

# ALERTING USERS TO PHISHING THREATS: A COMPREHENSIVE EVALUATION OF WARNING TECHNIQUES

Bachelor Thesis by Yunus Emre Yavuz

---

Date: 25.06.2024

Examiner: Univ.-Prof. Dr. Florian Alt

Supervisors: Felix Dietz, M.Sc.; Dr. Verena Distler



## MAJOR THREAT: PHISHING



Phishing causing  
financial losses and  
trust issues

## MAJOR THREAT: PHISHING

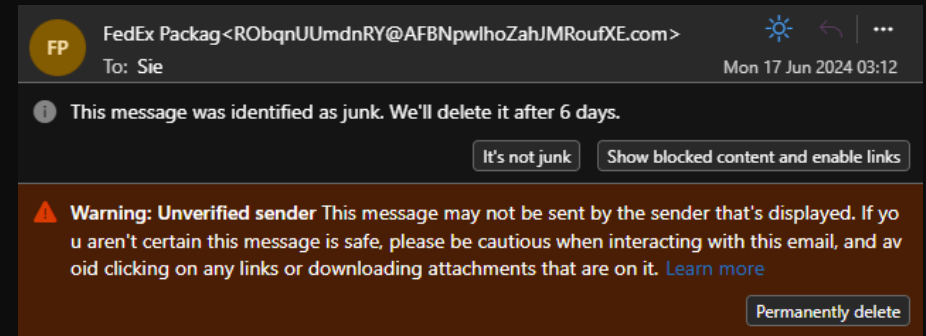


Phishing causing  
financial losses and  
trust issues

## WARNING ALERTS



Crucial defense  
mechanism against  
phishing attacks



## WHAT I HAVE DONE



- Designed and implemented phishing warnings
- Conducted a mixed-methods user study (N=16)
- Collected Eye Tracking Data + Qualitative Feedback

## RESEARCH QUESTIONS



- RQ1: How do users' perceptions differ regarding various phishing warnings, and which type is seen as the most effective?
  - *How do users perceive the usefulness of each warning type?*
  - *Which warning design do users prefer and why?*
- RQ2: What common gaze patterns emerge when users scan email content, and how can these patterns aid in strategically placing phishing warnings to maximize attention?

# RELATED WORK

COMBATTING  
PHISHING

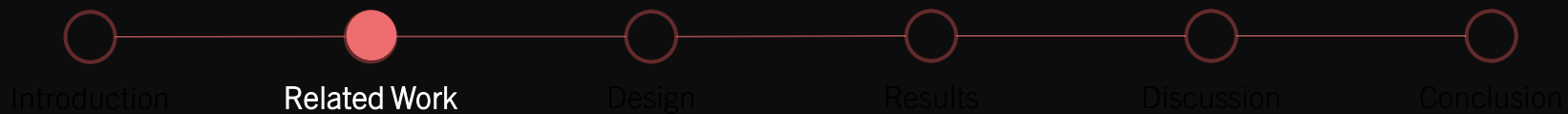


*Technical Strategies  
& User Education*

HUMAN  
FACTORS

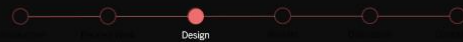
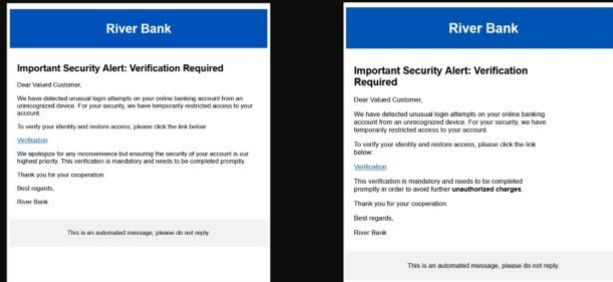


*Why does Phishing  
work?*



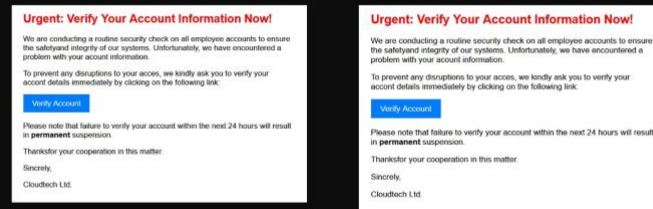
# WARNING DESIGNS

## GENERAL ALERTS



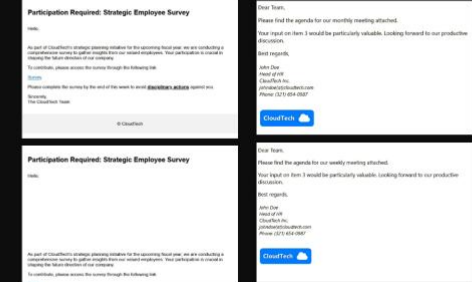
8

## TOOLTIP ON HOVER OVER LINK



9

## CONTENT SPECIFIC WARNINGS



10

# GENERAL ALERTS

## River Bank

### Important Security Alert: Verification Required

Dear Valued Customer,

We have detected unusual login attempts on your online banking account from an unrecognized device. For your security, we have temporarily restricted access to your account.

