THE Human Factor 2025

VOL. 1 | **SOCIAL ENGINEERING**

proofpoint®

Introduction

A hacker's most dangerous tool might not be a malicious link or sophisticated malware. Instead, it might be their ability to hack your brain using fake personas, seemingly innocent conversations and believable stories. Under the right circumstances, clever social engineering can be more effective than any technical attack.

Social engineering is the manipulation of human emotions such as fear, annoyance, excitement or urgency to trick a victim into performing an action that benefits the manipulator. A victim might make a call, click a link or download a file while under the well-hidden control of the attacker.

Cyberattacks that target people usually include a social engineering component, whether it's in a phishing email, a fake popup on a compromised website or even a deceptive QR code on a sticker. And they're easier to personalize than ever. Attackers can target virtually anyone because they're no longer hindered by languages or locations, thanks to generative AI.

Many criminals that conduct fraud like business email compromise (BEC), telephone-oriented attack delivery (TOAD), espionage and pig butchering scams use pure social engineering. This way, their activity avoids automated detection by tools that can flag malicious URLs and attachments. The goal of these activities is to get a person to engage with them.

As efforts at social engineering continue to evolve, it makes sense to ask how well people are holding up against these attacks. To answer this question, we looked at data from our own Proofpoint Nexus® threat intelligence platform to understand the scale of the challenges that organizations face in addressing these threats.

Key findings

Top 5 social engineering themes:

1. **Advanced fee fraud**
2. **Extortion**
3. **Telephone-oriented attack delivery**
4. **Quick task**
5. **Request for quote**

25%

Pure social engineering is featured in 25% of all APT campaigns

90%

More than 90% of pure social engineering APT campaigns pretend to be interested in collaboration and engagement

50%

Advanced fee fraud increased nearly 50% in the last year

70%

Extortion-based fraud threats dropped by almost 70% in the last year

About this report

Historically, *Human Factor* report has been a comprehensive look at the human-centric threats that Proofpoint has detected, mitigated and resolved in the previous 12 months. This year, we are changing the format. Rather than bringing all our insights into a single report, we're breaking them up into a multipart series.

While each volume will explore one category of threats, they will all share the same theme: new developments in the threat landscape and how technology and psychology are combining to make modern cyberattacks so dangerous.

Scope:

This report draws on data collected from Proofpoint deployments around the world: one of the largest, most diverse data sets in cybersecurity. Every year, we analyze more than **3.4 trillion** email messages, **21 trillion** URLs, **0.8 trillion** attachments, **1.4 trillion** suspicious SMS and more. Data is pulled from across all the digital channels that matter.

** Covers March 1, 2024–Feb. 28, 2025.*

Differentiating BEC and Fraud

Business email compromise (BEC) is often used as a general term to cover a wide class of email fraud threats where criminals use social engineering to steal billions of dollars per year. In the last five years, victims have lost over $50 billion to fraud, according to the most recent FBI Internet Crime Report.[1]

Proofpoint wanted to better differentiate and classify the important aspects of email deception that's socially engineered, financially motivated and response based, beyond just BEC. So our researchers created the Email Fraud Taxonomy.

1. FBI. Internet Crime Report. 2024.

Proofpoint Email Fraud Taxonomy

Using this taxonomy, Proofpoint built detections to identify and differentiate types of fraud. Our researchers use this data to better understand the landscape overall, like what types of social engineering themes are most often used by fraudsters—including BEC.

Fraud trends

Proofpoint Nexus sees more than 2 billion emails per month that are potentially malicious. Nexus uses advanced language analytics to detect and block pure social engineering at a rate that's equivalent to technical attacks like malware and credential phishing.

Our taxonomy's rule set, which was developed by human analysts and machine learning, means that we can further automatically classify some of this activity with social engineering-themed tags. Some of these tags include gift carding, invoice and payment redirection, authority figure requests (like CEO impersonation), money mules and many others.

After filtering our overall detection data to include only known malicious fraud types with specific tags, these are the most frequently observed social engineering themes:

Advanced fee fraud (AFF)

An attacker promises a significant sum of money or high-value items in exchange for a small payment that the target must send to them.

Extortion

An attacker threatens a target with physical harm or damage to their reputation if they do not comply with the attacker's demand. This is separate from ransomware-based data theft and extortion.

Telephone-oriented attack delivery (TOAD)

An attacker tries to persuade the target to call a phone number, which may be included in the message as text, a picture or an attachment. When a victim phones, they are manipulated into installing remote access software or otherwise engaging with malicious content. Proofpoint blocks 117 million TOAD threats annually.

