Why phishing still works in 2026



nimblr.
security awareness

Contents

01 INTRODUCTION

02 GONE PHISHING

03 TOP-FIVE LISTS

04 MOST CLICKED SIMULATIONS

06 SIMULATIONS THAT TRICK

11 HUMAN PSYCHOLOGY OF PHISHING

13 FINAL THOUGHTS

Introduction

Thirty years after email became a popular form of communication, email phishing is still a problem. Phishing continues to top the list of the most prevalent tactics in social engineering incidents, regardless of advancements in protective measures such as antivirus, spam filters, strong passwords and multi-factor authentication.

How far have we truly come in identifying phishing emails and when do we fall short? To answer this question, we dug deep into Nimblr usage data of email simulation tests that were sent to end users of Nimblr in 2025. The results show clear trends in terms of types of emails that people interact with, despite characteristics identifying them as phishing. These trends hold true across the 10 European countries that are included in this report, with small differences noted. Understanding the psychological factors at play explains why people continue to interact with phishing email, even when they know better.

Where the country data shows significant differences is in the average click rates of email simulations, with Poland performing the best with an average click rate of 3.4% and Estonia performing the worst with an average click rate of 6.1%.

In addition to the data analysis, Online Behavior Specialist at Nimblr, Martin Karlqvist helps to answer the question: why do people fall for phishing?



Gone phishing

How many people actually interact, or click, on phishing emails? Finding a benchmark click rate is complicated since most phishing campaign results are unknown. The criminals are not providing their data, while phishing simulation campaign data is from a sub-set of users that are undergoing security awareness training and have been taught to be more cautious.

We turned to the Verizon's 2025 Data Breach Investigations Report (DBIR) for a benchmark click rate from a trusted, industry source. The DBIR reports an average click rate of 1.5% for phishing simulations among companies that have taken part in security awareness training with simulations.

https://www.verizon.com/business/resources/reports/dbir/

According to the DBIR, social engineering incidents were the second most prevalent cyber security incidents after system intrusion, followed by miscellaneous errors, basic web application attacks and privilege misuse. Social engineering is the only data breach incident type, in the DBIR, that focuses solely on end users.

Looking specifically at social engineering incidents, as reported in the DBIR, we find phishing accounting for 57% of incidents, followed by pretexting (30%), prompt bombing (14%), and baiting (0.5%).

Business Email Compromise (BEC) continues to be a vehicle for financial gains. Orion S.A., a chemical manufacturing company in Luxembourg reported that they lost $60m after an executive employee was the target of a criminal scheme involving wire transfers.

https://www.infosecurity-magazine.com/news/manufacturinglos-es-60m-bec/

The DBIR also highlights the importance of phishing reporting and the role of continuous security awareness training. Their data shows that employees with recent training - within 30 days - are four times more likely to report phishing simulations compared to those who have not received recent training.

Martin Karlqvist, Online Behavior Specialist at Nimblr, explains, "Phishing continues to succeed because attacks are designed for how people actually behave, while most defenses are built around rules, policies, and idealized user behavior. This isn't a matter of employees being careless or untrained."

> "phishing accounts for **57%** of social engineering incidents"
>
> Verizon's DBIR 2025

Top-five lists

The Nimblr data analyzed includes all simulations sent at least 100 times during 2025. The analysis looks specifically at the click rates of the following 10 European countries: Denmark, Estonia, Finland, Latvia, Lithuania, the Netherlands, Norway, Poland, Sweden, and the United Kingdom. This data cohort includes 1714 simulations sent around 11 million times, with around 420,000 clicks recorded. The cohort also includes repeats, such as the same simulation being sent to people in multiple countries or one person clicking a simulation multiple times.

