Hello, Operator? A Technical Analysis of Vishing Threats

By Mandiant

Published: 2025-06-04 · Archived: 2026-04-02 11:25:59 UTC

Written by: Nick Guttilla

Introduction

Organizations are increasingly relying on diverse digital communication channels for essential business operations. The way employees interact with colleagues, access corporate resources, and especially, receive information technology (IT) support is often conducted through calls, chat platforms, and other remote technologies. While these various available methods enhance both efficiency and global accessibility, they also introduce an expanded attack surface that can pose a significant risk if overlooked. Prevalence of in-person social interactions has diminished and remote IT structures, such as an outsourced service desk, has normalized employees' engagement with external or less familiar personnel. As a result, threat actors continue to use social engineering tactics.

Vishing in the Wild: A Tale of Two Actors

Social engineering is the psychological manipulation of people into performing unsolicited actions or divulging confidential information. It is an effective strategy that preys on human emotions and built-in vulnerabilities like trust and the desire to be helpful. Financially motivated threat actors have increasingly adopted voice-based social engineering, or "vishing," as a primary vector for initial access, though their specific methods and end goals can vary significantly.

Two prominent examples illustrate the versatility of this threat. The cluster tracked as UNC3944 (which overlaps with "Scattered Spider") has historically used vishing as a flexible entry point for a range of criminal enterprises. Their operators frequently call corporate service desks, impersonating employees to have credentials and multi-factor authentication (MFA) methods reset. This access is then leveraged for broader attacks, including SIM swapping, ransomware deployment, and data theft extortion.

More recently, the financially motivated actor UNC6040 has demonstrated a different vishing playbook. Its operators also impersonate IT support, but with the specific goal of deceiving employees into navigating to Salesforce’s connected app page and authorizing a malicious, actor-controlled version of the Data Loader application. This single action grants the actor the ability to perform large-scale data exfiltration from the victim's Salesforce environment, which is then used for subsequent extortion attempts. While both actors rely on vishing, their distinct objectives—UNC3944’s focus on account takeover for broad network access versus UNC6040’s targeted theft of CRM data—highlight the diverse risks organizations face from this tactic.

By reviewing the techniques, tactics, and procedures (TTPs) of actors like UNC3944 and UNC6040, organizations can better assess their own internal policies and guidelines when it comes to employee identification and protection of infrastructure and confidential data. Red teamers can also learn from their methodologies to better emulate real-world attacks and assist organizations in developing defense-in-depth strategies.

Mandiant has successfully used the following approaches to perform voice-based social engineering during Red Team Assessments for clients of varying sizes. The described techniques have enabled Mandiant to mimic TTPs from sophisticated vishing actors like UNC3944 and UNC6040, resulting in administrative-level user impersonation, corporate network perimeter breaches, and sensitive data access. Mandiant has additionally convinced multiple service desks to reset credentials and alter several forms of MFA. These simulated incidents have empowered organizations to proactively identify and resolve deficiencies that otherwise may have gone unnoticed and potentially exploited by a real threat actor.

Open-Source Intelligence Gathering (OSINT)

Effective social engineering campaigns are built upon extensive reconnaissance. The amount of information an attacker can source about corporate culture, employees, policies, procedures, and technologies in use directly impacts the maturity of a phishing scenario's development. A thorough search to provide a comprehensive overview of an organization from an outside perspective would include, but is not limited to, discovery of the following items:

- Network ranges and IP address space
- Top-level domains and subdomains
- Cloud service providers and email infrastructure
- Internet-accessible and internally used web applications
- Code repositories
- Corporate phone numbers and email address formats
- Employee positions and titles
- Physical office locations
- Publicly exposed internal documentation

Much of this information can often be found through publicly accessible resources. Company websites and marketing materials often list corporate contact information, including numbers for main lines, specific departments, or even individual employees. Social media platforms provide another means of profiling an organization. Professional networking services can be utilized to scrape the full names of employees and recreate corporate emails matching discovered naming conventions. Resumes shared on these platforms may also contain additional contact information including phone numbers and personal email addresses. Attackers may attempt to elicit private information by sending messages to employees from disposable email accounts, aiming to retrieve

details through direct interaction or from out-of-office auto-replies. Additionally, public forums, where employees might seek troubleshooting assistance, can inadvertently reveal company-specific details.