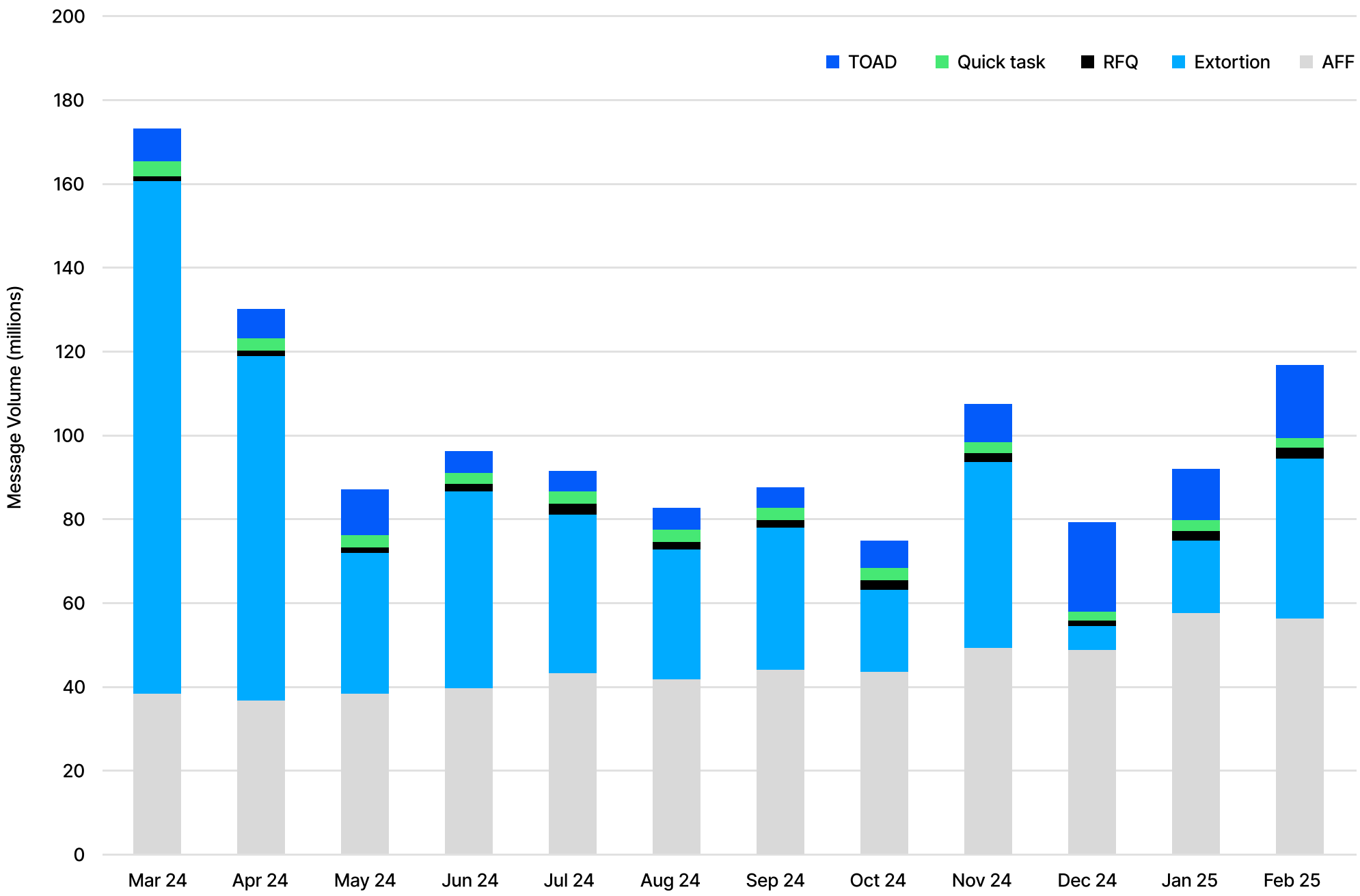
Quick task

An attacker does not request anything specific but instead aks that the target contact them again to fulfill a certain task, like making a purchase.

Request for quote

An attacker sends a bogus request for a quote, which leads to financial theft or follow-on activity like malware, credential theft or stealing physical goods.