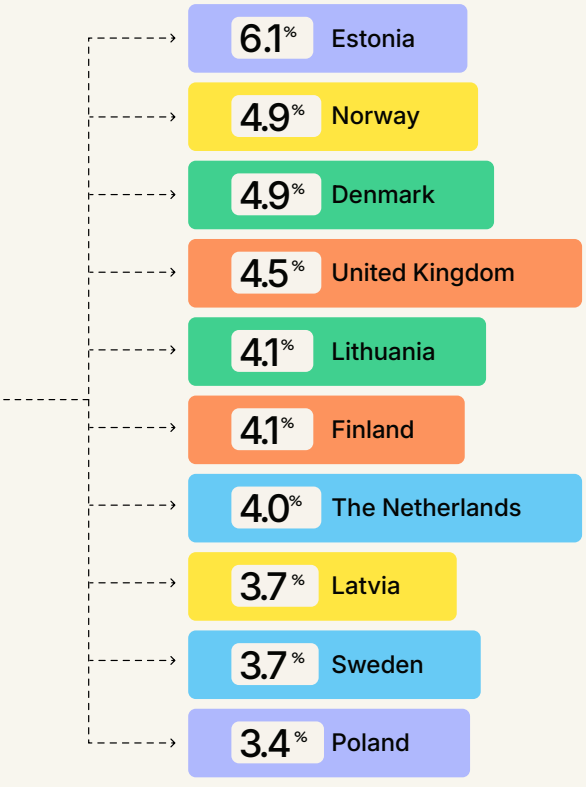
When looking at the average click rate of all of the simulations sent in a particular country we see Estonia with the highest average click rate of 6.1%, followed by Norway (4.9%), Denmark (4.9%), United Kingdom (4.5%), the Netherlands (4.0%), Latvia (3.7%), Lithuania (4.1%), Finland (4.1%), Sweden (3.7%) and Poland (3.4%).

We then analyzed the phishing simulations with the highest click rate in each country, creating a top-five list per country. The top-five list includes the simulation language, which showed that a combination of local language and English-language simulations made it into the top five list of several of the countries analyzed.

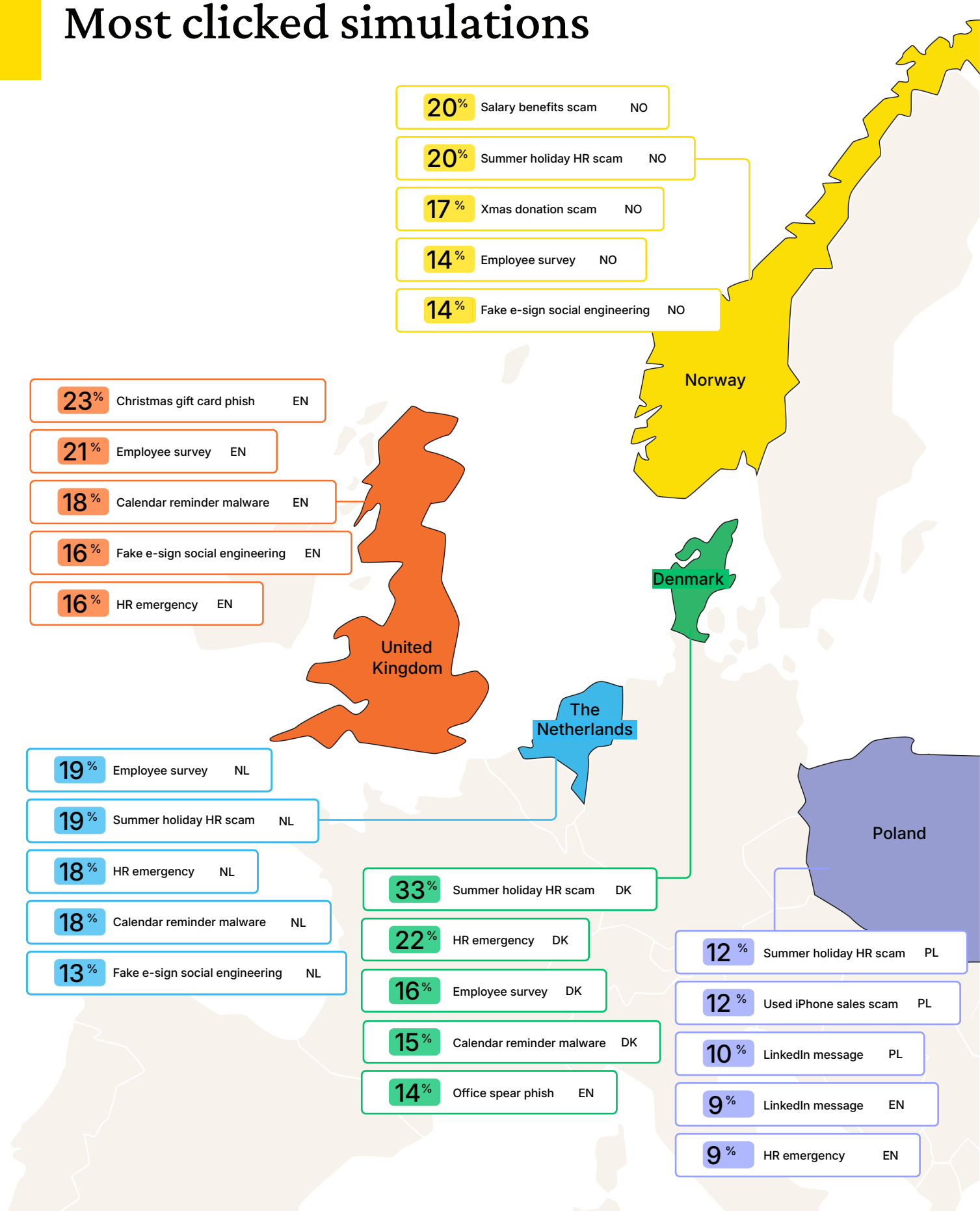
At Nimblr, we continuously monitor phishing trends globally and we actively expand our library of local-language phishing simulations as an important part of building user resilience. We aim to mimic actual phishing attacks that are designed for how people actually behave.