To verify your identity and restore access, please click the link below:

[Verification](#)

We apologize for any inconvenience but ensuring the security of your account is our highest priority. This verification is mandatory and needs to be completed promptly.

Thank you for your cooperation.

Best regards,

River Bank

This is an automated message, please do not reply.

## River Bank

### Important Security Alert: Verification Required

Dear Valued Customer,

We have detected unusual login attempts on your online banking account from an unrecognized device. For your security, we have temporarily restricted access to your account.

To verify your identity and restore access, please click the link below:

[Verification](#)

This verification is mandatory and needs to be completed promptly in order to avoid further **unauthorized charges**.

Thank you for your cooperation.

Best regards,

River Bank

This is an automated message, please do not reply.



Introduction



Related Work



Design



Results



Discussion



Conclusion



# TOOLTIP ON HOVER OVER LINK

## Urgent: Verify Your Account Information Now!

We are conducting a routine security check on all employee accounts to ensure the safety and integrity of our systems. Unfortunately, we have encountered a problem with your account information.

To prevent any disruptions to your access, we kindly ask you to verify your account details immediately by clicking on the following link:

Verify Account

Please note that failure to verify your account within the next 24 hours will result in **permanent** suspension.

Thank you for your cooperation in this matter.

Sincerely,

Cloudtech Ltd.

## Urgent: Verify Your Account Information Now!

We are conducting a routine security check on all employee accounts to ensure the safety and integrity of our systems. Unfortunately, we have encountered a problem with your account information.

To prevent any disruptions to your access, we kindly ask you to verify your account details immediately by clicking on the following link:

Verify Account

Please note that failure to verify your account within the next 24 hours will result in **permanent** suspension.

Thank you for your cooperation in this matter.

Sincerely,

Cloudtech Ltd.

# CONTENT SPECIFIC WARNINGS

**Participation Required: Strategic Employee Survey**

Hello,

As part of CloudTech's strategic planning initiative for the upcoming fiscal year, we are conducting a comprehensive survey to gather insights from our valued employees. Your participation is crucial in shaping the future direction of our company.

To contribute, please access the survey through the following link:

[Survey](#)

Please complete the survey by the end of this week to avoid **disciplinary actions** against you.

Sincerely,  
The CloudTech Team

© CloudTech

**Participation Required: Strategic Employee Survey**

Hello,

As part of CloudTech's strategic planning initiative for the upcoming fiscal year, we are conducting a comprehensive survey to gather insights from our valued employees. Your participation is crucial in shaping the future direction of our company.

To contribute, please access the survey through the following link:

[Survey](#)


Dear Team,

Please find the agenda for our monthly meeting attached.

Your input on item 3 would be particularly valuable. Looking forward to our productive discussion.

Best regards,

*John Doe*  
Head of HR  
CloudTech Inc.  
johndoe(at)cloudtech.com  
Phone: (321) 654-0987

**CloudTech** 


Dear Team,

Please find the agenda for our weekly meeting attached.