Most frequently observed BEC themes

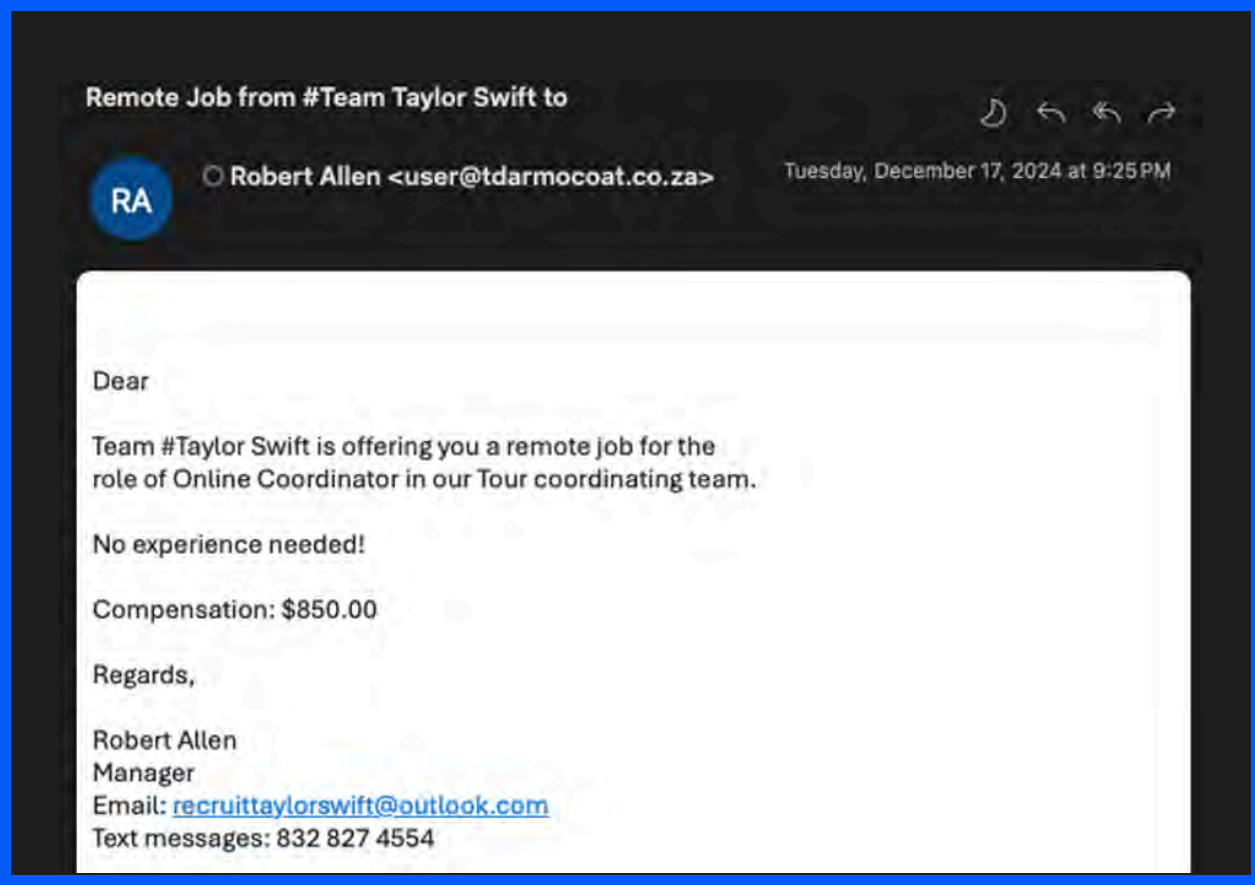


Top 5 social engineering themes identified by the Proofpoint Nexus BEC engine

Notably, extortion-themed fraud is decreasing across the threat landscape overall. Between March 2024 and February 2025, these threats dropped by more than 68%, from 122 million to 38 million per month. Meanwhile, AFF threats increased 47% in the same timeframe, from 38 million to 56 million. This could be due to the decreased efficacy of extortion themes. Or it could be because email providers have made improvements to crack down on these specific threats

These threats all end the same way: stolen money.