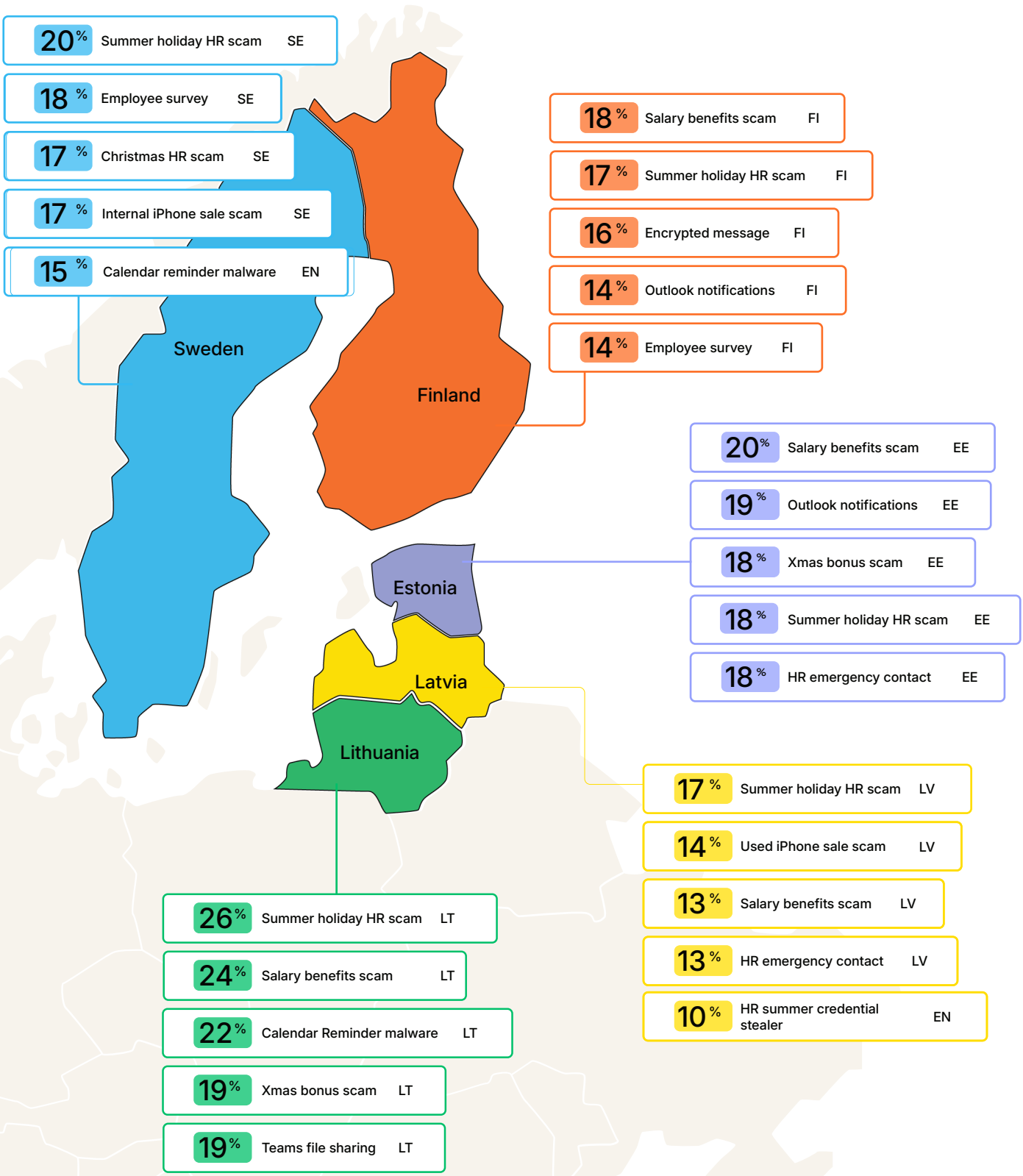
At the same time, we deliberately mix localized and English simulations, since many real campaigns that reach European organizations are sent in English. We balance local relevance with the exposure users need to recognize and resist English-language phishing scams that they are likely to encounter.