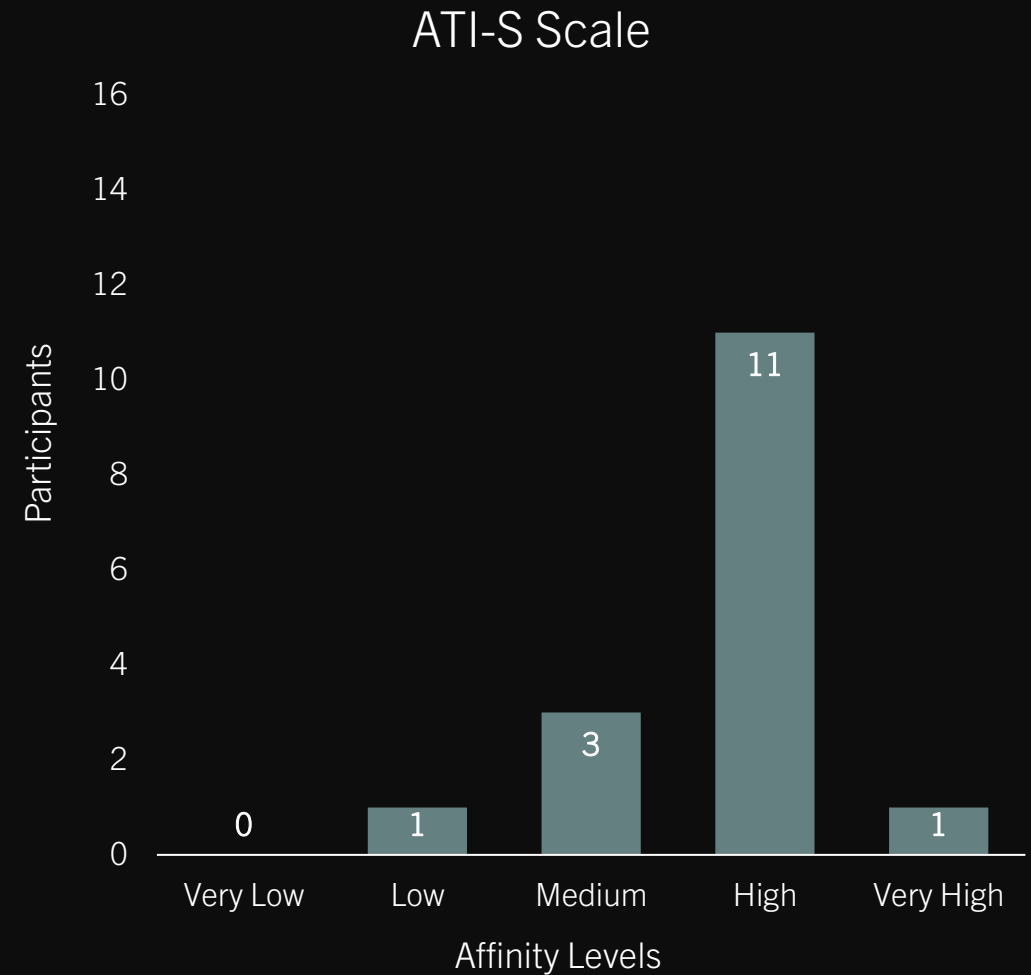
Your input on item 3 would be particularly valuable. Looking forward to our productive discussion.

Best regards,

*John Doe*  
Head of HR  
CloudTech Inc.  
johndoe(at)cloudtech.com  
Phone: (321) 654-0987

**CloudTech** 

Demographics		Total (N=16)	%
Age	20 - 29	13	81,25
	30 - 39	2	12,5
	40+	1	6,25
Gender	Male	10	62,5
	Female	6	37,5
	Non-binary	0	0
	Prefer not to tell	0	0
Education	Doctorate degree	1	6,25
	Graduate degree	2	12,5
	Undergraduate degree	9	56,25
	High school diploma	4	25
	Secondary education	0	0
	Other	0	0
Profession	Student	13	87,5
	Research Assistant	1	6,25
	Retiree	1	6,25



# USER FEEDBACK



- Attention grabbing
- Details are appreciated for their educational value



- Legibility & Animations
- Side-placed Warnings

**⚠ Warning:** This greeting is unusual for messages from "@cloudtech". For reference, see past greetings used in communications:

Email dated 01/01/24: "Dear CloudTech Employee, ..."

Email dated 01/12/23: "Dear CloudTech Employee, ..."

Email dated 10/11/23: "Dear CloudTech Employee, ..."

## Participation Required: Strategic Employee Survey

Hello,

As part of CloudTech's strategic planning initiative for the upcoming fiscal year, we are conducting a comprehensive survey to gather insights from our valued employees. Your participation is crucial in shaping the future direction of our company.

To contribute, please access the survey through the following link:

[Survey](#)

Please complete the survey by the end of this week to avoid **disciplinary actions** against you.

Sincerely,  
The CloudTech Team

© CloudTech

## River Bank

### Important Security Alert: Verification Required

Dear Valued Customer,

We have detected unusual login attempts on your online banking account from an unrecognized device. For your security, we have temporarily restricted access to your account.

To verify your identity and restore access, please click the link below.

[Verification](#)

This verification is mandatory and needs to be completed promptly in order to avoid further **unauthorized charges**.

Thank you for your cooperation.

Best regards,

River Bank

This is an automated message, please do not reply.

# INCORPORATING USER FEEDBACK

**⚠ Warning:** This greeting is unusual for messages from "@cloudtech". For reference, see past greetings used in communications:

Email dated 01/01/24: "Dear CloudTech Employee, ..."

Email dated 01/12/23: "Dear CloudTech Employee, ..."

Email dated 10/11/23: "Dear CloudTech Employee, ..."