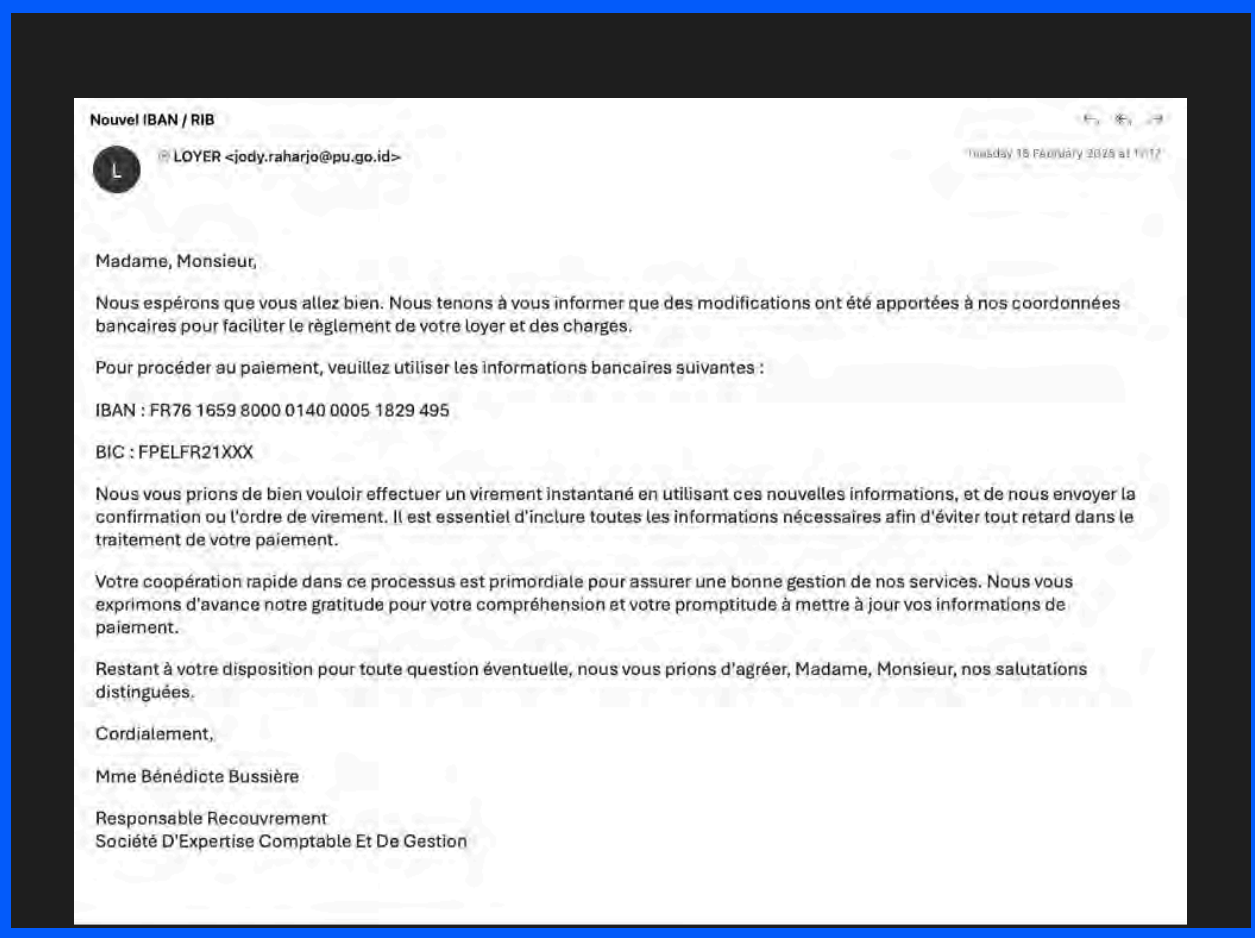
Not all fraud looks the same, though. For example, AFF scammers may use email lures like "piano for sale" or job offers to lure unsuspecting victims to engage with them. In December 2024, researchers even saw AFF scammers impersonate Taylor Swift's Eras Tour to send fake job offers. Swift-thinking observers would have immediately surmised "I Knew You Were Trouble." But the excitement caused by such an email may have compelled some people to fall for it.



Fake Taylor Swift recruitment email.

A **global** problem

Most of the fraud that's tracked by researchers is in English. However, Proofpoint also observes non-English language fraud. For example, a scammer known as TA2900 sends French language emails using rental payment themes to target people in France and occasionally in Canada.



Rental fraud phishing email.

In these campaigns, which Proofpoint observes multiple times per week, messages tell the recipient that the company's bank account details have changed and instructs them to send their next rent payment to a new account provided by the attacker. Interestingly, while we can't confirm this, based on some unusual phrasing and email body content, it's possible that the emails are written with the help of AI.