Search engines, such as Google, DuckDuckGo, and Bing, provide advanced filtering capabilities to narrow results from targeted queries based on keywords, file types, and other parameters. Figure 1 includes an example of a search filter designed to uncover sensitive files for a given target that may be unknowingly exposed.

```
 “TARGET” filetype:pdf | filetype:doc | filetype:docx | filetype:xls |
filetype:xlsx | filetype:ppt | filetype:pptx intext:"confidential" |
intext:"internal use only" | intext:"not for public release" |
intext:"restricted access"
```

Figure 1: Searching for documents with search filters

Anonymity networks, like The Onion Router (TOR), can be used to access hidden services, obtain restricted content, and identify supplemental data such as leaked employee IDs, usernames, passwords, and personally identifiable information (PII).

The internet offers a vast array of resources, and a good amount of intelligence can be discovered without any overt interaction with your target.

Leveraging Automated Phone Services

Some organizations make use of automated phone systems that have pre-recorded messages and interactive menus. These systems can provide callers with business-related information, facilitate employee self-service, or route calls to appropriate departments. If not found online, an attacker may attempt to obtain the phone number for an automated service by contacting an employee, often at a reception desk, claiming to have misplaced the number. Calling into these automated services allows an attacker to anonymously identify common issues faced by end users, names of internal applications, additional phone numbers for specific support teams, and, occasionally, alerts about company-wide technical issues. This type of information can be used to craft pretexts for subsequent activity that involves impersonating IT support.

Discovering Employee Identification Processes

Actors engaged in voice-based social engineering ultimately aim to interact with a human operator. While some automated systems provide a direct option to speak with a live agent, others can require some initial information to be provided, such as an employee ID. However, even in these cases, it is common for repeated incorrect entries to result in the transfer to a live agent anyway. Service desk agents handle a high volume of inbound calls ranging from internal employees needing a password reset to external customers experiencing problems with a public-facing application. They are generally given a scripted process for call handling including information they need to request from the caller for identification as well as where to escalate if they are unable to address the issue directly.

During the reconnaissance phase in social engineering a service desk, an attacker may feign ignorance or push boundaries of information disclosure before a requirement for identification is enforced. It is also important for an

attacker to take note of how service desk personnel react to incorrect or insufficient information being provided. For example, an attacker may provide an employee ID with an incorrect associated name to observe the response, potentially eliciting the correct full name or determining the validity of the employee ID format. Attackers may also call at different times to converse with varying staff members, use different voice modulations to conceal repeated reconnaissance attempts, and iteratively learn more about the service desk's identification process each time.

Alternatively, once a service desk number has been identified, an attacker can better target standard employees directly. Using publicly available resources, attackers can spoof the inbound number of a phone call to match that of the legitimate service desk. Without a procedure for verifying inbound callers claiming to be from IT, unsuspecting targets may be convinced by threat actors to perform actions that grant account access or divulge information that can be used to better impersonate staff.

Crafting a Convincing Narrative

With sufficient reconnaissance data, an attacker can formulate targeted campaigns reflecting plausible employee scenarios. A common pretext for contacting a service desk is a forgotten password. Many organizations verify employees using multiple factors. While initial reconnaissance might provide an attacker with answers for knowledge-based authentication methods, challenges arise if device-based verification is required. An attacker might impersonate an employee who claims their phone is unavailable (e.g., damaged or lost during travel) and who needs urgent account access. Another common practice is for actors to impersonate employees identified as being on personal time off (PTO) via out-of-office replies, leveraging a sense of urgency to persuade service desk personnel. Responses to such situations can vary, especially for executive-level users. In the event of a successful MFA reset, the attacker can then call back and try to get a different agent on the phone to further reset the impersonated user's password for a full account compromise. If the legitimate employee is genuinely unavailable, unauthorized account access can persist for an extended period of time.

The Evolution of an Exploit

The compromise of a single account can serve as a foundation for more complex social engineering campaigns. Breaching the perimeter of an organization often grants an attacker access to internal workflows, chats, documents, meeting invites, and ways to better uncover verified intelligence on existing employees. Open-source tools such as ROADrecon can extract details from entire Entra ID tenants, potentially revealing phone numbers, employee IDs, and organizational hierarchy. Attackers may also seek access to IT ticketing systems and support channels to impersonate service desk staff to end-users who have open requests. The more information an attacker possesses, the more believable their pretext becomes, increasing the probability of success.

Strategic Recommendations and Best Practices

Modern features in mobile technology, such as AI-powered Scam Detection on Android, demonstrate how software may be able to offer personal protection, but a comprehensive defense for organizations against vishing and related social engineering threats requires broad, proactive security initiatives and a defense-in-depth strategy. Mandiant recommends organizations consider the following best practices to reinforce their external perimeter and develop secure communication channels, particularly those involving IT support and employee verification.

