Email Scam Detection in the Real World: Evaluating Phishing Email Awareness Outside the IT Sector

Lana Mustafić
Software Engineering
University of "Džemal Bijedić" Mostar
Konjic, Bosnia and Herzegovina
lana.mustafic@edu.fit.ba

Abstract— **Phishing sensitization among non-IT employees at the reception of a four-star hotel in Bosnia and Herzegovina is analyzed in this research. The six employees were tested using a simulated phishing email that resembled a cancellation notice from booking.com. The test aimed to see how many employees would fall for a fake email and click the harmful link. Four out of six did, showing low awareness of phishing attacks. This paper shows how the test was done, what happened, and why teaching cybersecurity to non-technical people is important.**

Keywords: Phishing awareness, social engineering, email scams, cybersecurity, non-technical users

I. INTRODUCTION

Now, even non-technical staff depend on technology day by day. Though digital systems increase productivity and efficiency, they also make users vulnerable to cyber threats. One of the most insidious and common types of such attacks is phishing—one of a category of attacks that targets people rather than machines.

Phishing works by impersonating legitimate sources and making users do unsafe things, such as clicking on bad links or submitting credentials. Phishing is a social engineering attack wherein the attacker leverages the victim's confidence, sense of panic, or fear in the belief that the victim will react. Based on numerous reports from across the globe, phishing is among the top three causes of security breaches worldwide. [3]

Even if cybersecurity training and procedures are standard for IT-profession based positions, the vast majority of those who work outside of this category—receptionists, administrative assistants, or customer service workers, for example—are not given the same. Still, they usually are points of first contact and often work with sensitive information. This makes them high-priority targets for attackers.

In hospitality specifically, email communication is constant and time sensitive. Staff members are trained to be responsive and helpful, not skeptical. These behavioral expectations can make them especially vulnerable to phishing schemes. This paper seeks to better understand how this vulnerability manifests in practice, through a real-life simulation with receptionists in an active hotel environment.

II. METHODOLOGY

A. Participants

The six receptionists who took part in this experiment offer a true picture of hotel staff. They came from different educational backgrounds. Some had degrees in tourism or languages. Others had vocational training. However, no one had studied information technology or received formal training in cybersecurity awareness. This lack of training is common in hospitality environments, where employees typically prioritize guest experience instead of managing digital threats.

None of the people involved had anything to do with IT or cybersecurity stuff. Their jobs were more about helping guests — things like booking rooms, checking people in or out, answering calls, or talking to guests through Booking.com and similar sites. That's what they were good at. They weren't expected to know anything about phishing emails or spotting online threats — that's not part of what they normally deal with.

This group is important because phishing attacks rarely target IT professionals. Instead, cybercriminals target the average user. This includes people whose days are packed with multitasking, working with others, and strict schedules. These individuals are more likely to click on a suspicious link. It's not that they are careless; they simply don't have the time to think twice.

The goal of this study was to observe how a non-technical employee behaves when faced with a realistic phishing attempt. How do they interpret the message? What details do

979-8-3503-2994-0/24/$31.00 ©2024 IEEE

they focus on—or miss? And most importantly, do they react with caution or trust?

B. Phishing Simulation Design

The simulated phishing message was crafted to look like a real email that front desk staff frequently encounter. It said that a reservation had been canceled and that immediate action was needed through a link provided. The language was formal and polite, imitating the tone commonly used by booking platforms.

Visuals were important. The email used the same color schemes, fonts, and layout as a typical message from booking.com. It included a familiar logo, a standard footer, and formatting details that most people connect with professional communication. These elements were intentionally included to build trust and lessen suspicion.

The only slight hint that something was wrong was the sender's email address. It had a tiny typo in the domain, like @booklng.com instead of @booking.com. A seasoned individual might notice this detail but might easily not. This happens often when staff members feel stressed or rushed. The goal wasn't to deceive anyone in a harmful way. The purpose wasn't to try to trick anyone in an evil way. It was to see how convincingly the artificial human message would be accepted as real and whether the employees would react the same way they would in a real situation.

C. Execution

Timing was key in the simulation. The phishing email was sent when the workday was busy. The front desk was handling check-ins, guest calls, and a significant number of emails during that time. This choice was not random. Attackers in the real world often select busy periods on purpose. They know employees are more likely to act quickly and less likely to examine what they are clicking on.

The participants didn't know they were part of a test. This showed their true reactions, without the careful thinking that usually happens in formal training or planned drills.

