Optery

PII Removal for Executives is Not Enough

Protecting a Broader Range of Employees is Essential

Table of contents

Introduction: Closing the security gap

Historically, enterprise cybersecurity teams have prioritized removing personally identifiable information (PII) from the internet only for 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.

The prevalence of mass SMS-phishing (smishing) campaigns and other social engineering attacks targeting non-executive staff demonstrates the necessity of personal data removal for a broader range of employees. Such attacks rely on and exploit access to employee PII and have consistently been a top source of organizational breaches in recent years. This reality underscores a critical vulnerability: the PII of non-executive employees, often less guarded but equally valuable, is readily accessible and exploitable, and needs to be protected.

This white paper highlights recent data demonstrating this reality and advocates for a broader use of personal data removal software within organizations to more effectively protect against today's cybersecurity threats.

Summary of key points

- **For breaches where the attack vector is social engineering, non-executive employees are often the primary targets.**
- **Non-executive employees are targeted more than executives.**
- **PII is exploited for social engineering attacks against a variety of employee roles and departments.**
- **Effective PII removal is a critical proactive defense against social engineering and other PII-based threats.**
- **PII removal efforts must include a broad range of employees to close existing security gaps.**
- **No company is immune from successful attacks. The companies profiled have large and sophisticated cybersecurity teams, but were still breached.**

Non-executives are most often targeted

While executives remain high-value targets for cyber attackers, a recent report from Avanan research indicates that it is actually non-executives who are more often targeted. According to Avanan's report, 51.9% of all impersonation emails attempt to impersonate non-executive employees, and non-executives are targeted 77% more often than their executive counterparts. Two factors contribute to this trend. Firstly, security teams tend to focus their efforts on the C-Suite, leaving non-executives relatively vulnerable, and hackers have taken notice. Secondly, non-executives frequently hold sensitive information and financial data. When a non-executive can provide an attacker with the information they want, there is no need to go all the way to the top, especially if targeting senior leadership is more challenging. [1]

Recent breach cases of non-executives targeted

A number of breaches over the past several years illustrate the fact that cyber attackers successfully target non-executive employees across various roles. Contractors, engineers, IT staff, finance personnel, help desk personnel, HR staff, and generally any employees with credentials are in bad actors' crosshairs. Attackers are regularly leveraging the exposed data of these non-executives for social engineering, credential harvesting, and initial access. The following table provides a concise summary of some of these cases. This overview is followed by more detailed narratives of each incident.

Summary table of breach cases

Date	Type of Attack	Employee Group Targeted	Details/Impact
September 2022	Social Engineering	Contractor	Uber hack: Attacker obtained contractor's credentials, bombarded with MFA requests, posed as IT support on WhatsApp, and gained access to internal systems.
January 2023	Social Engineering	Employees & Contractors	Mailchimp breach: Unauthorized access to customer support tool via compromised credentials. 133 customer accounts breached.

[1] https://www.avanan.com/blog/how-impersonation-attacks-fool-users

Summary table of breach cases (cont.)

Date	Type of Attack	Employee Group Targeted	Details/Impact
February 2023	SMS Phishing	Engineers	Coinbase attack: Fraudulent SMS alerts led an engineer to enter credentials, resulting in exposure of employee contact information. Threat actor likely connected to 0ktapus campaign.
August 2023	SMS Phishing & Deepfake	IT Staff	Retool breach: Attackers used SMS phishing and voice deepfakes to compromise IT employee's Okta account, accessing 27 customer accounts.
February 2024	Phishing & Deepfake	Finance Personnel	Multinational corporation: Finance clerk deceived by deepfake technology impersonating CFO, resulting in $25 million transferred to attackers' accounts.
September 2023	Voice Phishing	Help Desk Personnel	MGM Resorts breach: Attackers used voice phishing to impersonate an employee and gain access to MGM's network. They encrypted over 100 ESXi servers, leading to a $100 million loss and the theft of customer data.
December 2022	SMS Phishing	HR Staff	Activision breach: SMS phishing attack exposed sensitive employee information and plans for future Call of Duty releases.
Throughout 2022	SMS Phishing	Broad Employee Targeting	0ktapus campaign: Targeted around 130 organizations, directing employees to fake login pages to harvest credentials. Compromised nearly 10,000 credentials.
September 2023	Social Engineering	IT Service Desk Personnel	Attackers used 0ktapus phishing kit and sought to trick targets into resetting MFA factors for highly privileged users.

