial access to existing privileged accounts. Additionally, it has been noted that they already possessed the personally identifiable information (PII) of its victims to bypass help desk administrators' user identity verification."

Bottomline

Organizations can no longer rely on MFA and security awareness training. The significant amount of employee data easily accessed on the open Web gives attackers the upper hand over existing defenses using social engineering.

Organizations must proactively remove employee PII from the Internet to effectively defend executives, employees, suppliers, customers, and sensitive company data.

(1). https://www.aha.org/news/headline/2024-01-12-hospital-it-help-desks-targeted-sophisticated-social-engineering-schemes
(2) https://www.hhs.gov/sites/default/files/help-desk-social-engineering-sector-alert-tlpclear.pdf
(3) https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications

DeleteMe®

DeleteMe Protects Privacy and Enhances Cyber Defenses

DeleteMe provides a comprehensive solution to ensure employees' and executives' privacy, reducing the risk of spear-phishing attacks, identity theft, and other threats.

DeleteMe proactively and continuously removes personal information from data brokers, search engines, and online sources, reducing employee's digital footprint and the risk of cyberattack, fraud, and harassment. With DeleteMe, you achieve:

- Comprehensive Data Removal: DeleteMe identifies and removes personal information from hundreds of web and data broker sites.
- Regular Monitoring: Continuous monitoring ensures that new data entries are detected and removed promptly.
- Detailed Reporting: Clients receive regular reports detailing the information removed and the current status of their data privacy.

Proactive Protection: DeleteMe eliminates personal information from the Web, reducing the risk of spear-phishing attacks and identity theft.

How DeleteMe Works

1 Employees, Executives, and Board Members complete DeleteMe's identification sign-up process.

2 DeleteMe AI searches the Internet for any exposed employee PII.

3 DeleteMe Data Privacy Experts utilize a mix of automated and manual opt-out processes to ensure that all data is removed.

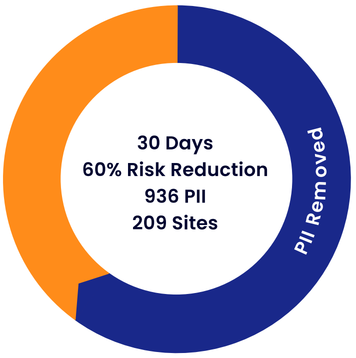
4 The opt-out process continues as DeleteMe Data Privacy Experts recheck and verify that PII is removed.

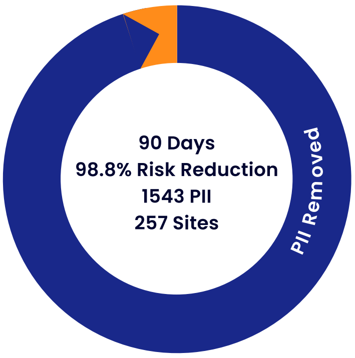
5 Monthly privacy reports are shared with staff and employees to show the status of their online PII data removal.

6 Because employees do not stop interacting with technology, their data is constantly being collected, so DeleteMe provides continuous privacy protection.

DeleteMe customers reduce the amount of employee PII data found on the Internet by 60% in just 30 days; by 90 days, that number exceeds 98%. Customers report significant value across multiple security categories, including:

- Enhanced cybersecurity: Reducing successful targeted cyber-attacks by removing employee PII used by Spear Phishing Attackers.
- ncreased protection for executives and customer-facing employees: Removing executives, board members, and customer-facing employees' PII from the Internet reduced incidents of doxing and harassment across the organization.
- Increase employee trust: Utilizing DeleteMe to protect employees and, for many of our customers, their families has fostered increased trust and loyalty within the organization.





DeleteMe's Commitment to our Customer's Privacy and Security

DeleteMe is trusted by over 30% of the Fortune 500 and multiple Federal, State and Local Government Agencies, and it is not just because of DeleteMe's superior continuous PII removal service. These organizations recognize that as a critical partner, DeleteMe also meets their stringent third-party risk standards.

DeleteMe maintains AICPA SOC 2 Type 2 certifications and conducts regular third-party audits to ensure compliance. DeleteMe also adheres to GDPR privacy standards. All PII (Personally Identifiable Information) maintained by DeleteMe is encrypted both in transit and at rest using 256-bit AES and TLS 1.2 encryption. We employ Multi-Factor Authentication (MFA) and role-based access control. Our Security Operations Center operates 24 hours a day, continuously monitoring for threats. We utilize the same strict third-party risk management practices that our Fortune 500 customers do.

We follow a secure software development life cycle (SDLC) to ensure that security is built into every stage of the development process.

We conduct regular code reviews, vulnerability assessments, and penetration testing to identify and address potential weaknesses. We provide regular cybersecurity training to update our employees on the latest threats, best practices, and security policies.

Additionally, we implement regular phishing simulations to improve employees' ability to recognize and respond to social engineering attacks. We have a robust data backup and disaster recovery strategy to ensure business continuity during data loss or system failure. Furthermore, we guarantee never sell or share any PII with third parties.

Finally, the DeleteMe privacy service requires no on-premise footprint, hardware, or software. Our 100% cloud-native service is operated, managed and upgraded by our world-class software team. With DeleteMe, overloaded IT teams will not struggle with another tool but reap the benefits of a proactive risk reduction service that operates beyond their traditional cybersecurity boundary.

AICPA SOC aicpa.org/soc

SOC 2 TYPE II CERTIFIED

GDPR COMPLIANT

Conclusion

In an era where data privacy is paramount, DeleteMe stands as a critical ally for businesses aiming to protect their most valuable assets: their employees, executives, and sensitive data. The digital landscape, rife with threats such as spear phishing, identity theft, and harassment, necessitates proactive and robust measures. DeleteMe's comprehensive solution addresses these challenges head-on by removing personal information from data brokers, search engines, and other online sources, significantly reducing the digital footprint of employees and executives.

DeleteMe's commitment to privacy and security is underscored by its adherence to rigorous standards and certifications, ensuring that client data is handled with the utmost care and security.

Trusted by a significant portion of the Fortune 500 and various government agencies, DeleteMe's cloud-native service integrates seamlessly, providing essential protection without adding to the burden of IT teams.

As businesses navigate the complexities of the digital age, the importance of safeguarding personal information cannot be overstated. DeleteMe offers a proactive, reliable, and efficient solution, enabling organizations to stay ahead of cyber threats and maintain the privacy and security of their most important resources. In choosing DeleteMe, businesses take a decisive step towards a safer, more secure digital future.