Average Click Rate



Most clicked simulations




20% Summer holiday HR scam SE
18% Employee survey SE
17% Christmas HR scam SE
17% Internal iPhone sale scam SE
15% Calendar reminder malware EN
Sweden
18% Salary benefits scam FI
17% Summer holiday HR scam FI
16% Encrypted message FI
14% Outlook notifications FI
14% Employee survey FI
Finland
20% Salary benefits scam EE
19% Outlook notifications EE
18% Xmas bonus scam EE
18% Summer holiday HR scam EE
18% HR emergency contact EE
Estonia
Latvia
Lithuania
17% Summer holiday HR scam LV
14% Used iPhone sale scam LV
13% Salary benefits scam LV
13% HR emergency contact LV
10% HR summer credential stealer EN
26% Summer holiday HR scam LT
24% Salary benefits scam LT
22% Calendar Reminder malware LT
19% Xmas bonus scam LT
19% Teams file sharing LT

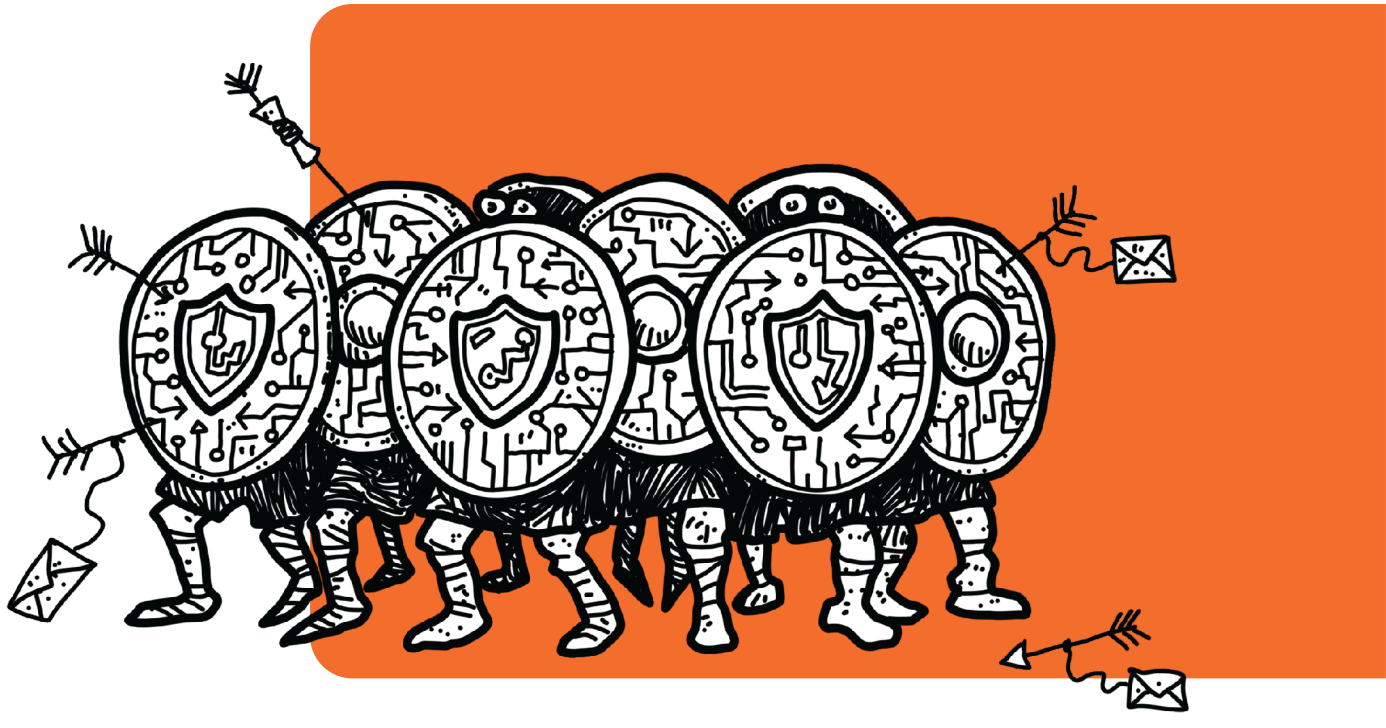
Simulations that trick

Nimblr sends a lot of phishing simulations, with more than 11 million being sent within this cohort in 2025. This makes this large data set particularly interesting to understand which type of simulation is successful at tricking the user and to identify themes and patterns.

Nimblr designs phishing simulations to reflect the real threats users face, because realism is what builds durable resistance. So, while our analysis dug deep into the simulations that experienced the highest click rates, there are hundreds that have very low click rates.

This is likely because users recognize the content of the email as suspicious. We will continue to send users a variety of simulations, with both high and low click rates, to mimic the real threats they face.

For this report we analyzed the top-five list for the 10 countries included and identified the following themes that are prevalent across multiple countries.



Human Resources (HR)

Every country saw HR-related simulations in the top-five list. In most cases these were delivered in local languages, making them appear more authentic, and asking people to provide personal data or click into a document. These simulations appear to come from people working in the company's HR department and the organization's name is referenced as well, lending credibility to the request.

While many people are wary of offers that appear too good to be true, such as a free iPhone, many are less suspicious of a human resources-related email asking for them to provide personal information. The context of the email gives people a sense of security, trust in the sender as well as in the request.