Positive Identity Verification for Service Desk Interactions

- Train service desk personnel to rigorously perform positive identity verification for all employees before modifying accounts or providing security-sensitive information (including during initial enrollment). This is critical for any privileged accounts.
- Mandated verification methods should include options such as:
    - On-camera/video conference verification where the employee presents a corporate badge or government-issued ID
    - Utilization of an internal, up-to-date employee photo database
    - Challenge/response questions based on information not easily discoverable externally (avoiding reliance on publicly available PII like date of birth or the last four digits of a Social Security number, as actors often possess this data)
- For high-risk changes, such as MFA resets or password changes for privileged accounts, implement out-of-band verification (e.g., a call-back to a registered phone number or confirmation via a known corporate email address of the employee or their manager).
- During periods of heightened threat or suspected compromise, consider temporarily disabling self-service password or MFA reset methods and routing all such requests through a manual service desk workflow with enhanced scrutiny.

Enforce Strong, Phishing-Resistant MFA

- MFA should be enforced on all sensitive and internet-facing portals to prevent unauthorized access even in the event of a password compromise.
- Standardize one primary MFA solution, for most employees, to simplify security architecture and centralize a platform for detections and alerts.
- Remove weak forms of MFA, such as SMS, voice calls, or simple email links, as primary authentication factors. These are susceptible to vishing, SIM swapping, and other attacks.
- Prioritize phishing-resistant MFA methods:
    - FIDO2-compliant security keys (hardware tokens), especially for administrative and privileged users
    - Authenticator applications providing number matching or robust geo-verification features
    - Soft-tokens that are not reliant on easily intercepted channels
- Ensure administrative users cannot register or use legacy/weak MFA methods, even if those are permitted for other user tiers.

Secure MFA Registration and Modification Processes

- Do not permit employees to self-register new MFA devices without stringent controls. Implement an IT-managed or otherwise secure enrollment process.
- Restrict MFA registration and modification actions to only be permissible from trusted IP locations and/or compliant corporate devices.
- Alert on and investigate suspicious MFA registration activities, such as the same MFA method or phone number being registered across multiple user accounts.

Manager Involvement and Segregation of Duties

- Service desks should notify managers (via verified contact channels sourced from internal directories) upon an employee's password reset, especially for sensitive accounts.
- Require manager approval, through a verified channel, for all MFA resets. This creates third-party awareness and an additional record.
- For larger organizations, consider segregating service desk responsibilities. Customer-facing support desks should generally not have permissions to modify internal corporate employee accounts.

Employee Training and Vishing Awareness

- Conduct regular phishing simulation exercises that include vishing scenarios to educate employees about the specific risks of voice-based social engineering.
- Train employees to always verify unexpected calls or requests for sensitive information, especially those claiming to be from IT support or other internal departments, by using an official internal directory to initiate a call-back or by contacting their manager.
- Train employees to recognize common vishing pretexts (e.g., urgent requests to avoid negative consequences, claims of system issues requiring immediate action, unexpected MFA prompts).
- Equip service desk employees with access to logs of previous calls and tickets to help identify abnormal patterns, such as repeated calls from unrecognized numbers or sequential MFA reset and password reset requests for the same user.

Security Monitoring and Alerting for Vishing-Related Activity

- Utilize security information and event management (SIEM) and security orchestration, automation, and response (SOAR) technologies to monitor employee sign-in activity and service desk interactions.
- Create specific alerts for the following:
    - Password reset activity, particularly for privileged accounts or outside of expected patterns
    - New MFA device enrollment or modification of existing MFA methods

    - Multiple failed login attempts followed by a successful password or MFA reset
    - MFA fatigue attacks (multiple sequential incomplete authentications)
- All activities flagged as abnormal should be reviewed by an internal security team and investigated with the impacted employee and their manager.

Further guidance on hardening against UNC3944-style threats, including broader identity, endpoint, and network infrastructure recommendations, is detailed by the Google Threat Intelligence Group (GTIG).

Conclusion

This discussion of voice-based social engineering and its proposed resolutions aims to provide insight into attack methodologies and preventative measures relevant to this threat vector. Organizations seeking direct support on this subject or other services related to attack simulation and red team exercises are encouraged to contact Mandiant for assistance. Mandiant can discuss specific needs in detail and explore tailored recommendations to better equip security postures against advanced and persistent threats.

Posted in

- Threat Intelligence