As generative AI becomes more common, threat actors will likely be able to expand their target pool by better tailoring social engineering to specific locations and languages. But it's important to remember that it doesn't matter whether emails are generated with AI or by an actual human, detection against these threats remains the same.

Benign conversations

Social engineering is all about getting a person to let their guard down. One proven method for accomplishing this is to approach someone with a benign message and engage them in a conversation over time. Not only does this help to build rapport, but the target is much more likely to trust the attacker after a sustained interaction that seems credible.

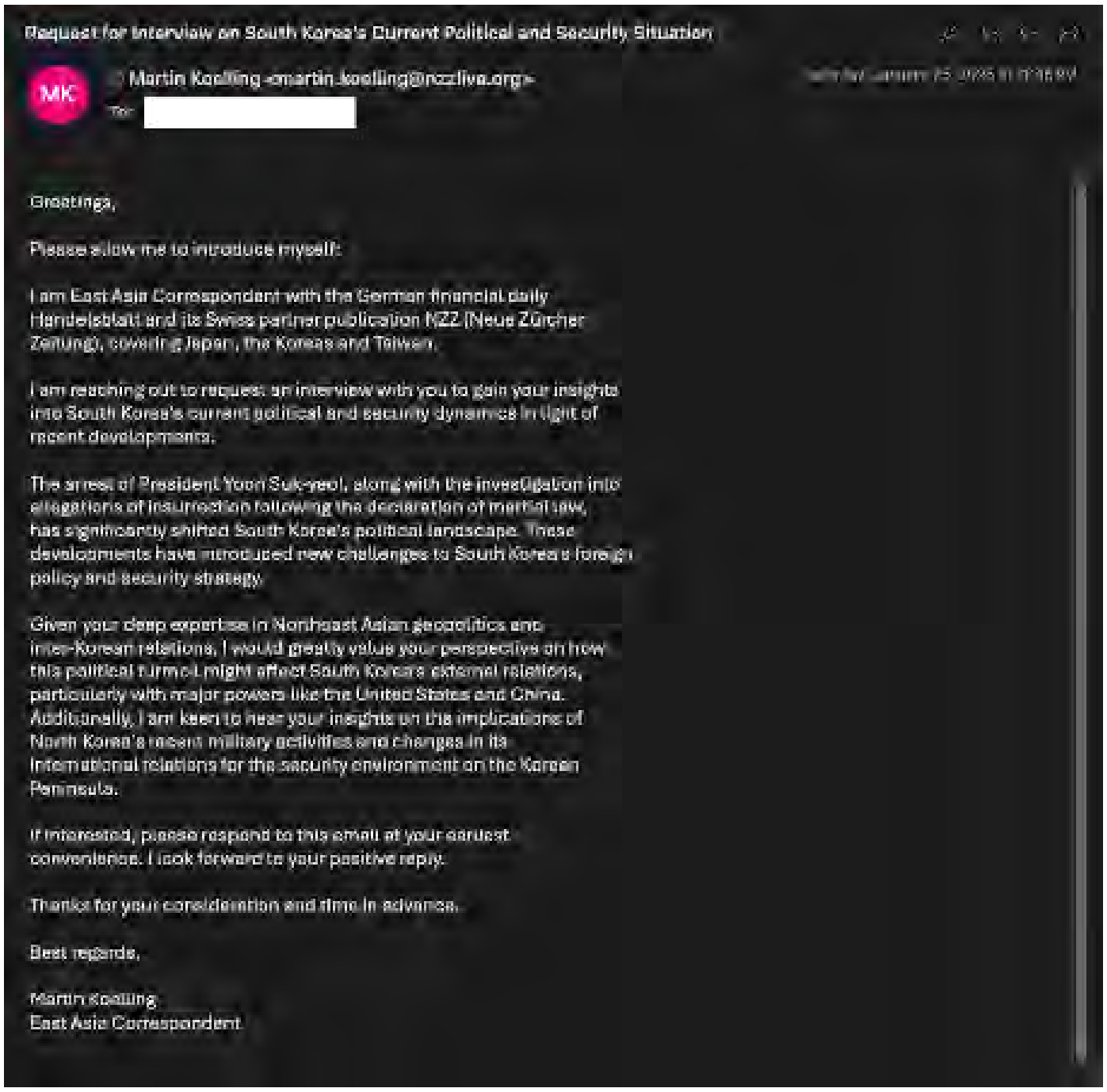
Once the attackers have established trust with someone, it serves as an inroad to follow-up emails that contain malicious links or attachments, which the target may now be more inclined to interact with. Threat actors also use benign conversations to test for a response and confirm engagement. This helps them to avoid the risk of burning their malware or an infection chain because it may be detected and blocked.