Examples:

- HR emergency contact credential stealing scam
- HR authority scam
- Summer holiday HR scam
- Employee survey
- Salary benefits scam

Information Technology (IT)

Email simulations related to IT are another strong theme among the top-five lists. These simulations appear to be system messages and play off of the urgent need for the user to quickly address the supposed problem. The content and the appearance of these simulations help them look authentic, which can be convincing enough to override caution and suspicion.

Examples:

- Calendar Reminder malware
- Encrypted message
- Fake e-sign social engineering
- Office spear phish

“This isn’t a matter of employees being careless or untrained”

Martin Karlqvist
Online Behaviorial Specialist at Nimblr

iPhone

It is interesting to note that iPhone-related simulations make the top-five lists in two of the 10 countries included in the cohort. iPhones hold a high perceived value and are widely considered desirable, while clicking the email to learn more is not considered a big enough threat. Tapping into people's inherent desire and curiosity is a key psychological method used by real phishers to scam.

Martin Karlqvist explains, "Beyond desirability, the effectiveness of iPhone-related phishing simulations is driven by low perceived risk and strong procedural familiarity. The message mirrors legitimate internal asset-resale practices, uses an informal tone consistent with everyday colleague communication, and frames the interaction as informational rather than transactional, keeping it below the user's internal security risk threshold. Scarcity cues then shift attention from verification to speed and competition, further suppressing critical evaluation at the moment of action."

Examples:

Internal iPhone sales scam
Used iPhone sale scam

Christmas

Holiday-themed simulations, especially related to Christmas, appeared in five of the top-five lists analyzed. These simulations include offers of Christmas gifts for employees and donations for people in need.

The human factors go beyond seasonal goodwill, explains Martin Karlqvist, "Christmas-themed phishing simulations succeed because they exploit administrative legitimacy and social obligation rather than overt incentive.