**⚠ Warning: Potential phishing attempt!**

This greeting is unusual for messages from CloudTech. For reference, see past greetings used in communications:

01/01/24: "Dear CloudTech Employee, ..." ➡

01/12/23: "Dear CloudTech Employee, ..." ➡

10/11/23: "Dear CloudTech Employee, ..." ➡

# EYE TRACKING RESULTS



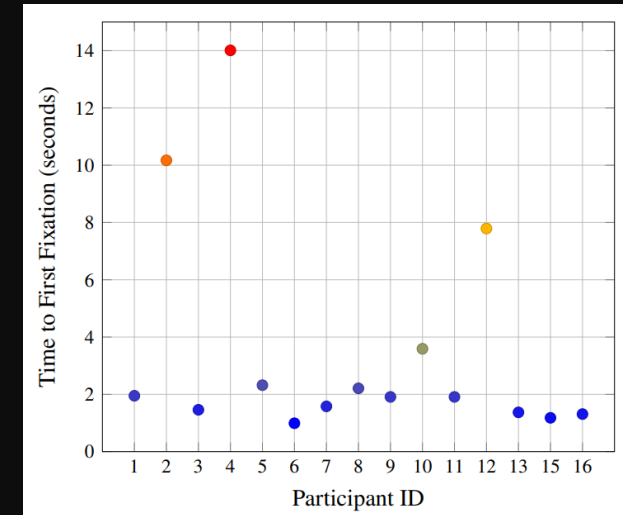
Hypothesis 1: *Delayed slide-in animations draw more attention* → *no significant difference observed*



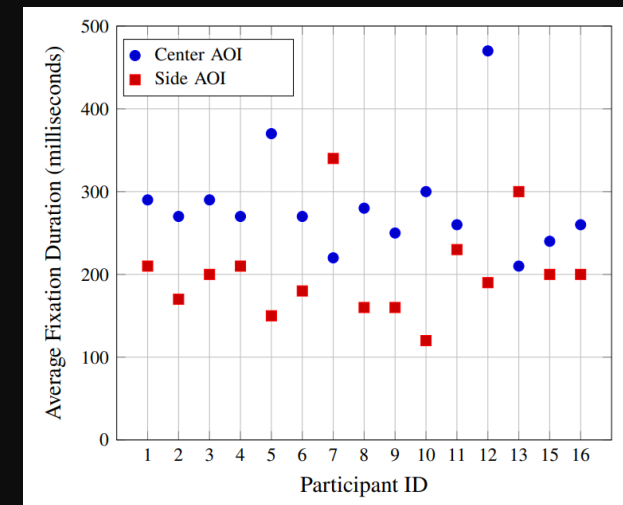
Hypothesis 2: *Side-placed warnings will be noticed later*  
→ *Median TtFF ~2s (Comparison Top-placed: ~1s)*



Hypothesis 3: *Body-integrated warnings will hold user attention for longer periods* → *Supported by a consistently longer Avg. Fixation Duration*



*Time to First Fixation for Side-placed Warnings*



*Avg. Fixation Duration: Comparing Center and Side AOI*

# EMERGING THEMES & BEST PRACTICES

## ATTENTION - GRABBING

*Animation Balance:  
Capture attention, avoid  
sensory overload with  
moderate animations*

## CLARITY

*Readability: Clear, legible  
text with contrasting  
background*

## TRUST

*User Confidence: Clear  
distinction of safe  
interactive elements*

## CONTEXTUAL INFORMATION

*Contextual Details:  
Explain why the email is  
flagged*

*Educational Value: Teach  
Users how to detect  
future attempts*

## INCORPORATING USER FEEDBACK

*Continuous Testing:  
Regular user feedback  
and design adjustments*

# RQ1: USERS' PERCEPTIONS: MOST EFFECTIVE & HELPFUL WARNING

## GENERAL PREFERENCES

*Visibility and Informativeness*

*Seamless Integration*

*Immediate Attention*

*Long-Term Recognition*

Warning Type	User Feedback
Tooltip on Hover	Very positive; users felt it was very effective and helpful
Content-Specific	Positive; users appreciated their specificity and novelty
General Alerts	Less favorable; often overlooked, too generic



# RQ2: COMMON GAZE PATTERNS AND OPTIMAL WARNING PLACEMENT

## WARNING PLACEMENT

*Peripheral Warnings:  
Noticed later and  
engaged with less.*

*Warnings in the center  
are engaged with more  
extensively.*

## SUMMARY

*Central Focus: Users  
naturally focus on the  
central area*

*→ Central placement  
for crucial warnings*

# LIMITATIONS

PARTICIPANT  
DIVERSITY &  
SAMPLE SIZE



STUDY SETUP



# CONCLUSION



---



Conclusion

# KEY TAKEAWAYS



Visibility is Crucial: Immediate and central placement of warnings ensures they are noticed and acted upon.



Informative Warnings: Providing context and reasoning in warnings helps users understand and recognize threats.



User-Centric Design: Incorporate user feedback for continuous improvement.



Broader Testing Needed

