

# Phishing Simulation Report

Comprehensive security awareness analysis for your organization

Generated on November 14, 2025



Total Simulations



4

Emails sent to employees

Open Rate



50%

Employees who opened emails

Click Rate



50%

Employees who clicked scams

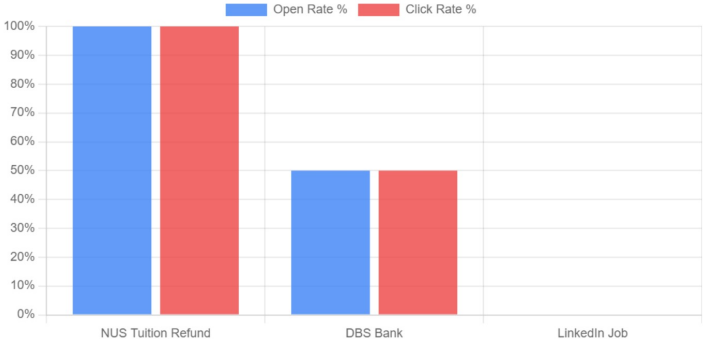
Total Scam Clicks



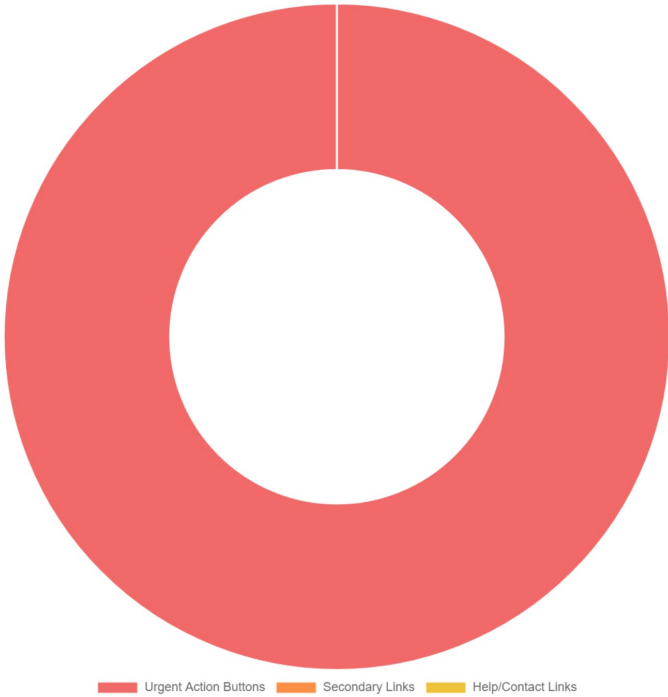
6

Total risky clicks recorded

## Template Performance



## Most Clicked Scam Types



## Employee Vulnerability Ranking

Employees ranked by total scam clicks (highest risk first)

High Risk Medium Risk Low Risk

#1



Demo  
thinkbeforeclick12@gmail.com

6 Scam Clicks  
High Risk Level

#2



TestUser1  
zouzhihuajosh@outlook.com

0 Scam Clicks  
Low Risk Level

## Scam Analysis & Prevention Guide

Detailed breakdown of scam types identified in phishing templates

### Scam Type 1: Urgent Action Buttons

"Verify My Identity Now", "Freeze Account", etc.

5

#### What is it?

Attackers create fake urgent buttons to pressure victims into immediate action, bypassing logical thinking.

#### How to prevent:

- Never click links in unexpected emails
- Always verify through official channels (call bank directly)
- Check sender email address carefully
- Legitimate organizations don't demand immediate action via email

### Scam Type 2: Secondary Action Links

0

 **What is it?**

Disguised as helpful links, these redirect to fake login pages to harvest credentials.

 **How to prevent:**

- Hover over links to see actual URL before clicking
- Look for misspelled domain names
- Use bookmarked official websites instead
- Enable 2-factor authentication on all accounts

 **Scam Type 3: Embedded Contact/Help Links**

0

"Click here for help", "Contact Support", etc.

 **What is it?**

These appear as legitimate support links but lead to phishing sites or trigger malware downloads.

 **How to prevent:**

- Search for official contact info separately
- Be suspicious of unsolicited "help" offers
- Check for HTTPS and valid SSL certificates
- Report suspicious emails to your IT department



**Recommendations for Improvement**

 **Immediate Actions**

- Provide additional training for high-risk employees
- Implement mandatory security awareness courses
- Enable 2FA for all company accounts
- Run monthly phishing simulations

 **Long-term Strategy**

- Establish a security-first culture
- Regular security policy updates
- Create an incident response plan
- Track improvement metrics quarterly