"Messages framed as holiday confirmations, scheduling corrections, or charitable actions activate anticipated regret and responsibility, shifting the user's focus from security evaluation to social correctness.

"This reframing lowers perceived risk and increases compliance, particularly when the request appears routine, time-sensitive, and aligned with expected end-of-year tasks."

Examples:

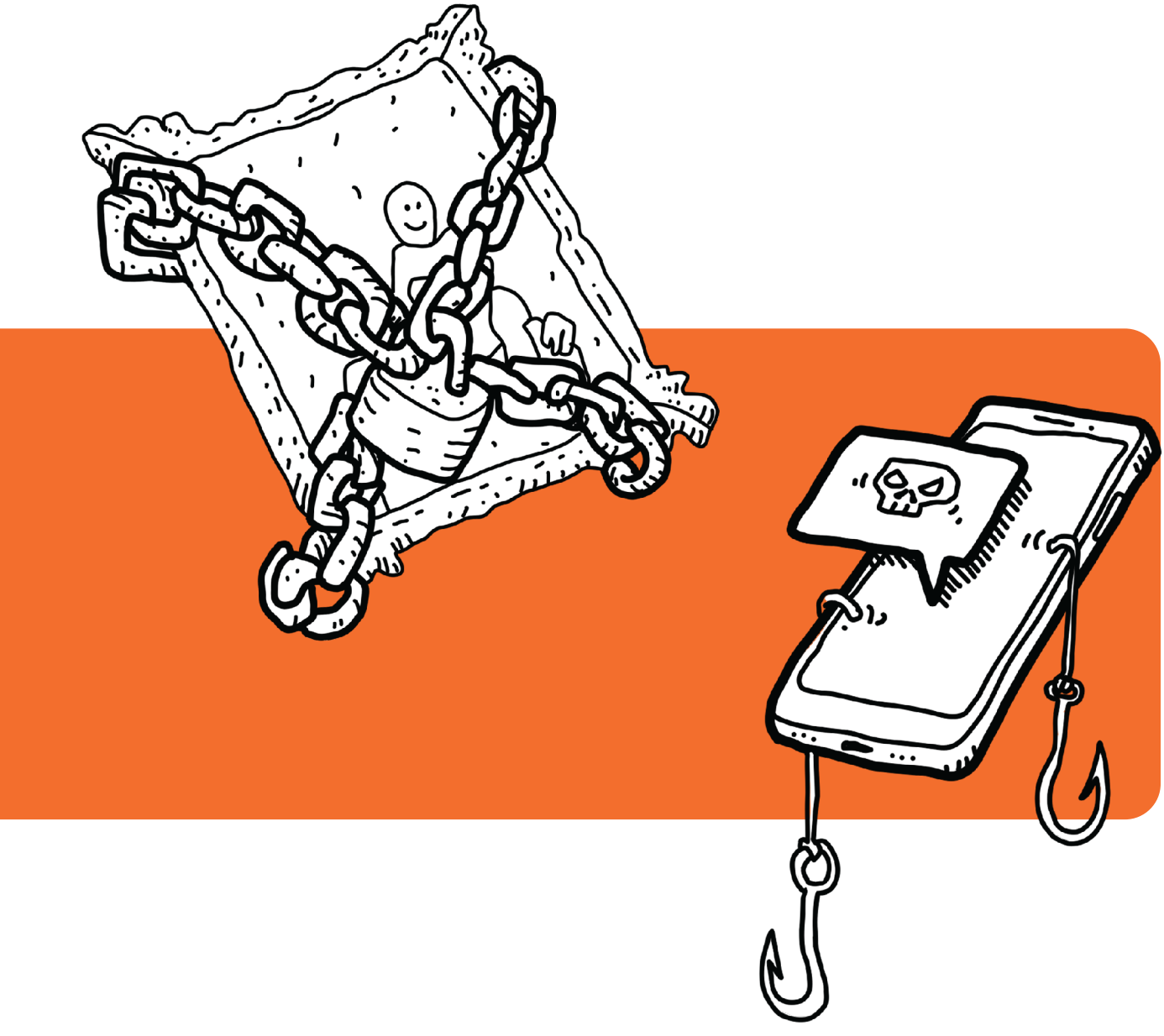
Xmas donation scam
Christmas gift card phish
Christmas HR scam

Personal photos

Photo-themed phishing simulations are highly effective because they exploit identity and uncertainty, creating an immediate need to verify potential personal exposure. By framing the interaction as a harmless, low-effort check (“Is this you?”) and adding vague contextual details, the message triggers curiosity and reputational concern while remaining below the user’s perceived security risk threshold.

Example:

Picture Social Scams



Human psychology of phishing

People don't get tricked by phishing because they are stupid or careless, but because the scammers exploit human psychology and modern digital tools. Even believing you will never fall for a scam can reduce your vigilance and make you more susceptible.

Let's take a deeper look at the six human psychology factors at play in phishing emails.

Tech-savvy users fall for well-crafted scams



Non-technical users fall for simple scams

01. Emotional triggers

Phishing emails often rely on emotion to elicit an action, like clicking a link or providing information. When we are not experiencing an emotional trigger, we can think rationally and slowly, but once the trigger is engaged, we can act quickly without thinking.









02. Authority bias

We are conditioned to trust authority and comply with requests quickly, whether it appears to come from a senior executive, an HR colleague, or the IT team. Work environments include inherent power structures that scammers use to trick people into complying.

03. Time pressure and distraction

Unlike the emotional trigger urgency, time pressure and distraction take advantage of the fact that people often check their email while they are multitasking, tired or using a mobile device.

Scammers know that it is more difficult, technically, to inspect send addresses and URLs when using a mobile phone. When we are under pressure, and distracted, we are more likely to act quickly without critical reflection over our decisions.

04. Advanced impersonation

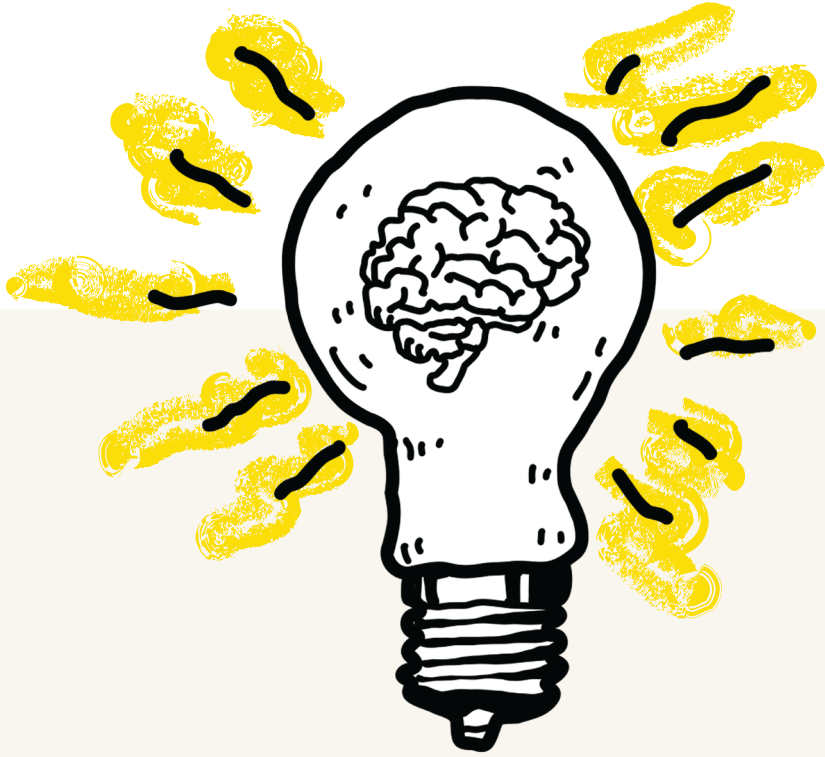
Phishing emails today are highly sophisticated with good grammar, correct branding and sometimes copy actual email templates from trusted brands, while personal leaked data is used to create highly-targeted messages. This level of advanced impersonation makes phishing emails look legitimate at first glance and requires a critical eye to spot a scam.

05. Mimic business processes

Phishing emails often mimic standard business processes, such as invoice requests, document sharing notifications and calendar reminders. These are common tasks that users are expected to manage in their daily work, which results in users not questioning them.