The simulation was not rushed. Instead, it was allowed to run for several hours. This allowed participants to decide whether to act or not at their own pace. This kind of approach stimulates how real phishing emails behave. They often stay unopened for some time before someone sees or replies to them. Sometimes, employees read these emails only when they finally have a quiet moment. People might reply to emails at the end of their shift when they are tired.

This experiment was designed to feel like real life, so it could show how people really act and how much they know about security. It showed what someone does when a "normal" email shows up in their inbox during a stressful, demanding shift.

D. Ethics and Consent

Maintaining ethical standards was a high priority during the experiment. The hotel's management team and IT department approved the simulation. It was designed to be safe and educational. No personal information was collected, and no real accounts were accessed, affected, or endangered.

After the test concluded, a debriefing session was held with all participants. During this session, staff learned that they had participated in a phishing simulation. They were shown the reasons for the exercise. They examined the elements of the email that seemed suspicious and were taught what to watch for in the future. Many were surprised by how convincing the message had been.

The debrief had a friendly tone. The goal was to help them see how even careful workers can be fooled.

By including them in the learning, the test gave a chance to learn, think about their actions, and be more careful in the future.

This way of teaching helped them understand that staying safe online is not only for IT people but for everyone.

III. RESULTS

A. Behavioral Data

Four of the six employees clicked the phishing link. Three of them submitted what looked like valid credentials. Two rejected the email outright—one reported the email as suspicious to the IT department and marked it, and the other simply deleted it.

This is to say that 66.7% of the participants engaged with a harmful aspect of the email, whereas 33.3% used caution. The three employees who provided credentials did so in haste, suggesting that they found the email urgent and authentic.

Surprisingly, none of the subjects checked the sender's email domain, although it was the sole obvious indication of fraud. It also reinforces the assumption that most users skim through emails quickly and trust brand visuals and tone rather than verifying technical details.

B. Influence of Experience

It is worth noting that two of the cautiously responding employees were the most experienced in hotel work, with more than three years each. On the other hand, the responders who clicked were either new staff members or had been working for less than a year. This suggests that professional maturity and familiar patterns of internal communication could be the reasons for phishing detection.

C. Post-Test Interviews

Employees who clicked on the link often reported that they "had no reason to doubt" the email. Most said they were used to seeing such messages and had never received guidance on identifying fake emails.

Others even believed that if they failed to react to an actual cancellation, they would be blamed for it.

This means that the fear of not acting can be such a strong influence as trust, and therefore, employees will act without hesitation.

IV. DISCUSSION

A. Broader Implications

The test only had six people, but it shows a bigger problem. Many workers in healthcare, schools, stores, and government don't get enough training to notice or handle things like phishing emails.

Many workers utilize the graphical aspect of emails virtually solely to determine if they are authentic. Their rationale is that if an email "appears official" with logos, proper formatting, and names that they recognize, it is fine. What they don't typically realize is that cyber attackers go out of their way to craft emails with a legitimate appearance and feel with scary accuracy.

Even worse is the excessive dependence on IT systems to automatically filter out threats. Most employees think that if an email reaches their inbox, it has already been screened by some security system.

This misplaced faith in technology over human judgment makes sharp blind spots in organizational security. [4] Firewalls and spam filters have a useful role to play, but no system is foolproof. Threats will get through. When they do, the last line of defense is the person reading the message.

This highlights the need for strong technical defenses and the creation of a human layer of awareness and vigilance to support those systems. Without that human element, even the best defenses can be easily bypassed by a cleverly written email.

B. The Psychology of Phishing

The results of the simulation are highly consonant with existing psychological studies on phishing and social engineering tactics. [3] Phishing emails mostly play on feelings like urgency, fear, trust, and obligation.

In this test, the fake email said a guest's reservation was canceled and needed a quick reply. Since front-desk workers are taught to act fast and keep guests happy, this message made them rush instead of thinking carefully.

Phishing criminals also benefit from authority bias—the fact that humans comply with messages they believe originate from a trusted or known source. [2] Because the email was an imitation of booking.com, which was an application staff used every day, it was instantly credible in the eyes of the recipients.

Another factor is cognitive load. At the hotel front desk, it's always really busy. People must do a bunch of things at the same time — reply to emails, answer phone calls, check guests in, and fix problems. When you're tired or stressed, it's hard to pay close attention to every email. Stuff like a weird sender or strange formatting can be missed.

Phishing works because people are tired or distracted, not because they're careless.