APT spotlight

As espionage continues to be the main motivation for state-sponsored actors, benign conversations are one tool that advanced persistent threat (APT) actors use in their phishing campaigns. Not only are these conversations used as lures to collect intelligence on foreign policy or current affairs, but they can also help actors gain insight into a government's position or decision-making process on a political issue. These insights may be valuable input into crafting the policy and reactions of the actors' sponsoring governments.

For example, North Korean threat actor TA427 engages targets from weeks to months using a series of benign conversations. The actor constantly rotates spoofed senders but engages with targets on similar subject matters, often related to current affairs in the Korean Peninsula. In January 2025, TA427 impersonated a journalist who was seeking details on how the attempted coup and subsequent arrest of former South Korean President Yoon Suk Yeol would affect South Korean security and foreign policies.

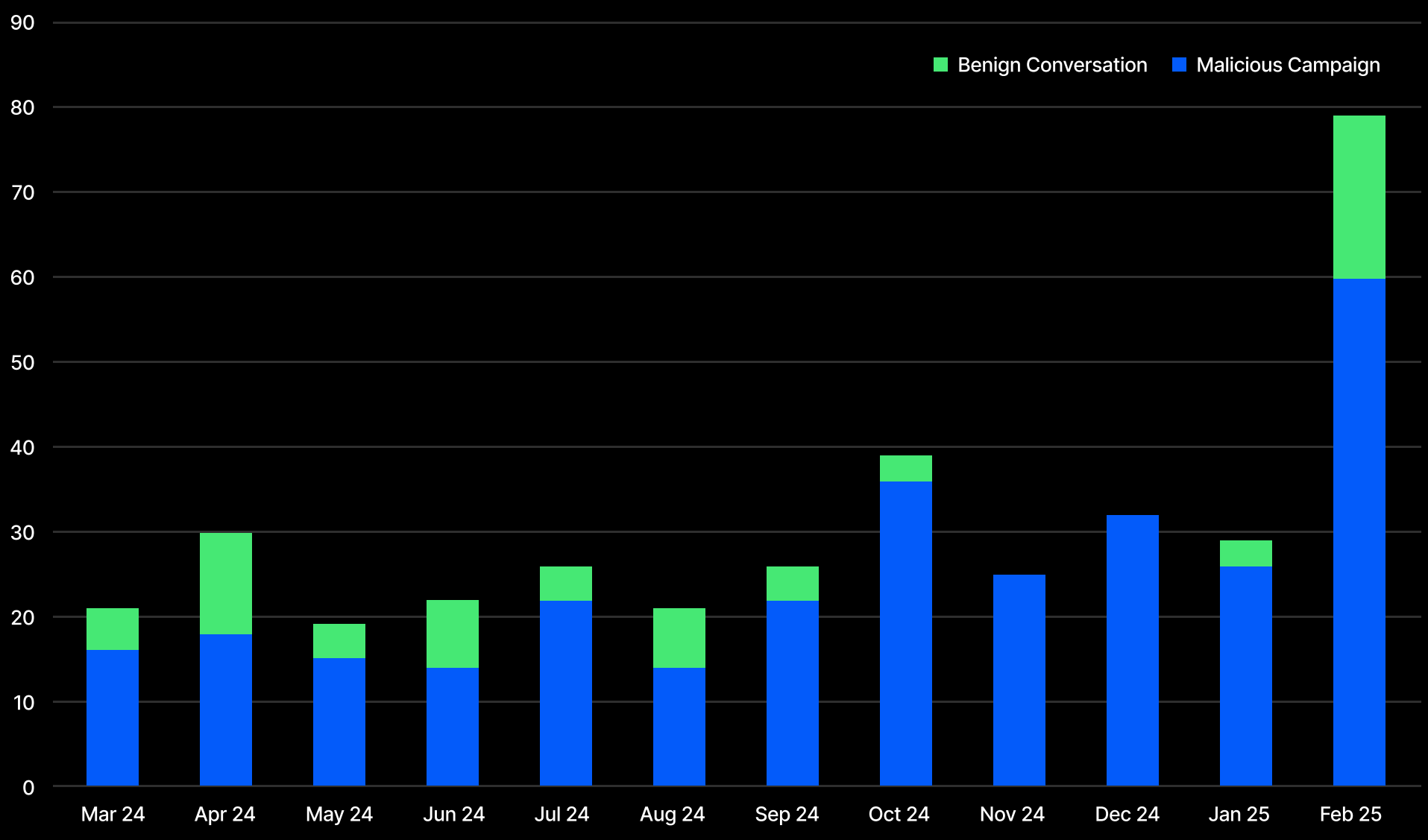
Proofpoint has also seen Iranian threat actor TA453 use similar benign conversation techniques, often focusing on Middle Eastern affairs.