06. Social proof and familiarity

Phishing emails that reference colleagues' names or systems that the organization uses are leveraging social proof and familiarity to create a sense of trust from the recipient and to override critical thinking.



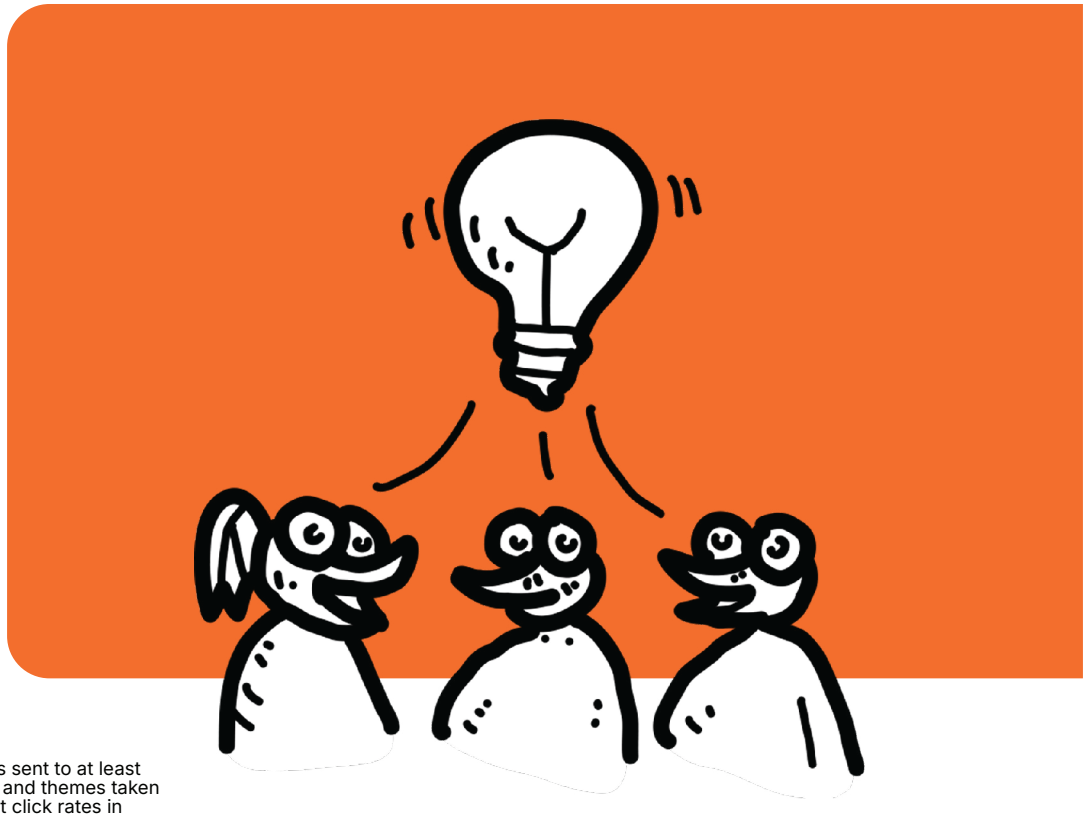
Final thoughts

It's been 30 years since email became a popular form of communication, and people are still getting tricked by phishing. Our data shows that users of Nimblr are most likely to click simulations in their local language that appear to come from their own organization, with content such as HR and IT requests. This isn't a surprise, since these simulations are designed to override people's critical thinking in a myriad of technical and psychological ways.

In fact, this is how our product is designed: train and test people in a safe environment where they can learn. Each simulation is linked to a customized reminder for those users who are tricked into clicking a link or opening an attachment. The reminder displays the message that tricked the user, along with interactive tips on what to do differently next time. The user is also offered to start an optional basic training module tied to the current simulation.

What is surprising in the data is the prevalence of iPhone and Christmas simulations among the top-five lists. It's a stark reminder that manipulating human psychology is extremely effective, even when the message content is not work related, or is commonly known to be a scam.

Phishing's success is not because employees are careless or untrained, but because attacks are designed for how people actually behave, while most defenses are built around rules, policies, and idealized user behavior.



Data analysis filtering:

The data cohort includes simulations sent to at least 100 people, with click rate averages and themes taken from the simulations with the highest click rates in each of the 10 countries.