A. Recommendations

If a company wants to stop phishing, everyone has to help out, no matter how much they know about computers. The team is only as strong as the person who's the weakest at spotting problems. So, everyone needs to be careful.

Based on what the study found, here are some ideas:

Make sure all new employees get training about phishing, not just the IT people. The training should teach them how to spot phishing emails, check if a message is suspicious, and how to report it safely.

Also, do tests like this one every few months to see how well employees recognize phishing. This helps them learn and remember to stay safe online. These simulations should vary and become more realistic. They should focus on different types of messages employees might receive. [5]

Create a place where people don't worry about getting blamed if they report a strange email. Mistakes should be treated as learning opportunities, not reasons to get in trouble.

Also, make it simple for employees to report suspicious emails by giving them easy-to-use tools. For example, include one-click "Report Phishing" buttons in email clients.

Create a workplace where people know it's okay to be careful. People shouldn't feel strange about spending some time checking their emails. It's way better to be careful than to hurry and make a mistake.

Places like hotels have to be serious about this since they handle lots of private info like names, emails, phone numbers, payment stuff, and passports.

If someone falls for a phishing email, it can cause serious trouble. The hotel could lose money, have security issues, and people might stop trusting it.

Everyone at work uses computers — front desk staff, cashiers, cleaning workers, and the people who handle bookings.

V. CONCLUSION

Phishing attacks are no longer isolated incidents aimed at highly technical users or system administrators. They have evolved into everyday threats that target anyone with access to email or digital platforms. This research highlights a sobering reality—non-technical staff, particularly those in customer-facing roles such as hotel receptionists, are not only frequent targets of phishing attacks but are also largely unprepared to detect or respond to them.

The findings of this study point to a fundamental deficit in organizational preparedness: though all employees utilize digital technologies daily, training in their safe use is generally provided to IT personnel only. But cybercriminals know how people think and use feelings like urgency, authority, and fear to trick them. They send emails that look real and use these feelings to catch workers who aren't expecting it. [1]

Through this simple simulation, where a fake cancellation email was sent to six receptionists, we observed a 66.7% success rate in phishing engagement—four of the six clicked the link, and three went so far as to submit their login information. This rate of success for the attacker would be considered extremely effective in a real-world cyber campaign, and it reinforces how dangerous the situation can become without preventative action.

That the two members of staff who escaped the attack were more experienced means that time in post can add to better instinctive judgment in online communication. Just learning from experience isn't enough or practical for a long time. New employees, especially in places like hotels where people come and go a lot, need proper training and help from the start.

Cybersecurity isn't just about the technology you add to. Everyone at the company has to help out with this. From the receptionist to the bosses, they all need to know what the risks are and how to keep safe.

Here's some easy things they can do to make it better:

Having mandatory phishing awareness training as part of the onboarding process.

Having regular unannounced phishing tests to track improvement.

Promoting a culture of openness in which employees don't hesitate to report suspicious emails, even if the prove to be false.

Cross-department cooperation—HR, IT, and management—so security is part of the company's mindset and not an afterthought.

More broadly, this study illustrates the imperative of paradigm changes in the way we teach cybersecurity. Rather than assuming technical know-how, organizations must meet employees at the level of everyday language, familiar examples, and regular drills. [5] This is especially important in service sectors like hospitality, where customer satisfaction might take the place of risk avoidance.

In the long run, employee training is not so much about deflecting one phishing email—it's about building an adaptive, responsive, and resilient culture that can deflect all forms of cyber-attack. By training employees to pause, verify, and report, organizations can dramatically reduce their exposure to social engineering and its typically disastrous consequences.

Lastly, the security of an organization does not solely rely on firewalls or anti-virus software but on human beings—on their awareness, actions, and analytical skills in the face of deception. This study has highlighted the need to include each member of the organization in the conversation on cybersecurity.

ACKNOWLEDGMENT

The author extends sincere thanks to the management and IT staff of the hotel involved in this study. Their cooperation, openness to improvement, and trust made this research possible and meaningful.

REFERENCES

[1] A. Jain and B. Gupta, "Phishing detection: analysis of visual similarity-based approaches," Security and Communication Networks, vol. 2017.
[2] M. Jakobsson and S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley, 2006.
[3] R. Kumar et al., "Human factors in phishing: A systematic literature review," Computers & Security, vol. 93, 2020.
[4] NIST, "Phishing: Guidance and Recommendations", 2021.
[5] L. M. Roberts, "Social Engineering in Non-IT Sectors: The Hidden Cyber Threat," Journal of Cybersecurity, 2022.