TA427 lure.

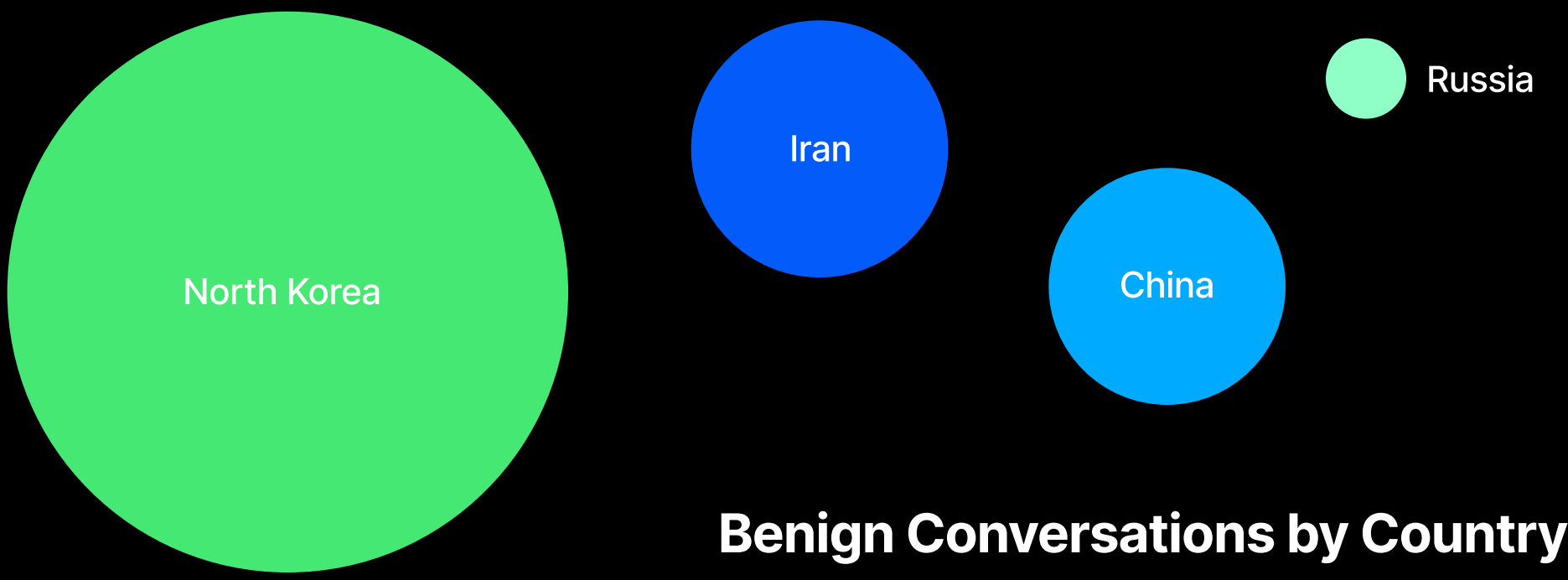
Based on data from observed state-sponsored campaigns over the last year, several trends—both data-driven and anecdotal—became apparent. As a subset of all observed state-sponsored activity, benign conversations accounted for around 25% of total campaigns.

APT campaigns observed over time



Benign conversations versus malicious campaigns observed over one year

Over the last year, the data from all observed state-sponsored campaigns shows that most benign conversations originated from North Korean actors. TA427 used benign conversations the most, representing almost 70% of all APT campaigns that used this technique.



