Hacking humans:
How to defend against your biggest cyber risk

Attackers are bypassing traditional cyber defenses by impersonating employees. Why help desks have become the target, and how agencies can reduce the growing risks.

By Scoop News Group

A tech support specialist at a public healthcare institution answered what sounded like a routine call: An oncologist, identifying himself as a staff member, explained he had purchased a new smartphone and needed to reset his credentials to access his accounts. The tech specialist asked a few standard identity challenge questions, but despite how easily the oncologist responded with the correct answers, something didn't feel right.

"By the way, where are you calling from?" he asked the doctor. "Well, at the moment, I'm in the ER," the oncologist replied. "I can give you the phone number if you like."

To a less-savvy help desk specialist, that response might have seemed credible. That's how convincing threat actors have become in impersonating employees and how capable they are at extracting personally identifiable information about their targets from the internet.

The tip-off in this case? The specialist knew that oncologists don't typically work in the emergency room and discerned this was a brazen breach attempt. Fortunately, it failed.

"Not all help desk individuals have that sixth sense or have the level of training needed to thwart attacks the way this individual did," says Ryan Witt, vice president of industry solutions at Proofpoint, which specializes in enterprise email risk and cyberthreat protection. "Nor do they have the level of technology and authentication capability built into their infrastructure right now to stop these types of attacks at scale."

And threat actors know it.

The Help Desk: High-Value Target Under Siege

For government agencies, institutions and enterprises at large, it's essential to recognize that the battle to protect enterprise resources has shifted, and why focusing on human behavior has become critical to cybersecurity operations.

Technical defenses like firewalls, continuous monitoring and remediation and AI-assisted analytics remain essential tools in that battle. However, malicious actors have found a way around those defenses, using deception and impersonation to prey upon unwitting individuals within organizations and tricking them into sharing their credentials.

The latest figures from Verizon's 2025 Data Breach Investigation Report bear that out. It found that of the 12,195 data breaches the DBIR unit investigated last year, 60% involved human interaction. Credential abuse and social actions, like phishing, were cited as leading factors. That compares to the exploitation of system vulnerabilities, which grew significantly last year but still only accounted for 20% of breaches.

People Struggle with Targeted Email Attacks

Email remains the #1 threat vector to target organizations. What makes cyber-attacks like business email compromise (BEC), credential phishing, ransomware and account takeover so successful is how effectively they target your users using a personalized approach. Email security built into productivity suites isn't stopping enough of these threats from reaching users. Stronger email protection is critical.

96% of users who take risky behavior are aware of the potential dangers

94% of human-targeted attacks are initiated via email

$ 4.8M average cost of Phising and BEC incidents

Source: Proofpoint threat research

What's changing, says Pablo Passera, vice president of product management and a security expert with Proofpoint, is the growing assault on help desks. Threat actors recognize that service desk agents, tasked with assisting employees and managing access, hold the keys to the kingdom.

"A service desk agent can change a password, reset credentials, manage multi-factor authentication (MFA) devices and troubleshoot access issues," says Passera. A successful impersonation doesn't just compromise one user; it provides the attacker with the legitimate tools to escalate privileges, move laterally, access sensitive data like payroll accounts or deploy ransomware, he adds. "So, the service desk is a very valuable target for threat actors right now."

Passera notes that attackers are also using the help desk to trick employees. He described a growing tactic called mail bombing, where an attacker identifies an employee within an organization and subscribes their email address

> "Not all help desk individuals…have the level of training… or technology and authentication capability built into their infrastructure right now to stop these types of attacks at scale."
>
> – Ryan Witt, vice president of industry solutions, Proofpoint

to thousands of newsletters. "Imagine your inbox suddenly has 1,000 welcome emails and then someone impersonating a help desk agent contacts you, saying, 'Hey, Paul, I'm from the service desk, and we noticed you're under attack. Click on this link so we can help resolve the issue.' The employee clicks the link, and suddenly they're compromised."

The Crumbling Wall of Traditional Verification

"One of the biggest challenges for service desk agents," notes Passera, "is being able to identify if someone is impersonating an employee or is the real employee."

For years, organizations relied on verifying identities by asking for Personally Identifiable Information (PII) – the last four digits of a Social Security number, a mother's maiden name, the date of birth. However, the era of massive data breaches has rendered this method dangerously obsolete. Vast quantities of PII are readily available on the dark web, allowing attackers to answer these traditional challenge questions easily. "Asking for PII doesn't work anymore," Passera says.

More recent verification methods, such as real-time video validation, where an individual displays their driver's license on camera, are no longer foolproof. The rise of AI-powered deepfakes—highly realistic fabricated video or audio—presents a relatively new but growing challenge.

Passera cites a reported example where a financial employee at a multinational firm in Hong Kong was asked to attend an internal video conference call. The call, however, was staged with deepfakes of senior officers, including the firm's chief financial officer, who duped the employee into transferring $25 million to a surreptitious account.

These and various other forms of deception create a tricky balancing act for cybersecurity officials. More stringent verification processes increase security but can frustrate users and impede productivity, especially at government agencies that serve diverse populations or share information with other agencies.

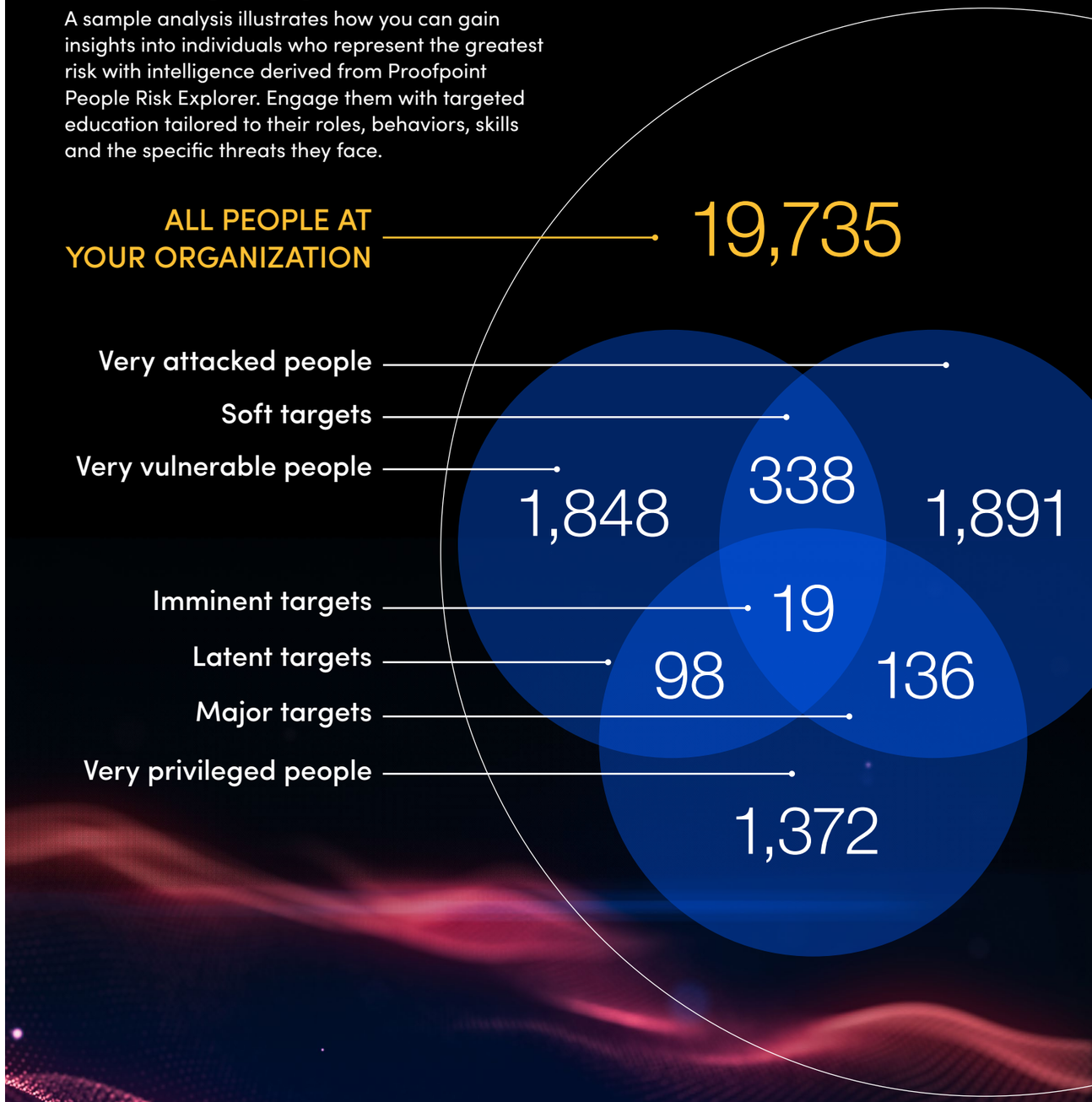
> "A service desk agent can change a password, reset credentials, manage multi-factor authentication (MFA) devices, and troubleshoot access issues. So, the service desk is a very valuable target for threat actors right now."
>
> – Pablo Passera, vice president of product management, Proofpoint

Once a malicious actor gets their foot in the digital door, however, it's just a matter of time before they gain wider access to an enterprise's network and begin their exploits, like:

- **Accessing sensitive data:** Navigating file shares, databases or cloud storage containing citizen PII, financial records or confidential government information.
- **Internal phishing:** Leveraging the compromised account's legitimacy to send phishing emails to colleagues, spreading the attack internally.
- **Privilege escalation:** Seeking ways to gain higher levels of administrative access.
- **Data exfiltration:** Copying and stealing sensitive information.
- **Ransomware deployment:** Encrypting critical systems and demanding payment.

Identify Who Attackers Are Targeting

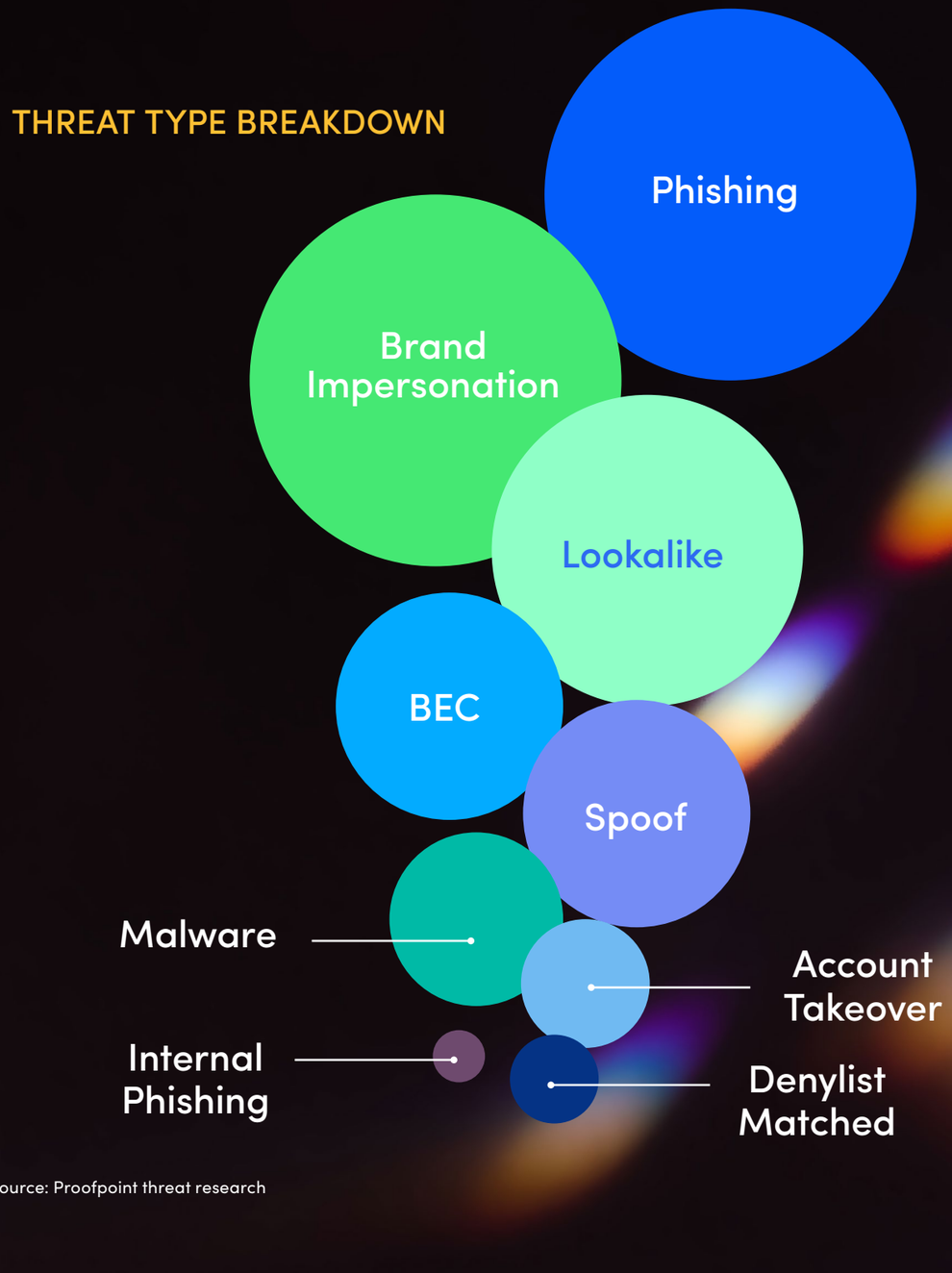
A sample analysis illustrates how you can gain insights into individuals who represent the greatest risk with intelligence derived from Proofpoint People Risk Explorer. Engage them with targeted education tailored to their roles, behaviors, skills and the specific threats they face.



Source: Proofpoint threat research

Stop the widest variety of advanced threats

We stop the broadest range of email cyberattacks with industry leading precision and intuitive classification. Security admins get visibility into the attack landscape faced by their organization, including the emerging threats and tactics used to reach users.



Source: Proofpoint threat research

Shifting to a Human-Centric Defense

Since attackers are exploiting human trust and behavior, IT and security officials need to develop defensive strategies that are also human-centric.

Adopting a human-centric security strategy involves taking several steps that yield a deeper, more granular understanding of user actions, context and inherent risks—particularly around email activity—rather than solely relying on technical controls, according to Passera and Witt.

Their perspective is based on Proofpoint's vast intelligence experience in monitoring 85% of the Fortune 100. Specifically, they recommend:

- **Assessing who is at greater risk** and deploying greater security controls around them. Witt points to three attributes to look for: high-profile individuals with a public persona, workers perceived to have access to valuable information and employees required to work with third-party systems.
- **Investing in specialized training,** especially for help desk staff. They need to understand the tactics used against them, recognize red flags in user requests (urgency, unusual demands, inconsistencies) and know the proper procedures for escalating suspicious interactions. Crucially, says Passera, "Service agents are not security experts." Training must be practical, synthesized and equip them to identify anomalies without overwhelming them with technical security details.
- **Re-evaluating identity verification processes** with an understanding of current threats like PII exposure and deepfakes, balancing security with usability. The key is a layered approach, potentially incorporating risk signals. For example, a simple password reset might require less stringent verification than enrolling a new MFA device, especially if the request originates from an unusual location or follows other suspicious activity indicators.
- **Deploying advanced monitoring and analytics tools that focus** on user behavior and correlate events across systems. This is where a human-centric approach diverges from traditional methods. Instead of just logging events, the focus shifts to understanding who is doing what, when, and why, and whether that behavior deviates from established norms.
- **Educating the entire workforce** about the risks of threat actors impersonating employees and the need for more vigilant cybersecurity awareness practices. Seven out of 10 working adults admitted to taking a risky action, such as reusing or sharing a password, clicking on links or QR codes from unknown senders or giving credentials to an untrustworthy source, according to Proofpoint's "2024 State of the Phish" report on human-centric cybersecurity.

Proofpoint's Integrated Human-Centric Platform

One way that Proofpoint safeguards its customers from the onslaught of potential threats is through its advanced Proofpoint Nexus Artificial Intelligence (AI) threat intelligence and machine learning (ML), which detects and blocks malicious emails before they reach users. It also remediates potentially threatening emails that reach users' inboxes.

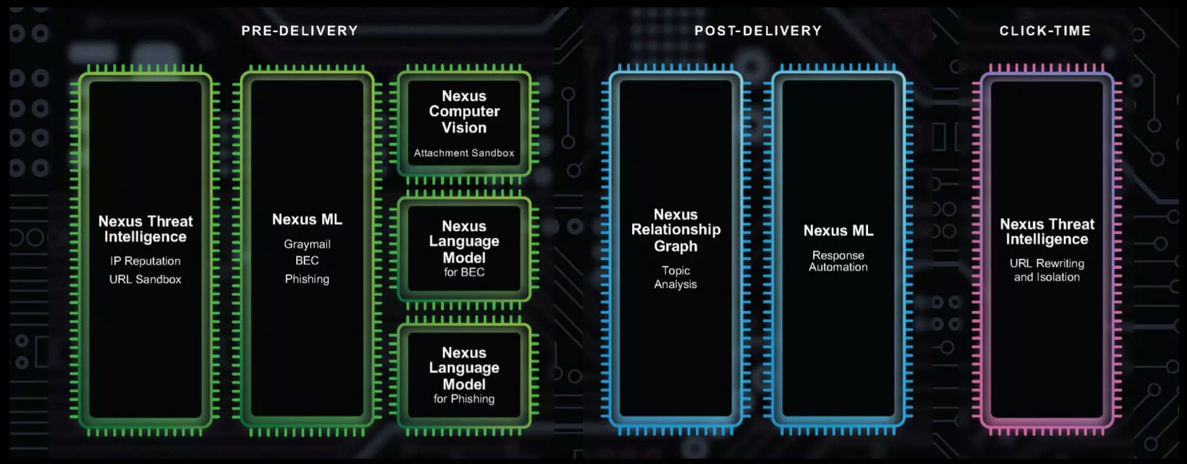
"We use a sandboxing technology that leverages information we glean from our broader email ecosystem that looks for problematic IP addresses,

Proofpoint's Multilayered, Integrated Cybersecurity Platform

PRE-DELIVERY
Detect malicious intent of email messages using high-performance machine learning and large language models with Proofpoint Nexus®.

POST-DELIVERY
Analyze and remediate messages in the inbox through behavioral analysis and API-based integrations into Microsoft 365.

CLICK-TIME
Get time-of-click protection for links included in emails through industry-leading threat intelligence and machine learning-powered sandboxing.



As a single strategic partner invested for your needs today and into the future, Proofpoint cybersecurity platform consolidates all your threat protection needs into a single offering.

Source: Proofpoint threat research

examines the nature of file attachments, and examines and, if need be, rewrites URLs to make sure they're safe," Witt explains.

"We can also give clients a very granular view of the most attacked individuals in their organization, based on volume or severity and sophistication of exploits being sent to them," he adds. By analyzing email activity on a client's network, Proofpoint, for instance, can identify who the last five people an individual emailed, or who sends email to that individual most often, or who that individual groups together.

"There is a whole other form of questioning that [a service desk agent] could ask when trying to go through the authentication and verification process," Witt notes.

Proofpoint's ZenGuide technology, meanwhile, complements those capabilities by providing a holistic architecture that identifies and mitigates risk across an organization's entire digital environment, reducing the burden on end-users and the service desk.

Agencies, for instance, can track user activities across various platforms – cloud application usage, file access patterns, permission changes, email sending behavior, login locations and times. Advanced tools utilizing AI and ML can establish baseline behaviors for individuals

and roles, automatically flagging deviations that indicate potential compromise. For instance, an employee suddenly accessing unusual files, attempting to change permissions or sending emails with suspicious links after contacting the help desk would trigger an alert.

Those and other capabilities led Gartner to name Proofpoint a "Leader" in its 2024 Magic Quadrant for email security platforms.

The Imperative for Government Agencies

Given the scale of highly sensitive citizen data they maintain, federal agencies stand to benefit most from advanced human-centric defenses. However, state, county and municipal governments and higher education institutions are already seeing added benefits from leveraging Proofpoint's solutions:

The City of Aurora, Colorado, struggled with high spam volumes, limited visibility into phishing attacks and lengthy response times. After switching to Proofpoint's Threat Response Auto-Pull (TRAP), Targeted Attack Protection (TAP), and other tools, the city gained "optics into email threats that we never had before," according to its CISO. It also stopped targeted ransomware attacks and reduced spam and bulk mail to zero.

The Mississippi Department of Child Protection Services faced various challenges in meeting regulatory and e-discovery requirements through archiving. After deploying Proofpoint Intelligent Compliance Solutions, the department is now able to easily access employees' communications, including the mailboxes of employees who have left the organization.

Princeton University needed to migrate multiple email platforms to the cloud while ensuring day-to-day operations and reliable communications between students, faculty, and staff. Proofpoint's Secure Email Relay provided the means to maintain the integrity of large volumes of outbound email while giving administrators necessary spam and malware detection and filtering capabilities.

Regardless of where government agencies are in their IT modernization journeys, agency leaders can build more resilient security postures by acknowledging that humans are both the primary target and the first line of defense.

Focusing on understanding and safeguarding human behavior, supported by intelligent technology, is the critical next step in protecting public data and ensuring the continuity of vital government services in an increasingly hostile digital world.

Learn more about how Proofpoint can help protect your agency by addressing human-centric risks.

This special report was produced by Scoop News Group for FedScoop and sponsored by Proofpoint.

FEDSCOOP proofpoint.