Specific breach breakdowns

Contractors

One of the most notable breaches in recent times was the September 2022 Uber hack, which occurred after a contractor's credentials were obtained via a social engineering attack. The attacker used the contractor's credentials to attempt a login, triggering a Multi-Factor Authentication (MFA) request. The attacker then bombarded the contractor with repeated MFA push notifications. After an hour, the attacker posed as Uber IT support on WhatsApp and convinced the contractor to accept the MFA request. The attacker then gained access to Uber's internal systems. The result was a very high-profile breach. [2]

In another example, on January 11, 2023, the security team of the marketing automation platform Mailchimp discovered that an unauthorized actor had accessed a tool used by customer support and account administration teams. This breach resulted from a social engineering attack on Mailchimp employees and contractors, allowing access to specific accounts via compromised credentials. As a result, 133 customer accounts were breached, leaving them at risk of further attacks. MailChimp was also breached twice in 2022 under similar circumstances.[3]

Engineers

Engineers, particularly those with access to sensitive systems, are prime targets for social engineering attacks. A recent example occurred on February 5, 2023, where attackers targeted several engineers of the cryptocurrency exchange platform Coinbase with fraudulent SMS alerts, urging them to log into their company accounts. While most employees ignored the messages, one engineer was deceived by the phishing link and entered his credentials. The attacker then impersonated an IT staff member, directing the engineer to follow further instructions. The incident resulted in exposure of some employees' contact information, data that could be leveraged in future attacks against the company. Coinbase believes the threat actor responsible is the same one involved in the 0ktapus campaign of 2022 that targeted over 130 organizations using a similar modus operandi (see further below). [4]

[2] https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
[3] https://mailchimp.com/newsroom/january-2023-security-incident/; https://www.digitalocean.com/blog/digitalocean-response to-mailchimp-security-incident; https://mailchimp.com/newsroom/august-2022-security-incident/; https://mailchimp.com/newsroom/march-2022-security-incident/
[4] https://www.bleepingcomputer.com/news/security/coinbase-cyberattack-targeted-employees-with-fake-sms-alert/

IT staff

IT staff are frequently targeted and impersonated on account of their access to sensitive information and critical systems. In one recent example, on August 27, 2023, the software provider Retool experienced a sophisticated attack where the attackers used SMS phishing and voice deepfakes to compromise an IT employee's Okta account. The attackers sent a phishing message that led to a fake login portal, which captured the employee's credentials. They then impersonated company personnel and called the targeted employee, using a deepfake voice to obtain an additional MFA code. This allowed the attackers to add their device to the employee's Okta account and access Retool's systems. As a result, the attackers took over accounts belonging to 27 of Retool's cloud customers. [5]

Finance personnel

Finance personnel are attractive targets for attackers due to their access to company funds and financial information. In February of 2024, an attack was reported in which a finance clerk at a large multinational corporation in Hong Kong fell victim to a sophisticated scam involving deepfake technology. The scam began with a phishing message that appeared to be from the company's chief financial officer, requesting an urgent confidential transaction. To authenticate the ruse, the attacker used deepfakes to impersonate the CFO and other senior executives in a video call. The convincing deepfakes eased the clerk's doubts, leading to over $25 million being transferred to the attacker. While executives were impersonated in the attack, they were not the primary target. This incident underscores the lengths to which cyber attackers will go to exploit non-executive employees and the advanced techniques they use to bypass security measures.[6]

Help desk personnel

Help desk personnel, who manage access controls and assist with IT issues, are critical yet vulnerable points within an organization. On September 11, 2023, MGM Resorts experienced a breach where attackers used voice phishing to impersonate an employee and target the help desk. This tactic allowed them to gain access to MGM's systems. The attackers, linked to the BlackCat/ALPHV ransomware group known as Scattered Spider, infiltrated the network and encrypted over 100 ESXi servers, significantly disrupting MGM's operations and leading to a $100 million loss. The breach also led to the theft of customer data, including names, addresses, and social security numbers, which could be used in future attacks and for identity theft.[7]

[5] https://www.bleepingcomputer.com/news/security/retool-blames-breach-on-google-authenticator-mfa-cloud-sync-feature/
[6] https://www.secureworld.io/industry-news/hong-kong-deepfake-cybercrime; https://news.rthk.hk/rthk/en/component/k2/1739119-20240204.htm
[7] https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/; https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft/

HR staff

Human resources staff handle vast amounts of personal and sensitive information, making them prime targets for cyberattacks. One recent example occurred on December 4, 2022, in which hackers targeted video game publisher Activision by executing an SMS phishing attack to gain access to an HR employee's computer. This breach exposed sensitive employee information, including full names, corporate emails, phone numbers, and other personal details that could be leveraged in future attacks. Additionally, the attackers accessed confidential plans for future Call of Duty releases. This incident highlights the importance of protecting HR personnel from social engineering attacks to safeguard sensitive organizational information.[8]

Employees targeted broadly

One of the most infamous attacks in recent years was the 0ktapus campaign that occurred in 2022 and targeted around 130 organizations. The threat group responsible, known as Scatter Swine, sent SMS phishing messages to multiple employees across these organizations, directing them to fake login pages to harvest credentials. The compromised credentials were then used to access corporate networks and systems.

Group-IB dubbed this campaign "0ktapus" because the attackers targeted employees of companies that are customers of IAM leader Okta. The campaign involved a phishing kit that included 169 unique domains mimicking Okta login pages, sharing common elements such as images and scripts to appear authentic. This widespread phishing campaign primarily targeted organizations in the United States and Canada and landed the attackers nearly 10,000 credentials. [9]

Multiple threat actors leveraging 0ktapus phishing kit

In September of 2023, Okta reported a consistent pattern of social engineering attacks on IT service desk personnel. The attackers' strategy was to trick them into resetting multi-factor authentication (MFA) factors for highly privileged users. The attackers used the 0ktapus phishing kit, which included templates for realistic fake authentication portals to collect credentials and MFA codes. This kit also used Telegram for command-and-control operations. Multiple threat actors are now using this phishing kit, underscoring the necessity of personal data removal for a much broader range of employees beyond executives.[10]

[8] https://insider-gaming.com/activision-data-breach/
[9] https://techcrunch.com/2022/08/25/twilio-hackers-group-ib/; https://www.group-ib.com/blog/0ktapus/; https://www.secureworld.io/industry-news/0ktapus-phishing-campaign
[10] https://thehackernews.com/2023/09/okta-warns-of-social-engineering.html?m=1

Threat actors and social engineering

Several prominent threat groups employ similar social engineering tactics to target a broad range of employees. The following are some of the key actors and their known tactics.

Scatter Swine: A threat actor referred to by Okta as 'Scatter Swine' is known for delivering phishing lures in bulk to individuals in targeted organizations via text messages, such as occurred in the 0ktapus campaign. The actor often leverages commercially available data aggregation services to harvest mobile phone numbers linked to employees, underscoring the need for organizations to implement comprehensive personal data removal. Scatter Swine's approach allows them to cast a wide net and increase the likelihood of compromising multiple employees across different levels within an organization.[11]

UNC3944: A threat actor tracked by Mandiant, designated as UNC3944, uses consistent social engineering tactics, often calling service desks to claim they are receiving a new phone, which warrants a multi-factor authentication (MFA) reset. They are also known for extensive SMS phishing campaigns. By targeting service desks and leveraging phishing, UNC3944 can reset passwords for privileged accounts and bypass associated MFA protections. This actor conducts extensive reconnaissance on their targets and uses PII to bypass security protocols, conduct MFA reset scams, and threaten victims and their families. Minimizing exposed employee PII is an essential step in protecting against this threat actor.[12]

Octo Tempest: A threat actor tracked by Microsoft and designated as 'Octo Tempest' commonly launches social engineering attacks targeting technical administrators, such as support and help desk personnel. Their tactics include SMS phishing, SIM swapping, and advanced social engineering techniques. Octo Tempest conducts extensive research on the organization to pinpoint specific targets for effective impersonation, adeptly mimicking the victim's speech patterns during phone calls and leveraging PII. This knowledge enables them to deceive technical administrators into resetting passwords and MFA methods. Proactive personal data removal is critical for disrupting this threat actor's reconnaissance and attack techniques.[13]

Carbon Spider/FIN7: One of the oldest and continually operating threat actors, known as Carbon Spider or FIN7, has transitioned from targeting companies with POS devices to broader operations using phishing attachments and links to deliver malware to a large number of victims across various sectors. This adaptability highlights the group's broadening scope and targets. For instance, on April 14, 2020, they likely compromised a legitimate email distribution service to conduct a spam campaign targeting thousands of recipients across numerous verticals.[14]

[11] https://sec.okta.com/scatterswine
[12] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications/; https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/
[13] https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
[14] https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

Threat actors and social engineering (cont.)

Since this campaign, Carbon Spider has been casting a wide net, using deceptive emails with harmful attachments and links to spread various types of malicious software. This includes software that can secretly gather information from a computer, like taking screenshots, recording browsing history, and more. Organizations with large amounts of exposed employee data are vulnerable to the kind of broad targeting employed by this threat actor.

Scattered Spider: An adversary tracked by CrowdStrike, tentatively identified as Scattered Spider (mentioned above in connection with the MGM breach), typically targets non-executive employees within telecommunications and business process outsourcing (BPO) companies. The group employs social engineering techniques, such as phone calls, SMS, and Telegram messages, to impersonate IT staff and gain initial access. They often direct victims to credential-harvesting sites or instruct them to run remote monitoring and management (RMM) tools. The attackers' focus on broad employee groups highlights the need for more comprehensive personal data removal across all organizational levels.[15]

The need for personal data removal beyond executives

Today's enterprise attack surfaces have expanded beyond traditional boundaries, now including personal information exposed by data brokers online. In the current cyber threat landscape, personal data removal as a threat mitigation tactic should move beyond just protecting executives.

According to the MITRE ATT&CK framework, the pre-attack phase of a cyberattack involves adversaries conducting reconnaissance to gather information about their targets. This includes organizational details and information about employees at all levels in the organization. The latter, as seen above, is frequently exploited for social engineering, credential theft, and initial access.

Personal data removal is an essential proactive and preventative security measure that complements other measures such as employee education, applying the principle of least privilege, using MFA and FIDO2 compliant tokens, and employing robust incident response strategies.

[15] https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Prioritizing personal data removal for high-risk roles

To implement a successful personal data removal strategy, organizations must first identify and prioritize the most vulnerable roles.

Certain roles within an organization are more attractive to attackers due to their access to sensitive information and systems. The following high-risk roles should be prioritized for personal data removal.

- The executive leadership team and board members are high-value targets due to their privileged access to financial accounts, core information systems, sensitive company IP, trade secrets, and strategic decision-making processes. Their high-profile positions make them prime targets for cyber espionage and social engineering. Similarly, the executive support team, including personal assistants and other support staff, are vulnerable because they have access to executives' communications and systems. Even family members of executive leaders can be at risk, as threat actors may exploit these personal connections to gain access to sensitive information.
- IT and Operational Technology (OT) staff are prime targets based on their privileged access to sensitive systems and data. These employees play a critical role in maintaining and securing IT infrastructure, making them attractive to attackers who aim to compromise these systems. Additionally, IT support staff, who manage access controls and assist with IT issues, are high-risk due to their extensive system access and susceptibility to impersonation.
- Administrator roles, including those managing key systems such as CRM, HR, and financial systems, are particularly attractive targets. Their administrative privileges make them valuable for attackers seeking to gain access to critical systems and sensitive data.
- Engineers and research and development (R&D) personnel are at heightened risk due to their access to company IP, production systems, and trade secrets. These individuals are often targeted for industrial espionage and cyberattacks aimed at stealing valuable intellectual property.
- Human resources staff handle vast amounts of sensitive personal data, including PII, payroll information, and employment records. This makes them prime targets for cyberattacks aimed at accessing confidential employee information. Protecting HR personnel from social engineering attacks is crucial for safeguarding this sensitive data.
- Finance personnel are attractive targets for attackers due to their access to payment systems, financial accounts, and sensitive financial data. Their personal data is particularly valuable to cybercriminals looking to conduct financial fraud.

Prioritizing personal data removal for high-risk roles (cont.)

- Employees managing third-party vendor relationships are at high risk due to their access to external partners who may have sensitive data. Supply chain attacks often target these individuals to exploit vulnerabilities in vendor management processes.
- Legal personnel handle sensitive legal documents and communications, often containing confidential and proprietary information. Their access to this information makes them high-value targets for cyber espionage and social engineering.

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.

PII removal beyond executives

Extending personal data removal beyond executives ensures organizations are more difficult targets for attackers. By implementing personal data removal for a broader range of employees, organizations can significantly improve their security posture against today's sophisticated cyberattacks and reduce the risk of devastating breaches.

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, credential theft, identity theft, doxing, and harassment. Optery has completed its AICPA SOC 2, Type II security certification, 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, and 2024, received Fast Company's Next Big Things in Tech award for security and privacy in 2023, and named winner in the Employee Privacy Protection, Attack Surface Management, and Digital Footprint Management categories of the 2024 Cybersecurity Excellence Awards. Tens of thousands of customers rely on Optery to prevent attacks and keep their personal information off the Internet.