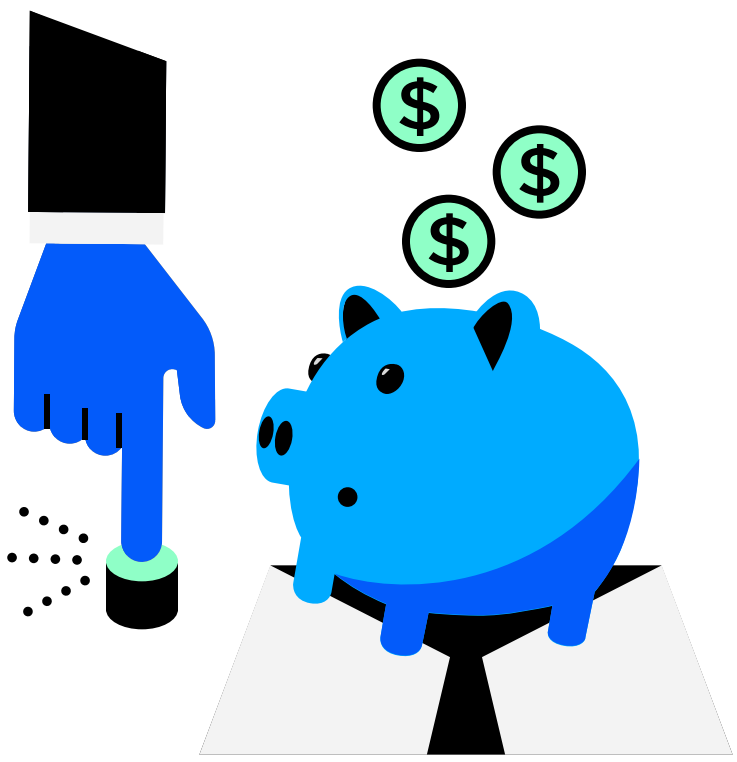
Benign Conversations by Country

Common themes and trends

While TA427 campaigns heavily influenced the data set, several trends emerged. Across about 80 campaigns that featured benign conversations documented by Proofpoint researchers, more than 90% were from spoofed senders. This includes spoofed organizations as well as people who work there. These were often think tanks, national or international government organizations, media outlets and academic institutions.

Senders consistently spoofed real individuals rather than creating email accounts for fake people at the spoofed organizations. The likely reason for this was to help to add credibility to their lures. In several cases, the sender address spoofed someone's personal account rather than their professional email address.

Another interesting trend is the consistency in theme and subject of benign approaches. More than 90% of state-sponsored campaigns pretended to be interested in collaboration and engagement, whether it was an invitation to participate in an event, a request for a comment on a news story, or a request for a meeting. What all these approaches have in common is that the attacker is likely trying to get a response by praising the target's reputation and soliciting their expertise.



Pig butchering on the rise

For years, pig butcher scammers have used benign conversations to swindle people out of billions of dollars of cryptocurrency. These fraudsters use similar techniques to BEC actors. Typically, they lure targets in with long-winded social engineering and eventually direct them to a fake cryptocurrency investment platform. According to the latest FBI Internet Crime Report, victims reported more than $6.5 billion in losses to investment fraud.[2]

Unfortunately, these scams are built on the back of real-world crimes, including human trafficking. In recent months, such fraudsters have also expanded into more traditional scamming territory like employment fraud. Pig butchering revenue increased 40% in 2024, with the number of deposits growing 210% annually.[3] Interestingly, the average deposit amount declined, with threat actors collecting more —but significantly smaller—payments.

2. FBI. Internet Crime Report. 2024.
3. Chanalysis. "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication." February 2025.

Conclusion

From fraud to spying, one tool is common in the threat actor toolkit. Instead of so-called technically sophisticated attacks, savvy scammers use social engineering. While themes and objectives vary, all have the same initial objective: to get people to talk back.

Proofpoint data shows that in the vast majority of attacks, the technical specifics matter far less than the human factors. That's why we recommend the following for a human-centric defense.

Visibility.

You want to know who's being attacked, how they're being attacked, and whether they act. It's important to know the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

AI-based detections.

Social engineering threats like TOAD and BEC are constantly evolving. Look for a platform that integrates language modeling, which can recognize subtle linguistic patterns and behavioral cues. This will ensure it can identify these threats before they cause any harm.

Impersonation protection.

Your teams should have total visibility into risks like domain spoofing and compromised supplier accounts. They should also have controls to address impersonation tactics, including the ability to take down and remove malicious look-alikes of your domain.

Tailored security awareness.

Training should be personalized and built around the latest threat intelligence. Also, giving users contextual warning banners and real-time coaching helps them make informed security decisions.

Automated workflows.

Threat detection, remediation and response should all be done automatically. This reduces the volume of email threats that security teams need to investigate.

To learn more about how Proofpoint helps you see your organization's human-centric risks and mitigate them, visit proofpoint.com

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →