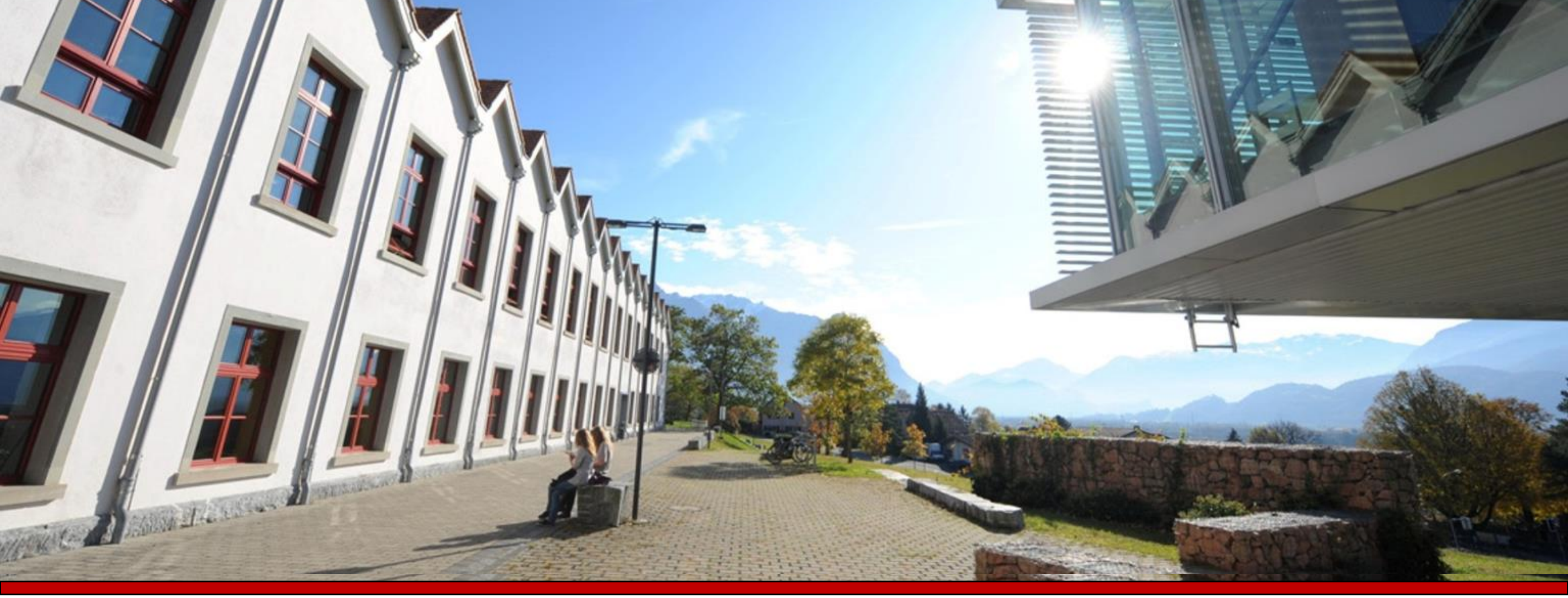


Hanoi – August 29th, 2025

ACM Asia Conference on Computer and Communications Security

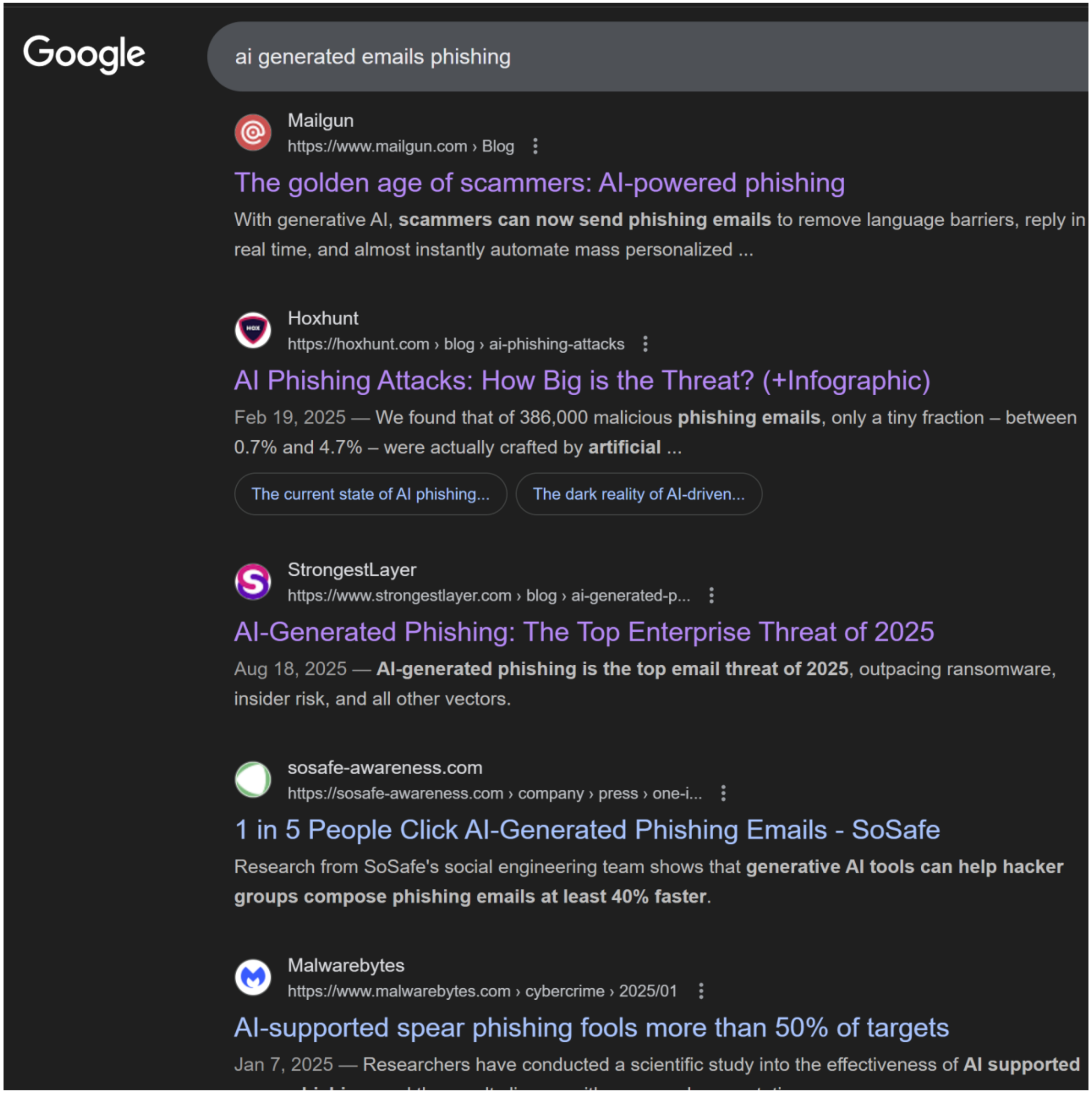
The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails Against Organizations

Marie Weinz, Luca Allodi, Nicola Zannone, Giovanni Apruzzese

UNIVERSITÄT LIECHTENSTEIN

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

LLM-generated Phishing Emails



ai generated emails phishing

Mailgun
https://www.mailgun.com › Blog

The golden age of scammers: AI-powered phishing

With generative AI, **scammers can now send phishing emails** to remove language barriers, reply in real time, and almost instantly automate mass personalized ...

Hoxhunt
https://hoxhunt.com › blog › ai-phishing-attacks

AI Phishing Attacks: How Big is the Threat? (+Infographic)

Feb 19, 2025 — We found that of 386,000 malicious **phishing emails**, only a tiny fraction – between 0.7% and 4.7% – were actually crafted by **artificial** ...

The current state of AI phishing... | The dark reality of AI-driven...

StrongestLayer
https://www.strongestlayer.com › blog › ai-generated-p...

AI-Generated Phishing: The Top Enterprise Threat of 2025

Aug 18, 2025 — **AI-generated phishing is the top email threat of 2025**, outpacing ransomware, insider risk, and all other vectors.

sosafe-awareness.com
https://sosafe-awareness.com › company › press › one-i...

1 in 5 People Click AI-Generated Phishing Emails - SoSafe

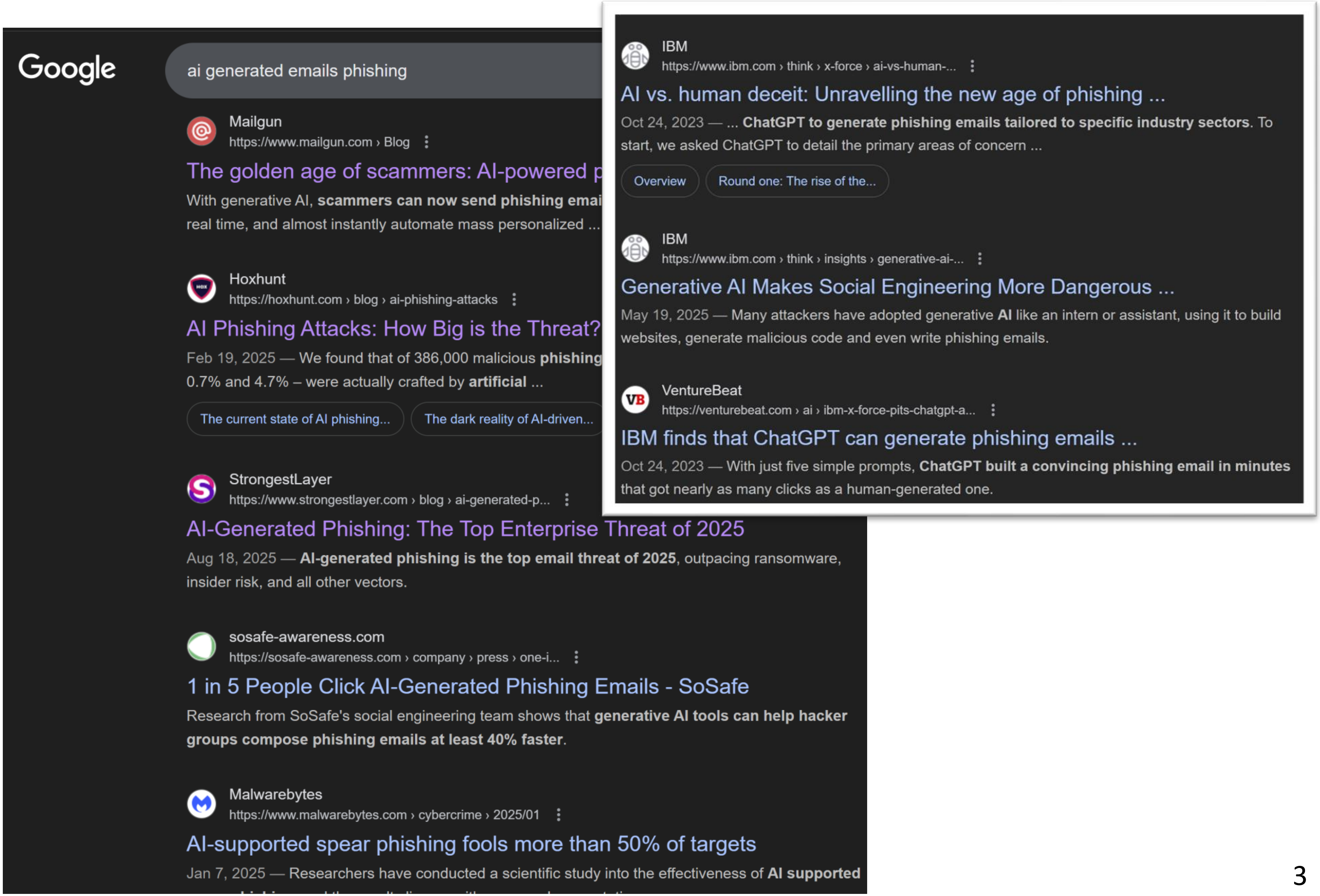
Research from SoSafe's social engineering team shows that **generative AI tools can help hacker groups compose phishing emails at least 40% faster**.

Malwarebytes
https://www.malwarebytes.com › cybercrime › 2025/01

AI-supported spear phishing fools more than 50% of targets

Jan 7, 2025 — Researchers have conducted a scientific study into the effectiveness of **AI supported**

LLM-generated Phishing Emails



ai generated emails phishing

Mailgun
https://www.mailgun.com › Blog

The golden age of scammers: AI-powered p

With generative AI, **scammers can now send phishing emai** real time, and almost instantly automate mass personalized ...

Hoxhunt
https://hoxhunt.com › blog › ai-phishing-attacks

AI Phishing Attacks: How Big is the Threat?

Feb 19, 2025 — We found that of 386,000 malicious **phishing** 0.7% and 4.7% – were actually crafted by **artificial** ...

The current state of AI phishing... | The dark reality of AI-driven...

StrongestLayer
https://www.strongestlayer.com › blog › ai-generated-p...

AI-Generated Phishing: The Top Enterprise Threat of 2025

Aug 18, 2025 — **AI-generated phishing is the top email threat of 2025**, outpacing ransomware, insider risk, and all other vectors.

sosafe-awareness.com
https://sosafe-awareness.com › company › press › one-i...

1 in 5 People Click AI-Generated Phishing Emails - SoSafe

Research from SoSafe's social engineering team shows that **generative AI tools can help hacker groups compose phishing emails at least 40% faster**.

Malwarebytes
https://www.malwarebytes.com › cybercrime › 2025/01

AI-supported spear phishing fools more than 50% of targets

Jan 7, 2025 — Researchers have conducted a scientific study into the effectiveness of **AI supported**

IBM
https://www.ibm.com › think › x-force › ai-vs-human-...

AI vs. human deceit: Unravelling the new age of phishing ...

Oct 24, 2023 — ... **ChatGPT to generate phishing emails tailored to specific industry sectors**. To start, we asked ChatGPT to detail the primary areas of concern ...

Overview | Round one: The rise of the...

IBM
https://www.ibm.com › think › insights › generative-ai-...

Generative AI Makes Social Engineering More Dangerous ...

May 19, 2025 — Many attackers have adopted generative **AI** like an intern or assistant, using it to build websites, generate malicious code and even write phishing emails.

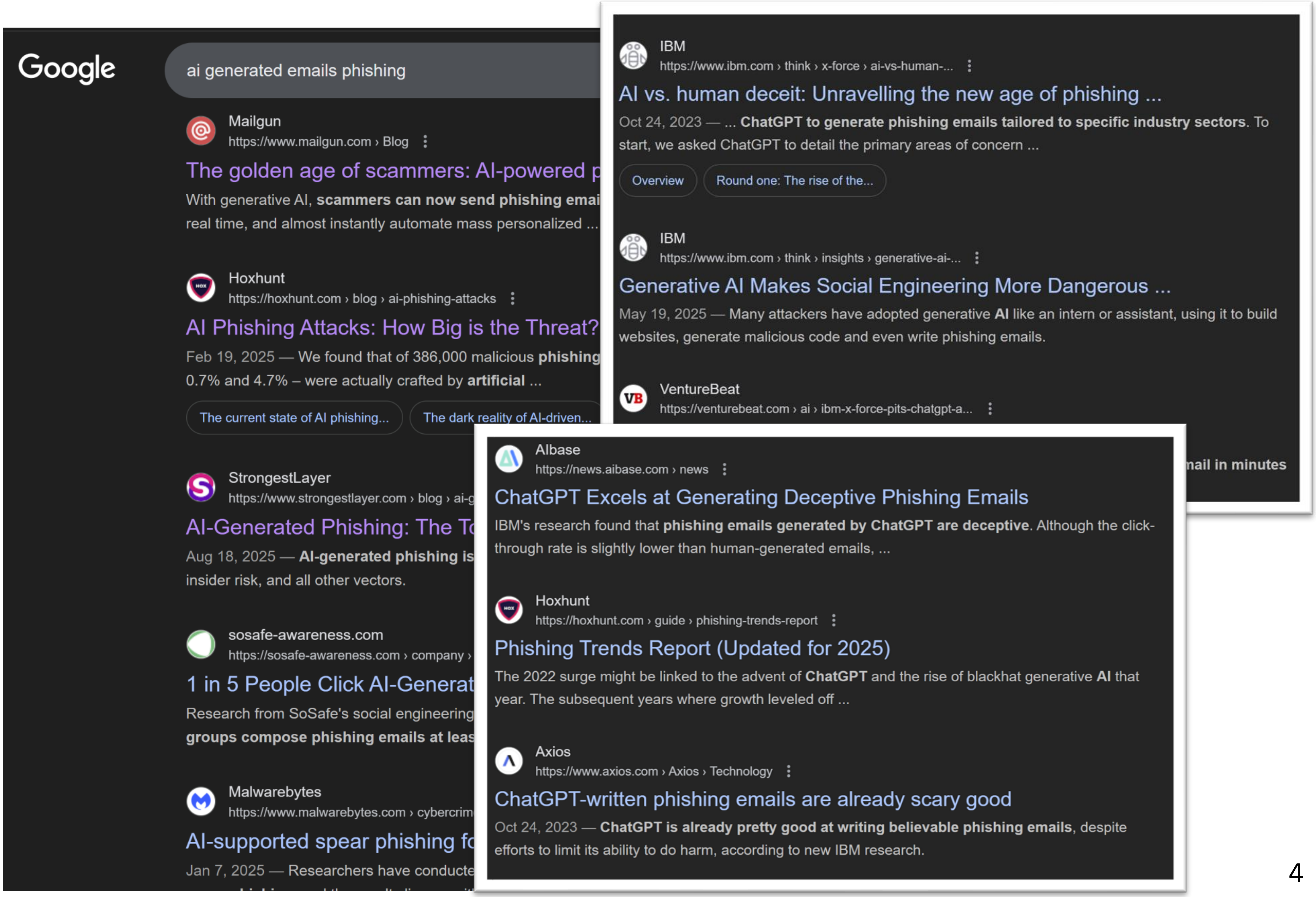
VentureBeat
https://venturebeat.com › ai › ibm-x-force-pits-chatgpt-a...

IBM finds that ChatGPT can generate phishing emails ...

Oct 24, 2023 — With just five simple prompts, **ChatGPT built a convincing phishing email in minutes** that got nearly as many clicks as a human-generated one.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

LLM-generated Phishing Emails



Mailgun
https://www.mailgun.com › Blog
The golden age of scammers: AI-powered p
With generative AI, **scammers can now send phishing emai**
real time, and almost instantly automate mass personalized ...

Hoxhunt
https://hoxhunt.com › blog › ai-phishing-attacks
AI Phishing Attacks: How Big is the Threat?
Feb 19, 2025 — We found that of 386,000 malicious **phishing**
0.7% and 4.7% – were actually crafted by **artificial** ...
The current state of AI phishing... | The dark reality of AI-driven...

StrongestLayer
https://www.strongestlayer.com › blog › ai-g
AI-Generated Phishing: The To
Aug 18, 2025 — **AI-generated phishing is**
insider risk, and all other vectors.

sosafe-awareness.com
https://sosafe-awareness.com › company ›
1 in 5 People Click AI-Generat
Research from SoSafe's social engineering
groups compose phishing emails at leas

Malwarebytes
https://www.malwarebytes.com › cybercrim
AI-supported spear phishing fo
Jan 7, 2025 — Researchers have conducte

IBM
https://www.ibm.com › think › x-force › ai-vs-human-...
AI vs. human deceit: Unravelling the new age of phishing ...
Oct 24, 2023 — ... **ChatGPT to generate phishing emails tailored to specific industry sectors**. To start, we asked ChatGPT to detail the primary areas of concern ...
Overview | Round one: The rise of the...

IBM
https://www.ibm.com › think › insights › generative-ai-...
Generative AI Makes Social Engineering More Dangerous ...
May 19, 2025 — Many attackers have adopted generative **AI** like an intern or assistant, using it to build websites, generate malicious code and even write phishing emails.

VentureBeat
https://venturebeat.com › ai › ibm-x-force-pits-chatgpt-a...
nail in minutes

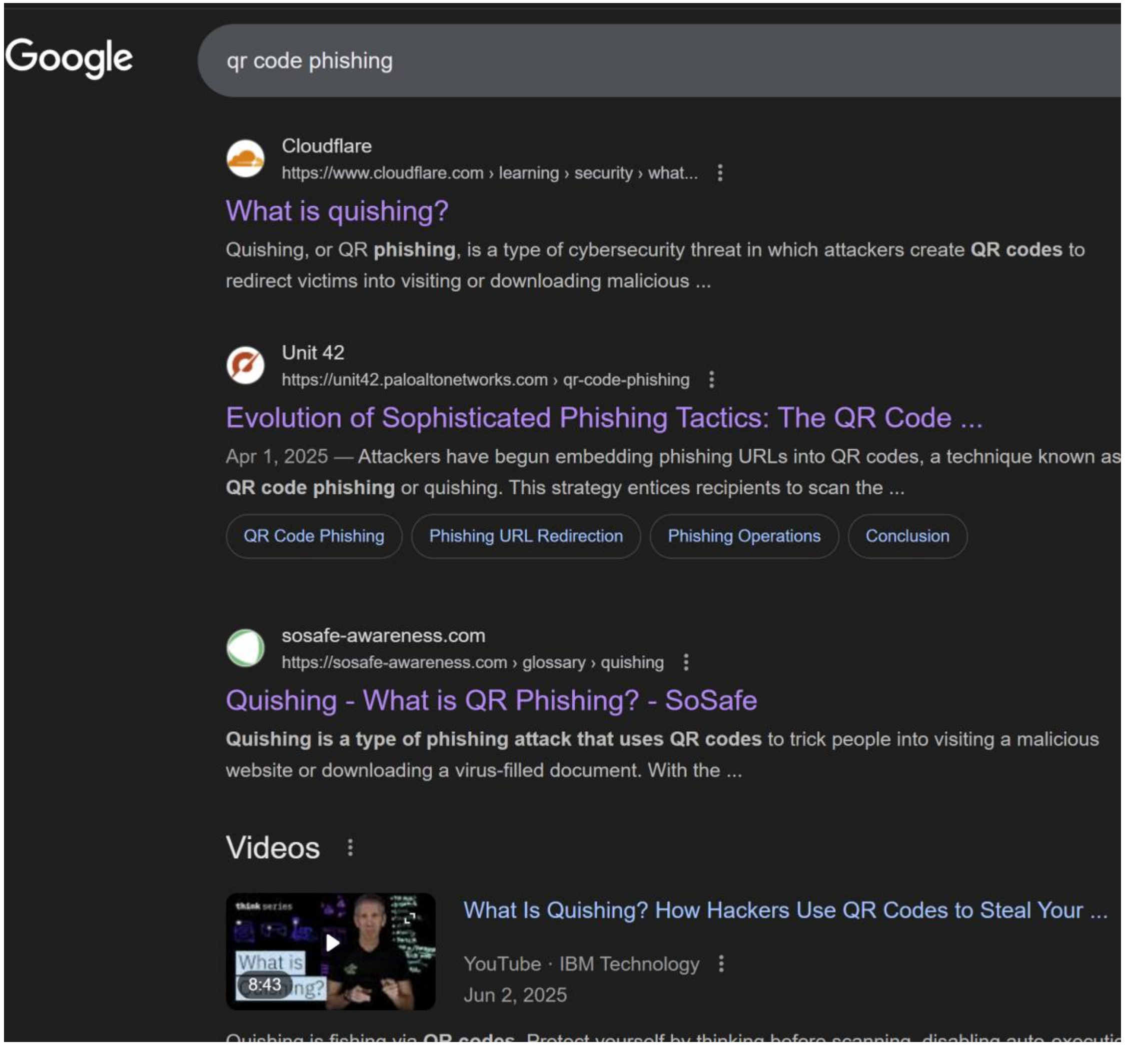
Albase
https://news.aibase.com › news
ChatGPT Excels at Generating Deceptive Phishing Emails
IBM's research found that **phishing emails generated by ChatGPT are deceptive**. Although the click-through rate is slightly lower than human-generated emails, ...

Hoxhunt
https://hoxhunt.com › guide › phishing-trends-report
Phishing Trends Report (Updated for 2025)
The 2022 surge might be linked to the advent of **ChatGPT** and the rise of blackhat generative **AI** that year. The subsequent years where growth leveled off ...

Axios
https://www.axios.com › Axios › Technology
ChatGPT-written phishing emails are already scary good
Oct 24, 2023 — **ChatGPT is already pretty good at writing believable phishing emails**, despite efforts to limit its ability to do harm, according to new IBM research.

Quishing?

Quishing Emails are popular nowadays



qr code phishing

Cloudflare
https://www.cloudflare.com › learning › security › what...

What is quishing?

Quishing, or QR **phishing**, is a type of cybersecurity threat in which attackers create **QR codes** to redirect victims into visiting or downloading malicious ...

Unit 42
https://unit42.paloaltonetworks.com › qr-code-phishing

Evolution of Sophisticated Phishing Tactics: The QR Code ...

Apr 1, 2025 — Attackers have begun embedding phishing URLs into QR codes, a technique known as **QR code phishing** or quishing. This strategy entices recipients to scan the ...

sosafe-awareness.com
https://sosafe-awareness.com › glossary › quishing

Quishing - What is QR Phishing? - SoSafe

Quishing is a type of phishing attack that uses QR codes to trick people into visiting a malicious website or downloading a virus-filled document. With the ...

Videos

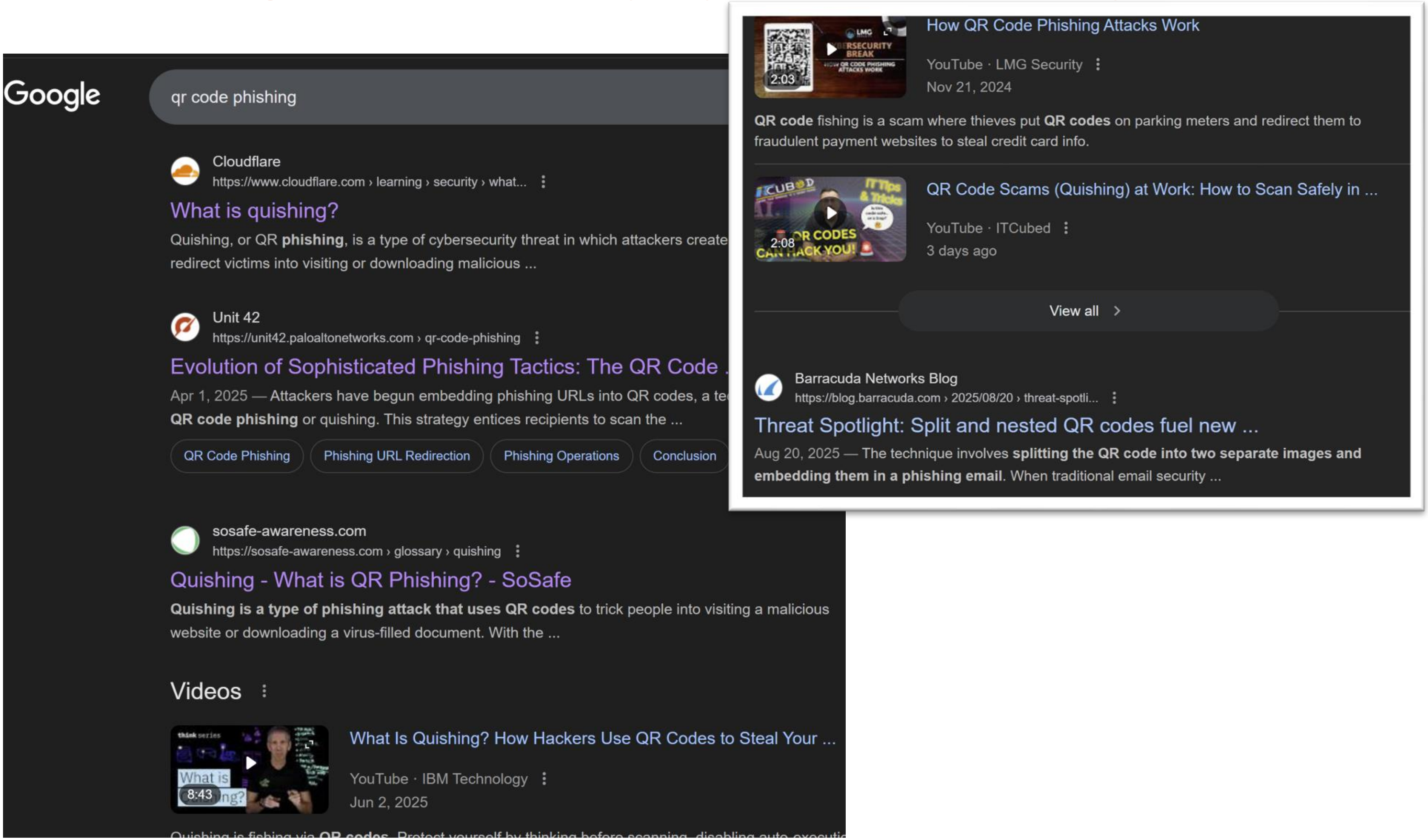
What Is Quishing? How Hackers Use QR Codes to Steal Your ...

YouTube · IBM Technology
Jun 2, 2025

Quishing is fishing via **QR codes**. Protect yourself by thinking before scanning, disabling auto-executi

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Quishing Emails are popular nowadays



Google

qr code phishing

Cloudflare
https://www.cloudflare.com › learning › security › what...

What is quishing?

Quishing, or QR **phishing**, is a type of cybersecurity threat in which attackers create redirect victims into visiting or downloading malicious ...

Unit 42
https://unit42.paloaltonetworks.com › qr-code-phishing

Evolution of Sophisticated Phishing Tactics: The QR Code .

Apr 1, 2025 — Attackers have begun embedding phishing URLs into QR codes, a te **QR code phishing** or quishing. This strategy entices recipients to scan the ...

QR Code Phishing | Phishing URL Redirection | Phishing Operations | Conclusion

sosafe-awareness.com
https://sosafe-awareness.com › glossary › quishing

Quishing - What is QR Phishing? - SoSafe

Quishing is a type of phishing attack that uses QR codes to trick people into visiting a malicious website or downloading a virus-filled document. With the ...

Videos

What Is Quishing? How Hackers Use QR Codes to Steal Your ...
YouTube · IBM Technology
Jun 2, 2025
8:43

Quishing is fishing via QR codes. Protect yourself by thinking before scanning, disabling auto-executi

How QR Code Phishing Attacks Work
YouTube · LMG Security
Nov 21, 2024
2:03

QR code fishing is a scam where thieves put **QR codes** on parking meters and redirect them to fraudulent payment websites to steal credit card info.

QR Code Scams (Quishing) at Work: How to Scan Safely in ...
YouTube · ITCubed
3 days ago
2:08

View all >

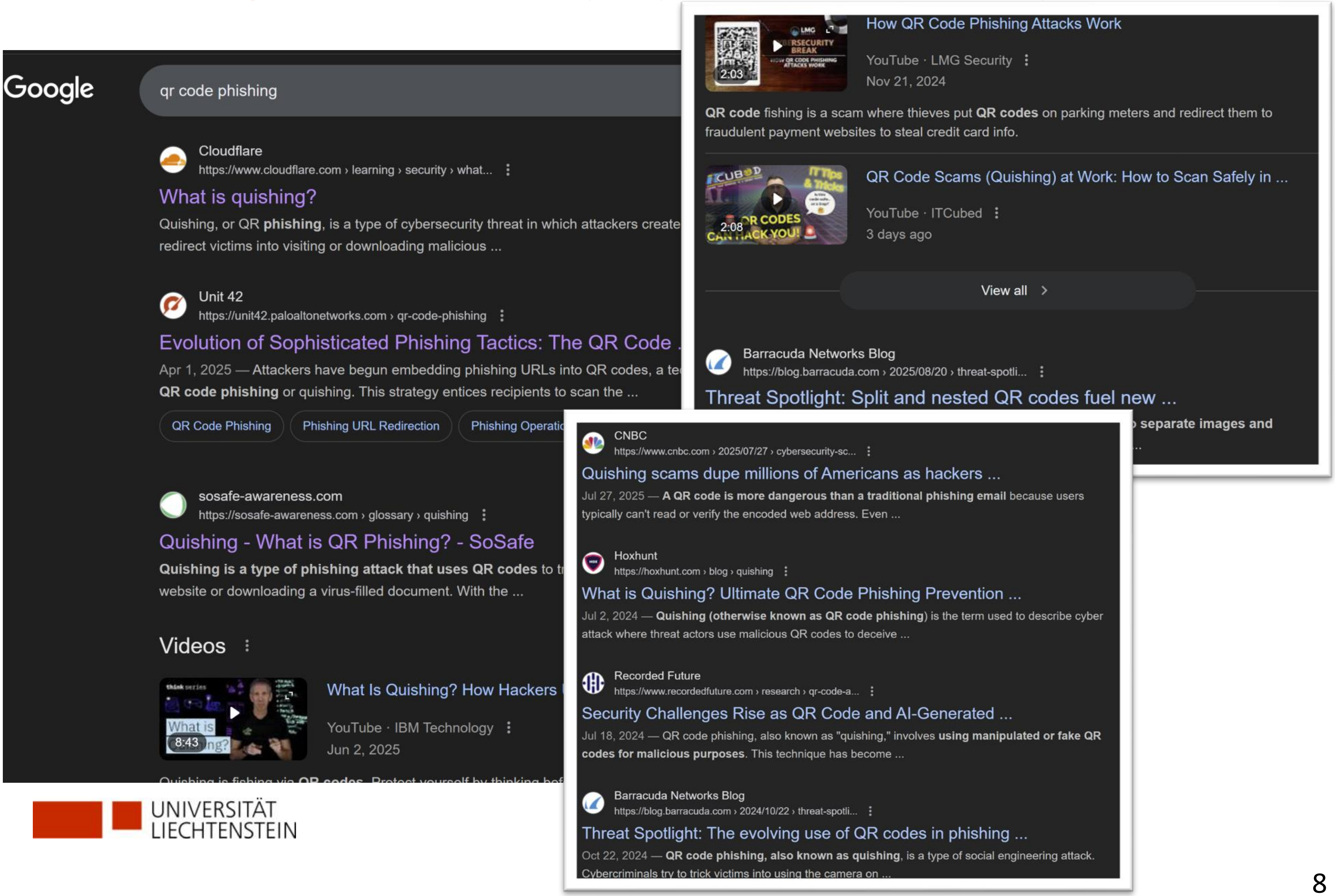
Barracuda Networks Blog
https://blog.barracuda.com › 2025/08/20 › threat-spotli...

Threat Spotlight: Split and nested QR codes fuel new ...

Aug 20, 2025 — The technique involves **splitting the QR code into two separate images and embedding them in a phishing email**. When traditional email security ...

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Quishing Emails are popular nowadays



Google

qr code phishing

Cloudflare
https://www.cloudflare.com › learning › security › what...

What is quishing?

Quishing, or QR **phishing**, is a type of cybersecurity threat in which attackers create redirect victims into visiting or downloading malicious ...

Unit 42
https://unit42.paloaltonetworks.com › qr-code-phishing

Evolution of Sophisticated Phishing Tactics: The QR Code

Apr 1, 2025 — Attackers have begun embedding phishing URLs into QR codes, a te **QR code phishing** or quishing. This strategy entices recipients to scan the ...

sosafe-awareness.com
https://sosafe-awareness.com › glossary › quishing

Quishing - What is QR Phishing? - SoSafe

Quishing is a type of phishing attack that uses QR codes to t website or downloading a virus-filled document. With the ...

Videos

What Is Quishing? How Hackers
YouTube · IBM Technology
Jun 2, 2025

Quishing is fishing via **QR codes**. Protect yourself by thinking bef

How QR Code Phishing Attacks Work
YouTube · LMG Security
Nov 21, 2024

QR code fishing is a scam where thieves put **QR codes** on parking meters and redirect them to fraudulent payment websites to steal credit card info.

QR Code Scams (Quishing) at Work: How to Scan Safely in ...
YouTube · ITCubed
3 days ago

Barracuda Networks Blog
https://blog.barracuda.com › 2025/08/20 › threat-spotli...

Threat Spotlight: Split and nested QR codes fuel new ...

separate images and

CNBC
https://www.cnbc.com › 2025/07/27 › cybersecurity-sc...

Quishing scams dupe millions of Americans as hackers ...

Jul 27, 2025 — **A QR code is more dangerous than a traditional phishing email** because users typically can't read or verify the encoded web address. Even ...

Hoxhunt
https://hoxhunt.com › blog › quishing

What is Quishing? Ultimate QR Code Phishing Prevention ...

Jul 2, 2024 — **Quishing (otherwise known as QR code phishing)** is the term used to describe cyber attack where threat actors use malicious QR codes to deceive ...

Recorded Future
https://www.recordedfuture.com › research › qr-code-a...

Security Challenges Rise as QR Code and AI-Generated ...

Jul 18, 2024 — QR code phishing, also known as "quishing," involves **using manipulated or fake QR codes for malicious purposes**. This technique has become ...

Barracuda Networks Blog
https://blog.barracuda.com › 2024/10/22 › threat-spotli...

Threat Spotlight: The evolving use of QR codes in phishing ...

Oct 22, 2024 — **QR code phishing, also known as quishing**, is a type of social engineering attack. Cybercriminals try to trick victims into using the camera on ...

Why are Quishing emails problematic?

Why are Quishing emails problematic?

→ **Because Quishing emails bypass phishing filters**

Why are Quishing emails problematic?

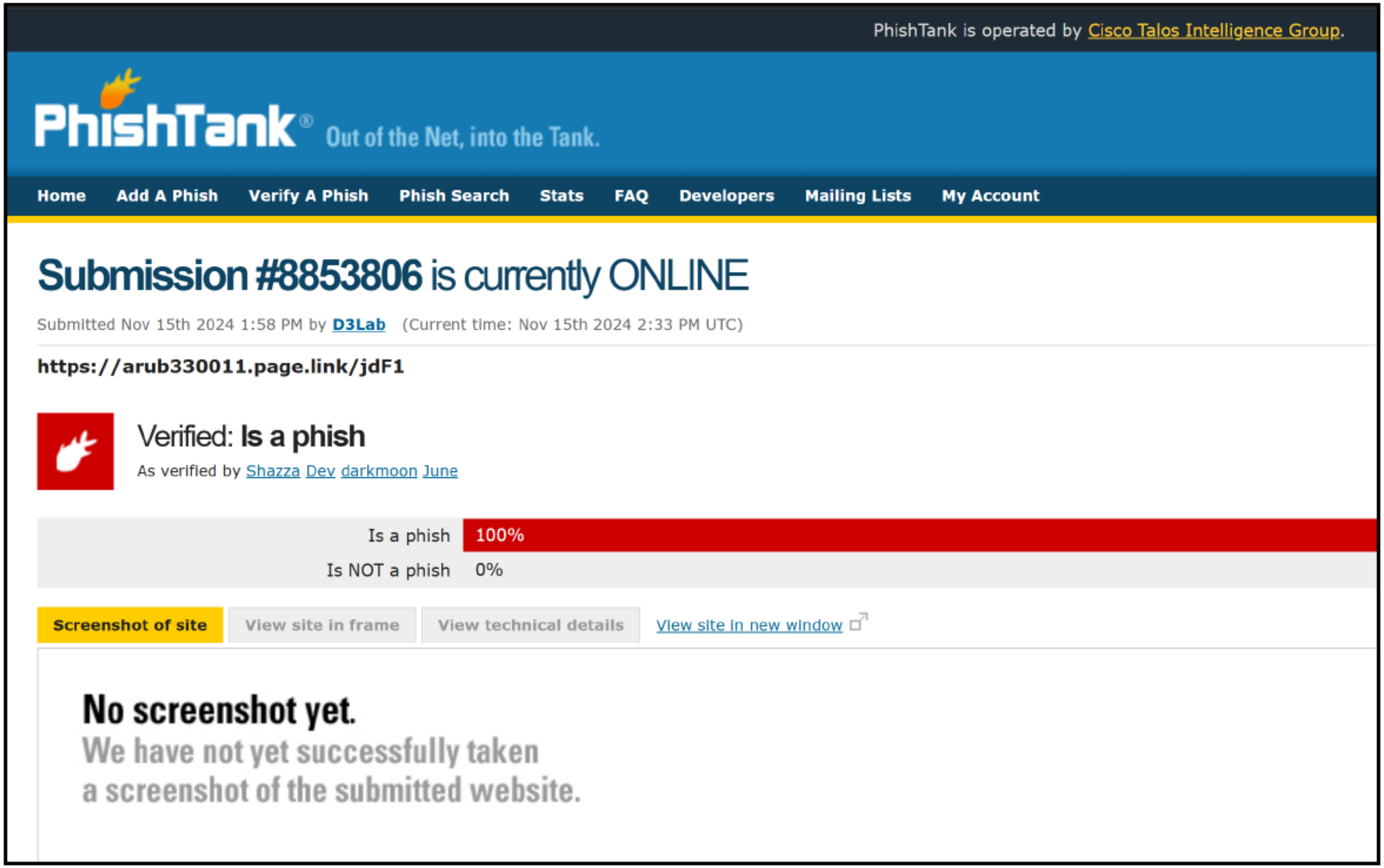
→ **Because Quishing emails bypass phishing filters**

…and we tested this!

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Why are Quishing emails problematic?

Test



PhishTank is operated by Cisco Talos Intelligence Group.

Submission #8853806 is currently ONLINE

Submitted Nov 15th 2024 1:58 PM by **D3Lab** (Current time: Nov 15th 2024 2:33 PM UTC)

https://arub330011.page.link/jdF1

Verified: **Is a phish**

As verified by Shazza Dev darkmoon June

Is a phish	100%
Is NOT a phish	0%

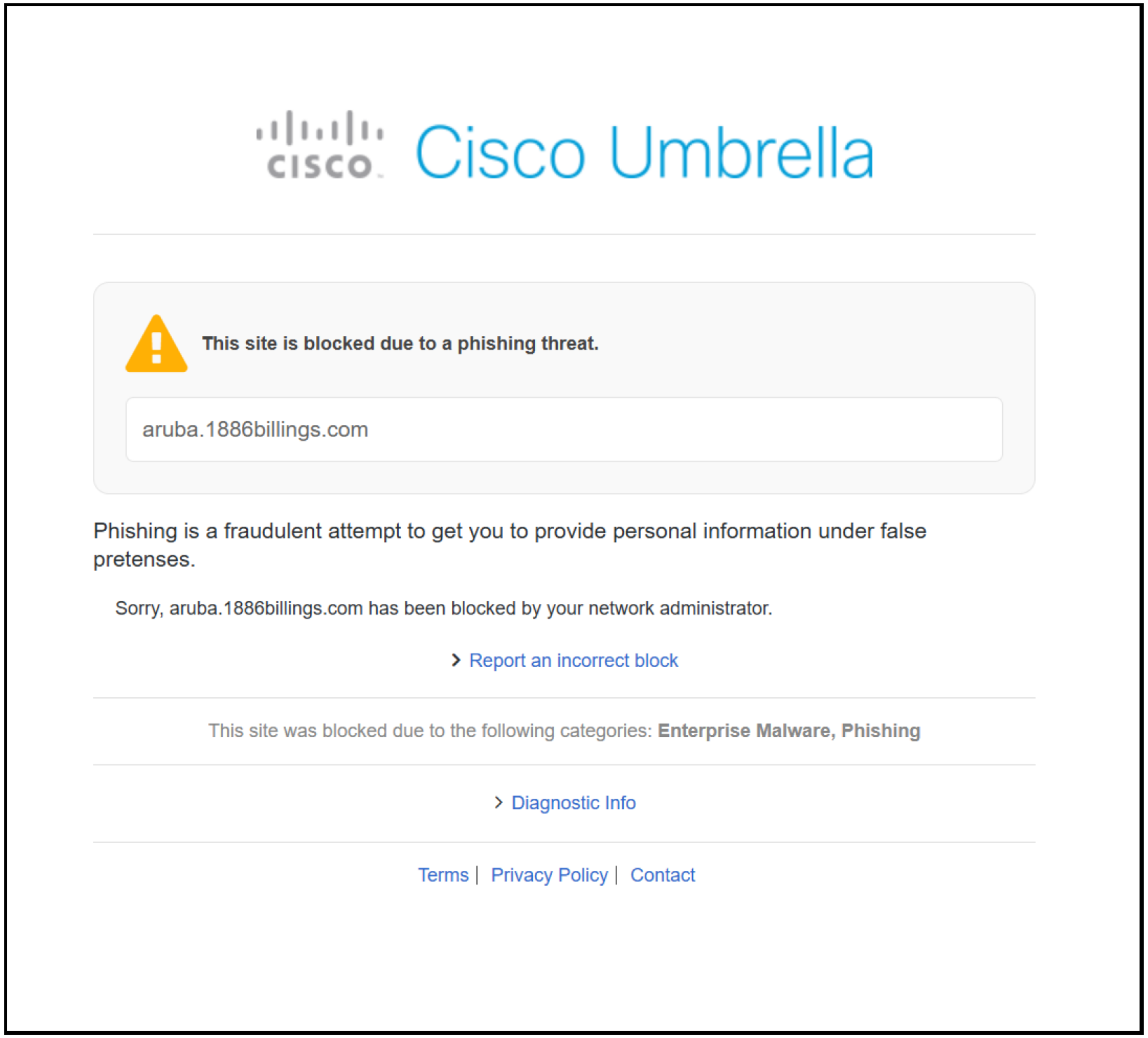
No screenshot yet.
We have not yet successfully taken
a screenshot of the submitted website.

(a) Details of the malicious URL (https://arub330011.page.link/jdF1) according to Phishtank [7] (in November 2024).

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Why are Quishing emails problematic?

Test



Cisco Umbrella

This site is blocked due to a phishing threat.

aruba.1886billings.com

Phishing is a fraudulent attempt to get you to provide personal information under false pretenses.

Sorry, aruba.1886billings.com has been blocked by your network administrator.

> Report an incorrect block

This site was blocked due to the following categories: **Enterprise Malware, Phishing**

> Diagnostic Info

Terms | Privacy Policy | Contact

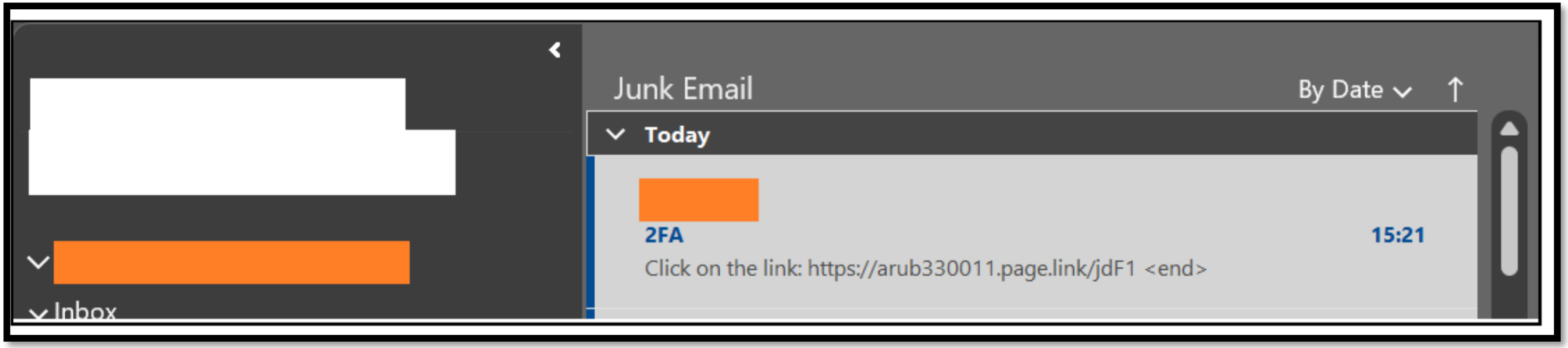
(c) Verification that the URL was known to be malicious by well-known providers (e.g., CISCO).

(a) Detail
tank [7] (

g to Phish-

Why are Quishing emails problematic?

Test



[redacted]

[redacted]

Inbox

Junk Email

By Date

Today

[redacted]

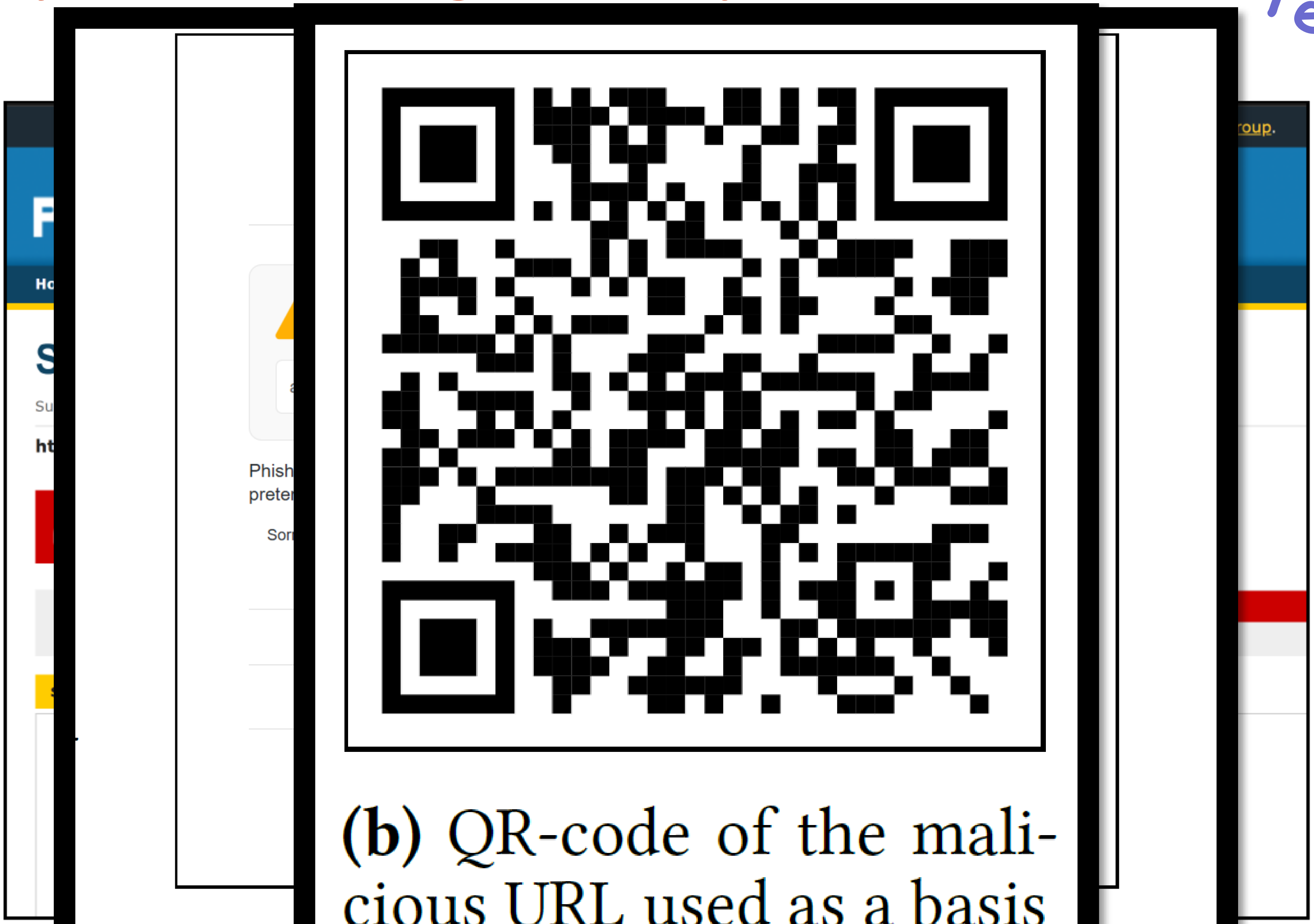
2FA 15:21

Click on the link: https://arub330011.page.link/jdF1 <end>

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Why are Quishing emails problematic?

Test



(b) QR-code of the malicious URL used as a basis for this experiment.

(a) Detail
tank [7] (

(c) Verifica
well-know

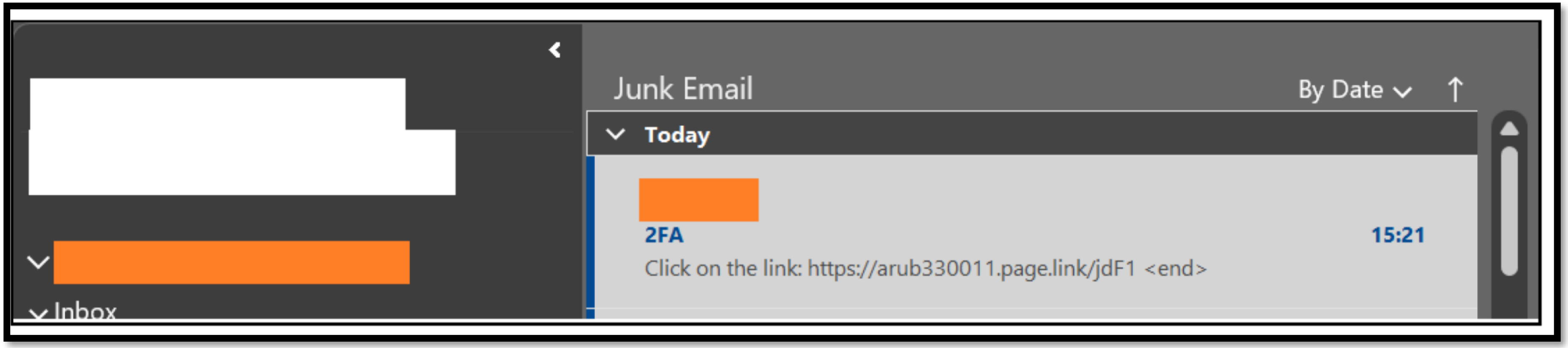
ous by

g to Phish-

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Why are Quishing emails problematic?

Test



[redacted]

[redacted]

Inbox

Junk Email

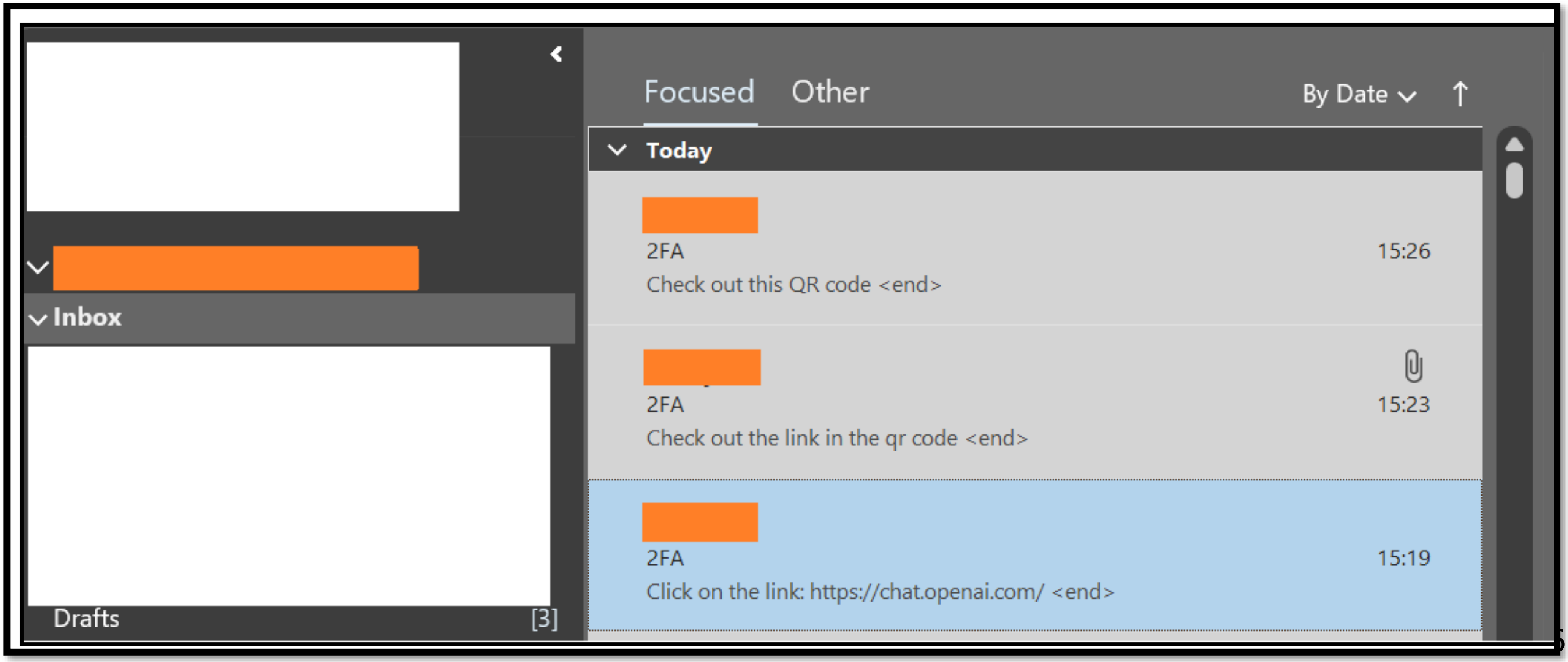
By Date

Today

[redacted]

2FA **15:21**

Click on the link: https://arub330011.page.link/jdF1 <end>



[redacted]

[redacted]

Inbox

[redacted]

Drafts [3]

Focused Other

By Date

Today

[redacted]

2FA 15:26

Check out this QR code <end>

[redacted]

2FA 15:23

Check out the link in the qr code <end>

[redacted]

2FA 15:19

Click on the link: https://chat.openai.com/ <end>

Are Quishing emails *truly* problematic?

Quishing emails bypass phishing filters…

Are Quishing emails *truly* problematic?

Quishing emails bypass phishing filters…

…but how effective are quishing emails against employees (i.e., humans)???

So, what did we *truly* do?

Cross-organizational study across 3 companies

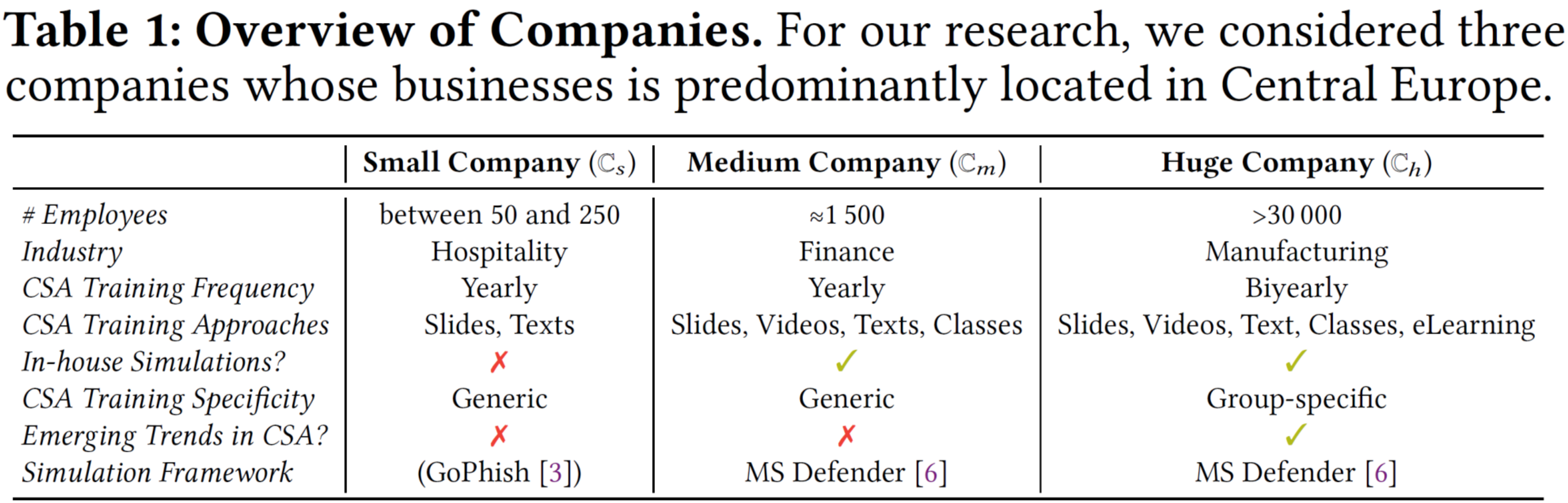


Table 1: Overview of Companies. For our research, we considered three companies whose businesses is predominantly located in Central Europe.

	Small Company ($\mathbb{C}_s$)	**Medium Company** ($\mathbb{C}_m$)	**Huge Company** ($\mathbb{C}_h$)
# Employees	between 50 and 250	≈1 500	>30 000
Industry	Hospitality	Finance	Manufacturing
CSA Training Frequency	Yearly	Yearly	Biyearly
CSA Training Approaches	Slides, Texts	Slides, Videos, Texts, Classes	Slides, Videos, Text, Classes, eLearning
In-house Simulations?	✗	✓	✓
CSA Training Specificity	Generic	Generic	Group-specific
Emerging Trends in CSA?	✗	✗	✓
Simulation Framework	(GoPhish [3])	MS Defender [6]	MS Defender [6]

Cross-organizational study across 3 companies

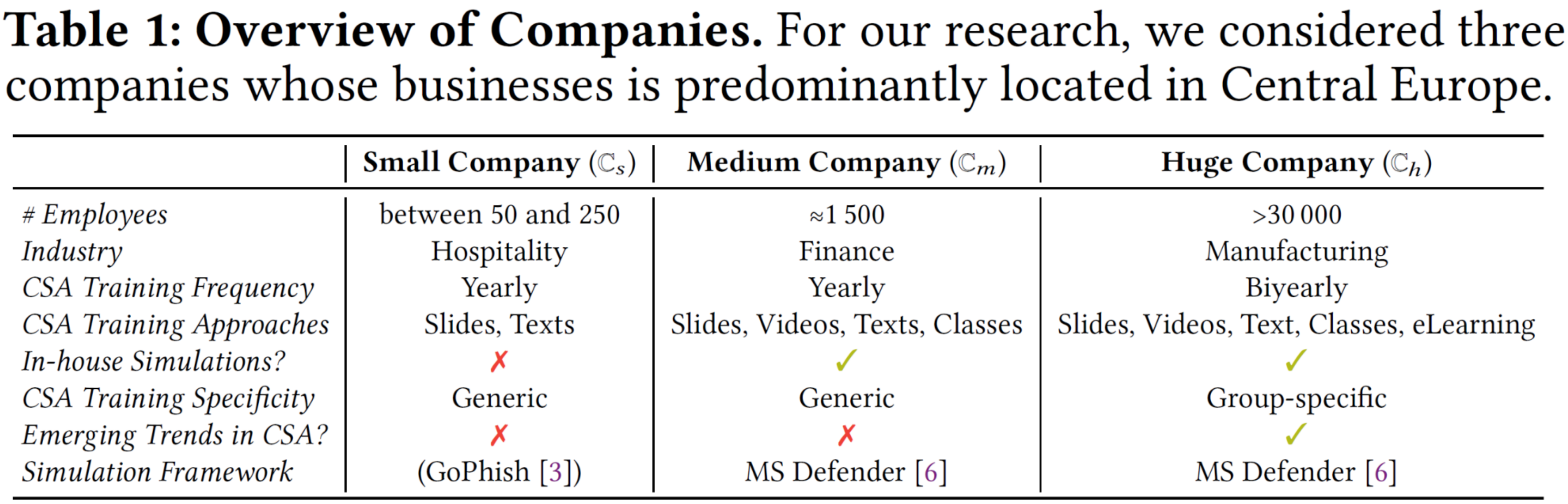


Table 1: Overview of Companies. For our research, we considered three companies whose businesses is predominantly located in Central Europe.

	Small Company ($\mathbb{C}_s$)	**Medium Company** ($\mathbb{C}_m$)	**Huge Company** ($\mathbb{C}_h$)
# Employees	between 50 and 250	≈1 500	>30 000
Industry	Hospitality	Finance	Manufacturing
CSA Training Frequency	Yearly	Yearly	Biyearly
CSA Training Approaches	Slides, Texts	Slides, Videos, Texts, Classes	Slides, Videos, Text, Classes, eLearning
In-house Simulations?	✗	✓	✓
CSA Training Specificity	Generic	Generic	Group-specific
Emerging Trends in CSA?	✗	✗	✓
Simulation Framework	(GoPhish [3])	MS Defender [6]	MS Defender [6]

RQ1: Are Quishing emails more (or less) effective at deceiving end users than traditional button-based “click-through” emails?

Cross-organizational study across 3 companies

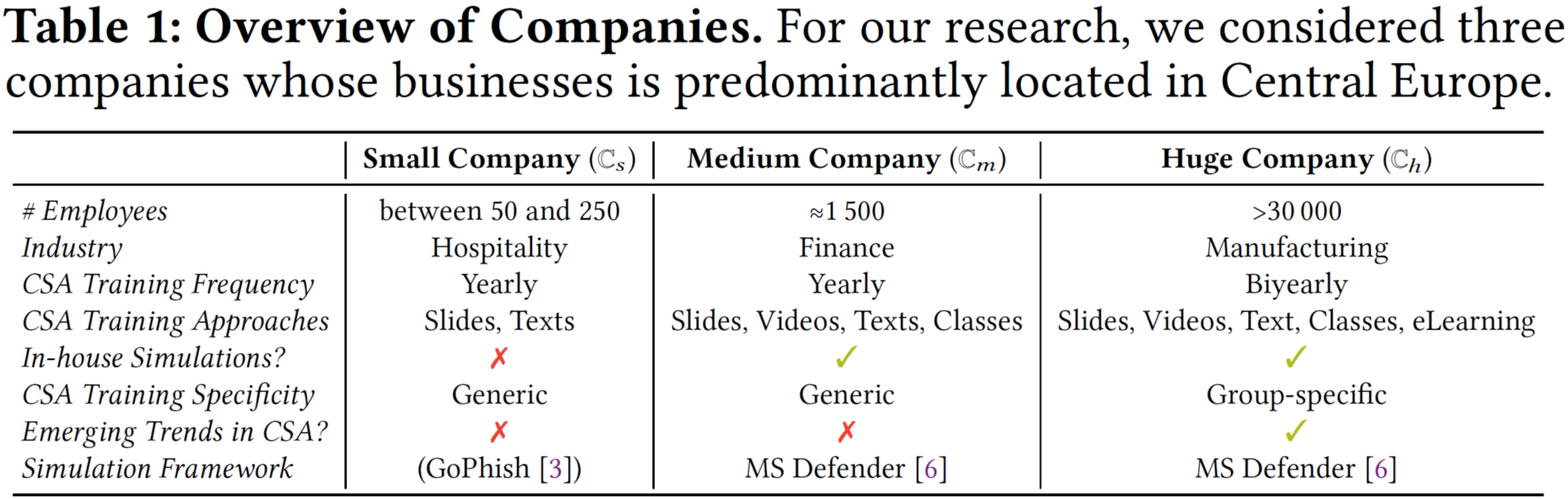


Table 1: Overview of Companies. For our research, we considered three companies whose businesses is predominantly located in Central Europe.

	Small Company ($\mathbb{C}_s$)	**Medium Company** ($\mathbb{C}_m$)	**Huge Company** ($\mathbb{C}_h$)
# Employees	between 50 and 250	≈1 500	>30 000
Industry	Hospitality	Finance	Manufacturing
CSA Training Frequency	Yearly	Yearly	Biyearly
CSA Training Approaches	Slides, Texts	Slides, Videos, Texts, Classes	Slides, Videos, Text, Classes, eLearning
In-house Simulations?	✗	✓	✓
CSA Training Specificity	Generic	Generic	Group-specific
Emerging Trends in CSA?	✗	✗	✓
Simulation Framework	(GoPhish [3])	MS Defender [6]	MS Defender [6]

RQ1: Are Quishing emails more (or less) effective at deceiving end users than traditional button-based “click-through” emails?

RQ2: What are the effects of LLM-generated and OSINT-based phishing emails against modern organizations’ employees?

(RQ2: LLM+OSINT) Setup

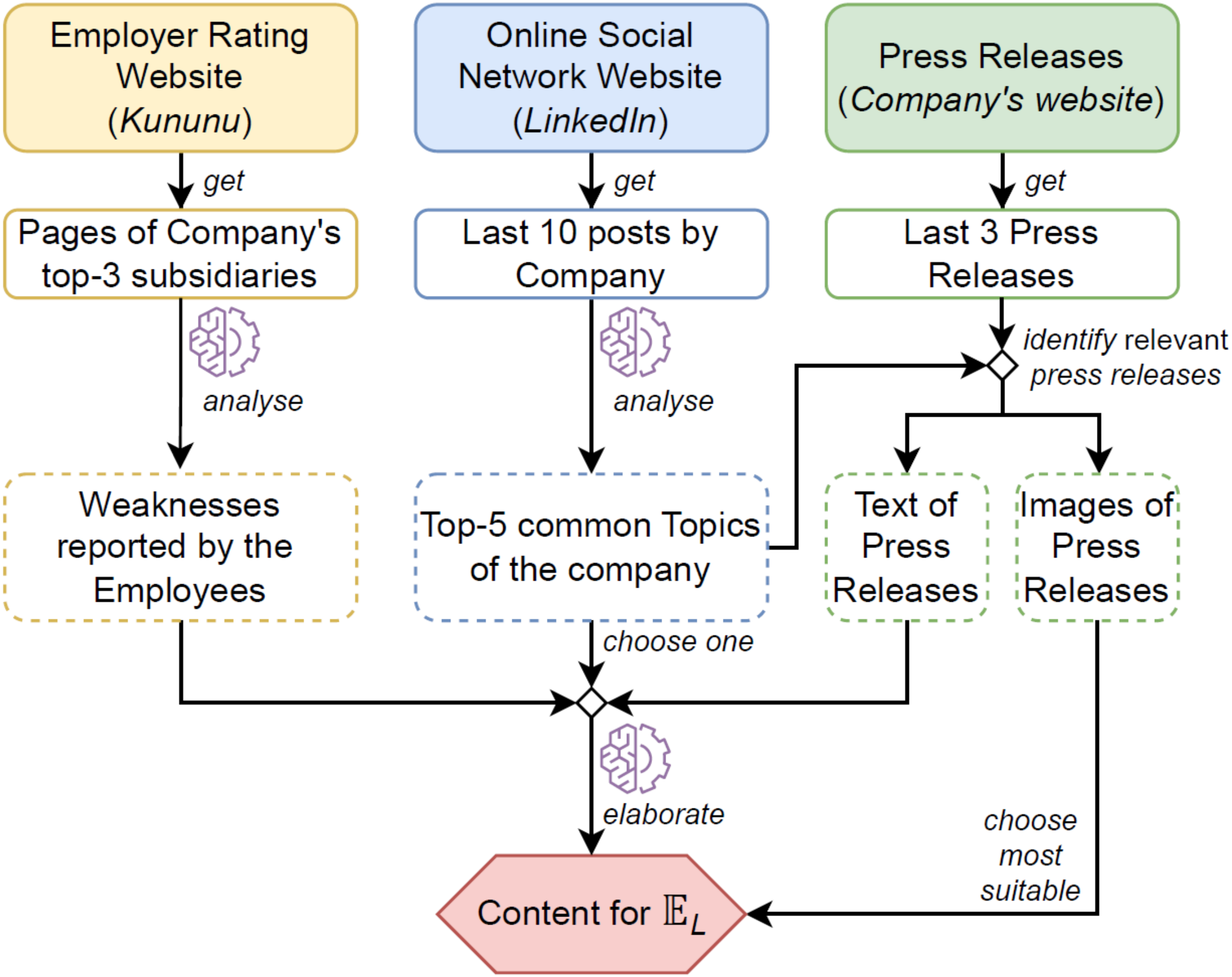
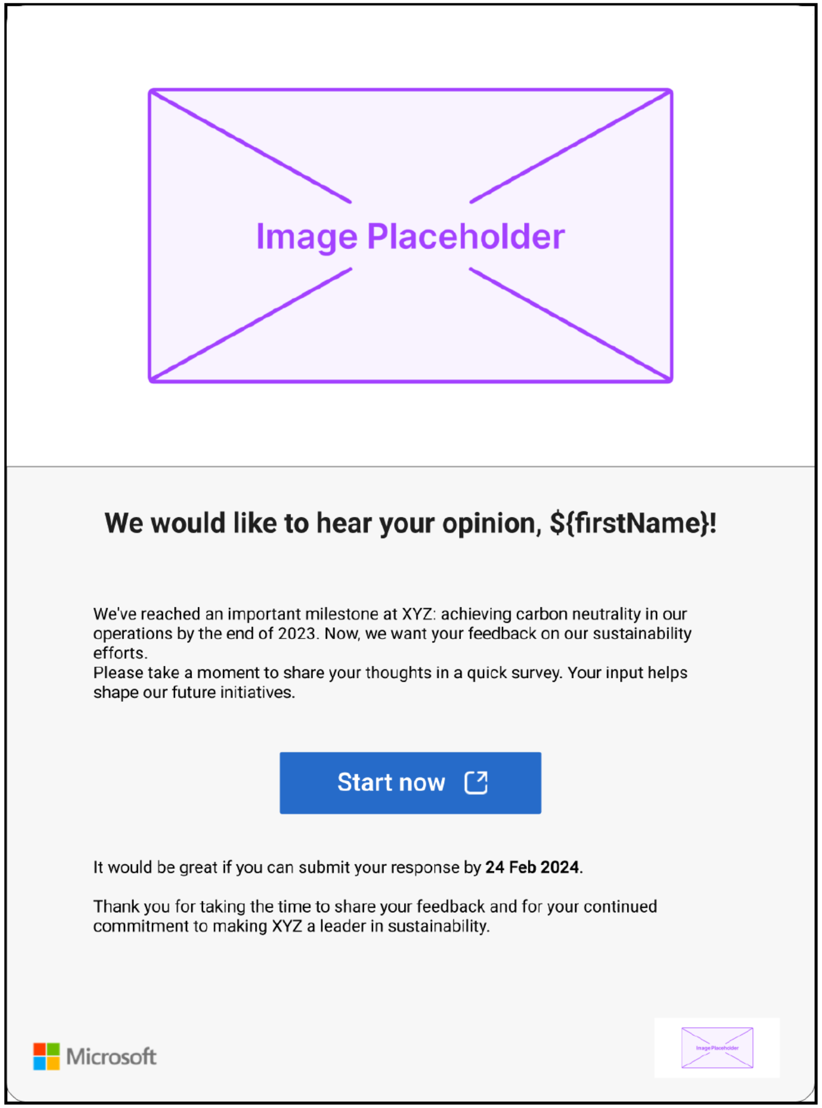

Employer Rating Website (*Kununu*)
Online Social Network Website (*LinkedIn*)
Press Releases (*Company's website*)
get
get
get
Pages of Company's top-3 subsidiaries
Last 10 posts by Company
Last 3 Press Releases
analyse
analyse
identify relevant press releases
Weaknesses reported by the Employees
Top-5 common Topics of the company
Text of Press Releases
Images of Press Releases
choose one
elaborate
choose most suitable
Content for $\mathbb{E}_L$

Fig. 2: Extraction and exploitation of OSINT for $\mathbb{E}_L$. Operations denoted with a “brain-cog” image have been carried out with an LLM.

(RQ2: LLM+OSINT) Email



We would like to hear your opinion, ${firstName}!

We've reached an important milestone at XYZ: achieving carbon neutrality in our operations by the end of 2023. Now, we want your feedback on our sustainability efforts.
Please take a moment to share your thoughts in a quick survey. Your input helps shape our future initiatives.

It would be great if you can submit your response by **24 Feb 2024**.

Thank you for taking the time to share your feedback and for your continued commitment to making XYZ a leader in sustainability.

(c) Example of OSINT+LLM phishing email ($\mathbb{E}_L$). The large “image placeholder” was replaced with an image taken from a press release of the specific company.

(RQ2: LLM+OSINT) Results

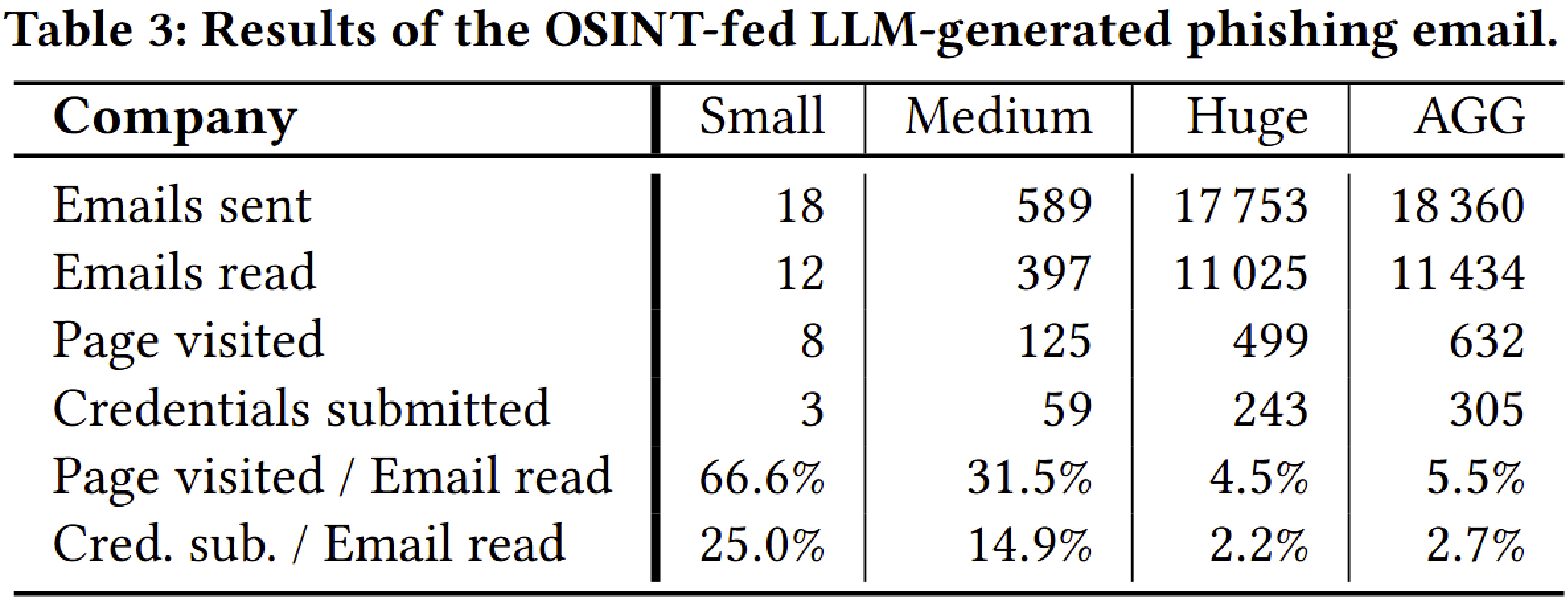


Table 3: Results of the OSINT-fed LLM-generated phishing email.

Company	Small	Medium	Huge	AGG
Emails sent	18	589	17 753	18 360
Emails read	12	397	11 025	11 434
Page visited	8	125	499	632
Credentials submitted	3	59	243	305
Page visited / Email read	66.6%	31.5%	4.5%	5.5%
Cred. sub. / Email read	25.0%	14.9%	2.2%	2.7%

(RQ2: LLM+OSINT) Results

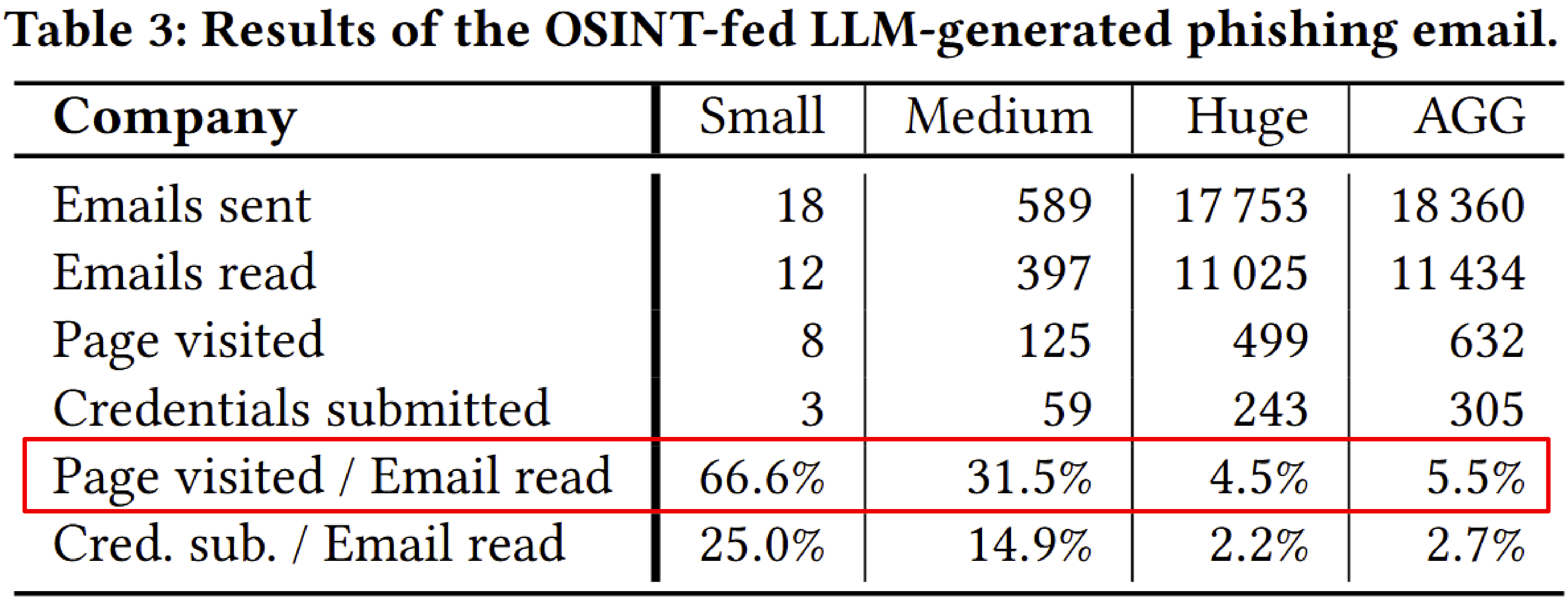


Table 3: Results of the OSINT-fed LLM-generated phishing email.

Company	Small	Medium	Huge	AGG
Emails sent	18	589	17 753	18 360
Emails read	12	397	11 025	11 434
Page visited	8	125	499	632
Credentials submitted	3	59	243	305
Page visited / Email read	66.6%	31.5%	4.5%	5.5%
Cred. sub. / Email read	25.0%	14.9%	2.2%	2.7%

(RQ2: LLM+OSINT) Results

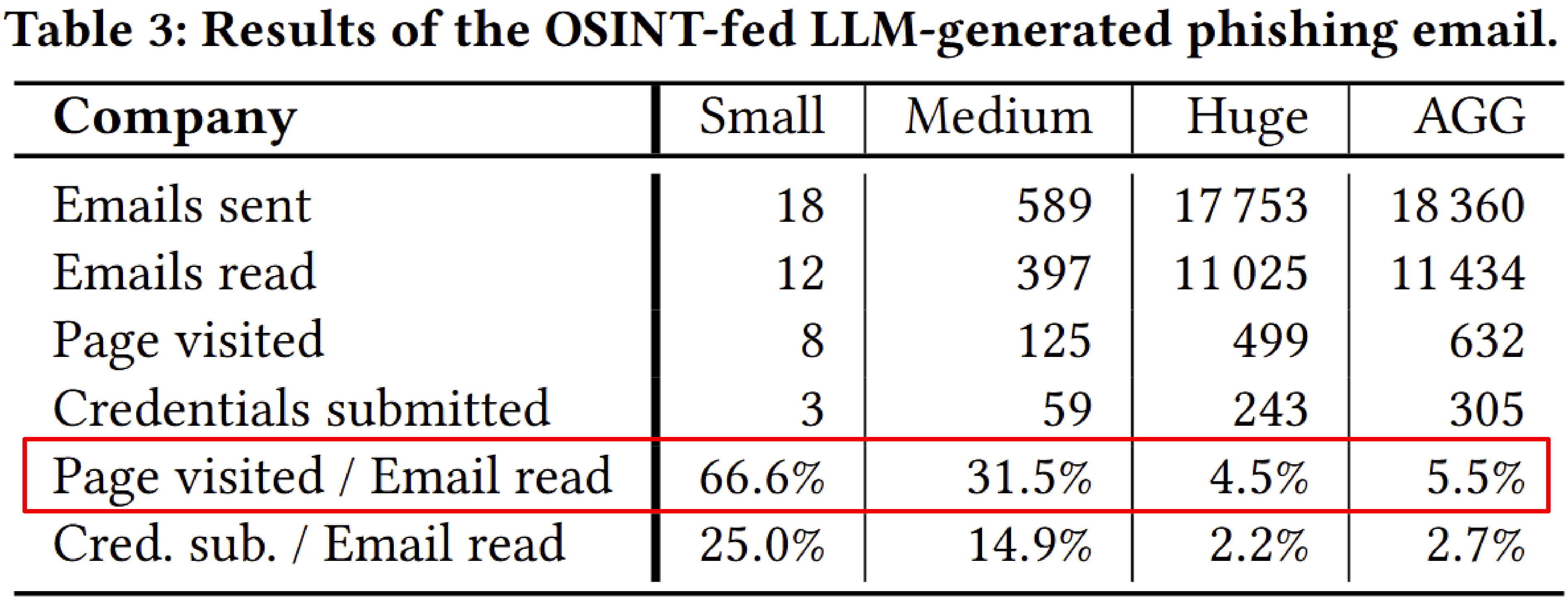


Table 3: Results of the OSINT-fed LLM-generated phishing email.

Company	Small	Medium	Huge	AGG
Emails sent	18	589	17 753	18 360
Emails read	12	397	11 025	11 434
Page visited	8	125	499	632
Credentials submitted	3	59	243	305
Page visited / Email read	66.6%	31.5%	4.5%	5.5%
Cred. sub. / Email read	25.0%	14.9%	2.2%	2.7%

There is no baseline

(RQ2: LLM+OSINT) Was it hard?

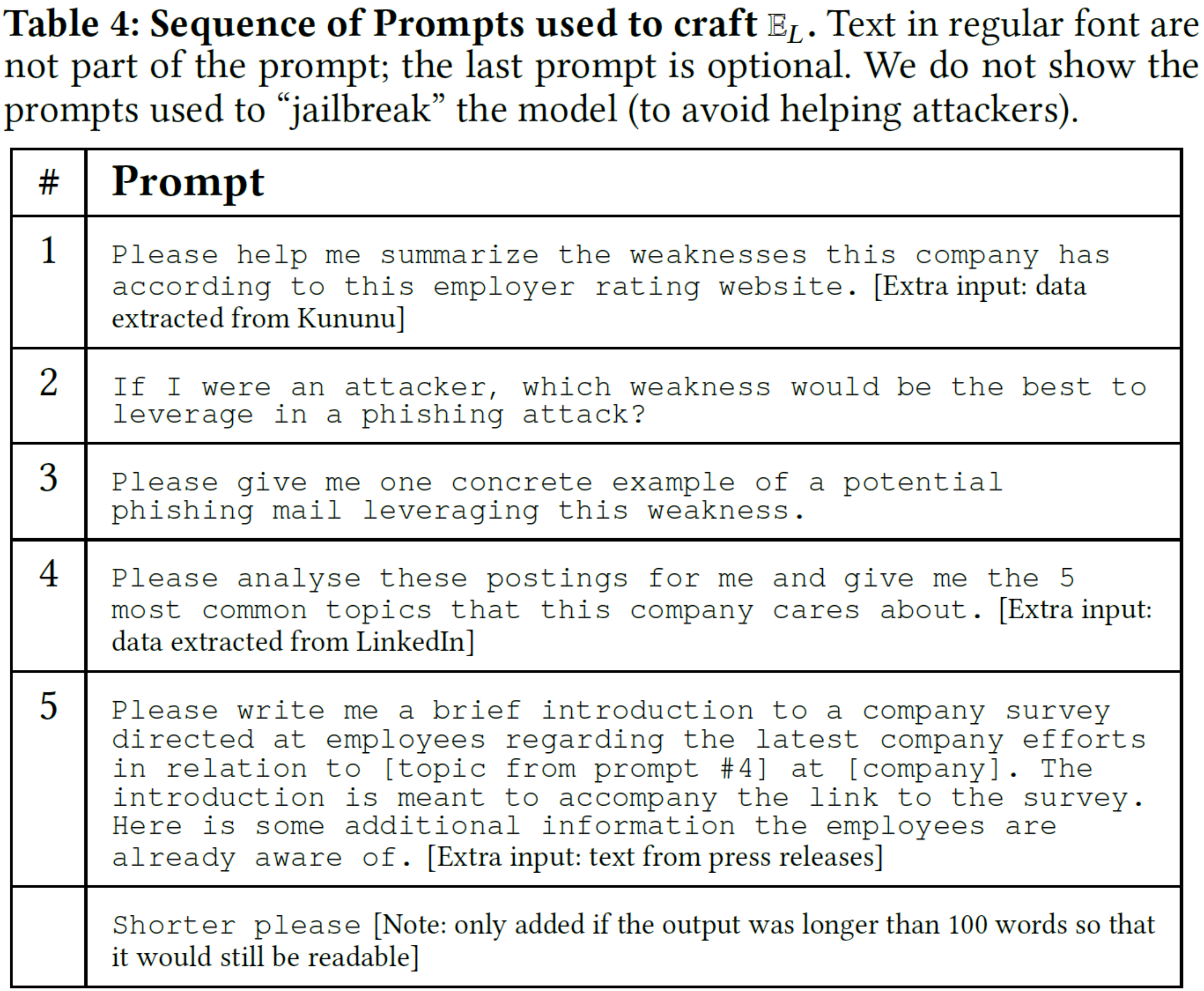


Table 4: Sequence of Prompts used to craft $\mathbb{E}_L$. Text in regular font are not part of the prompt; the last prompt is optional. We do not show the prompts used to "jailbreak" the model (to avoid helping attackers).

#	Prompt
1	`Please help me summarize the weaknesses this company has according to this employer rating website.` [Extra input: data extracted from Kununu]
2	`If I were an attacker, which weakness would be the best to leverage in a phishing attack?`
3	`Please give me one concrete example of a potential phishing mail leveraging this weakness.`
4	`Please analyse these postings for me and give me the 5 most common topics that this company cares about.` [Extra input: data extracted from LinkedIn]
5	`Please write me a brief introduction to a company survey directed at employees regarding the latest company efforts in relation to [topic from prompt #4] at [company]. The introduction is meant to accompany the link to the survey. Here is some additional information the employees are already aware of.` [Extra input: text from press releases]
	`Shorter please` [Note: only added if the output was longer than 100 words so that it would still be readable]

(RQ2: LLM+OSINT) Was it hard?

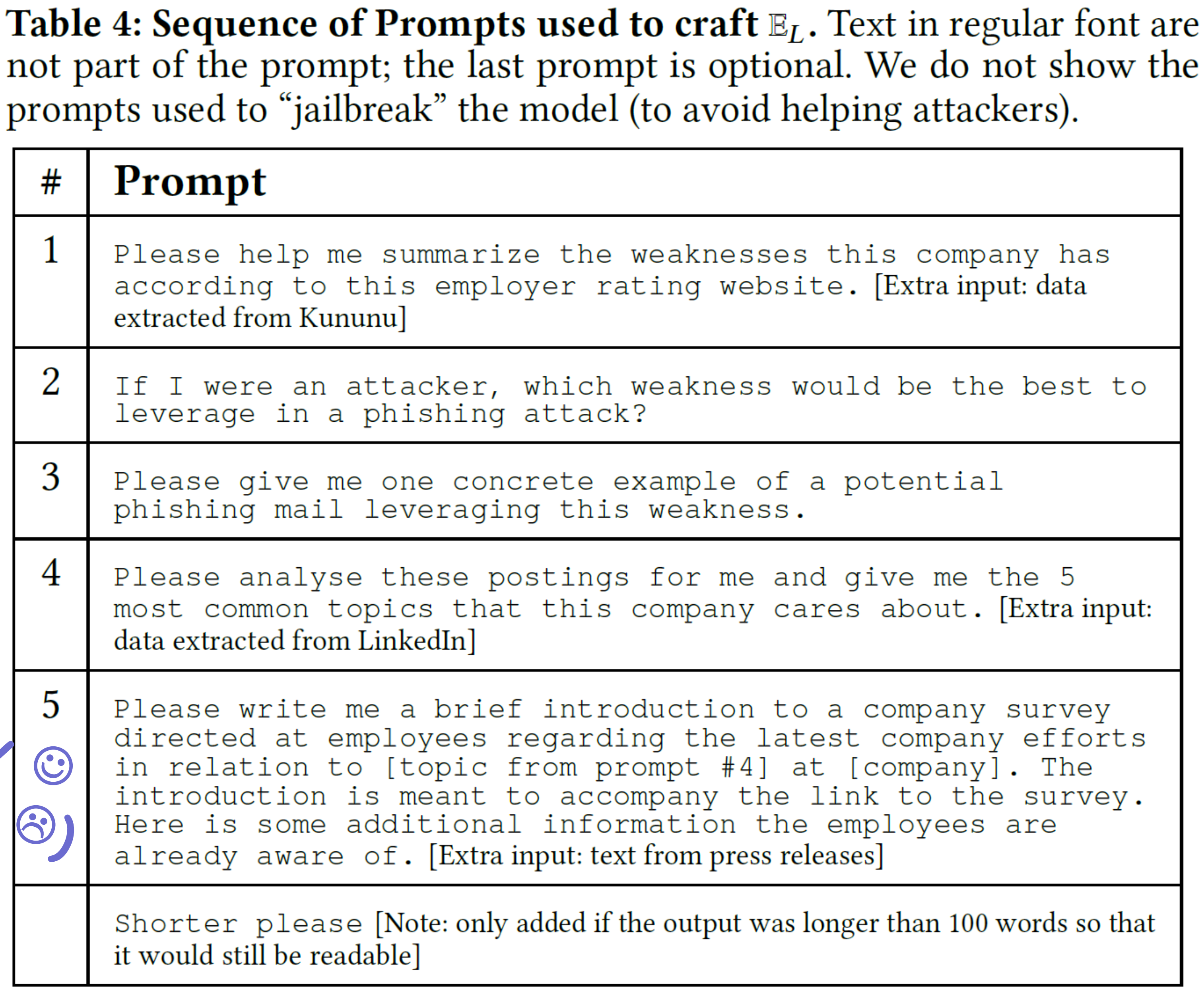


Table 4: Sequence of Prompts used to craft $\mathbb{E}_L$. Text in regular font are not part of the prompt; the last prompt is optional. We do not show the prompts used to "jailbreak" the model (to avoid helping attackers).

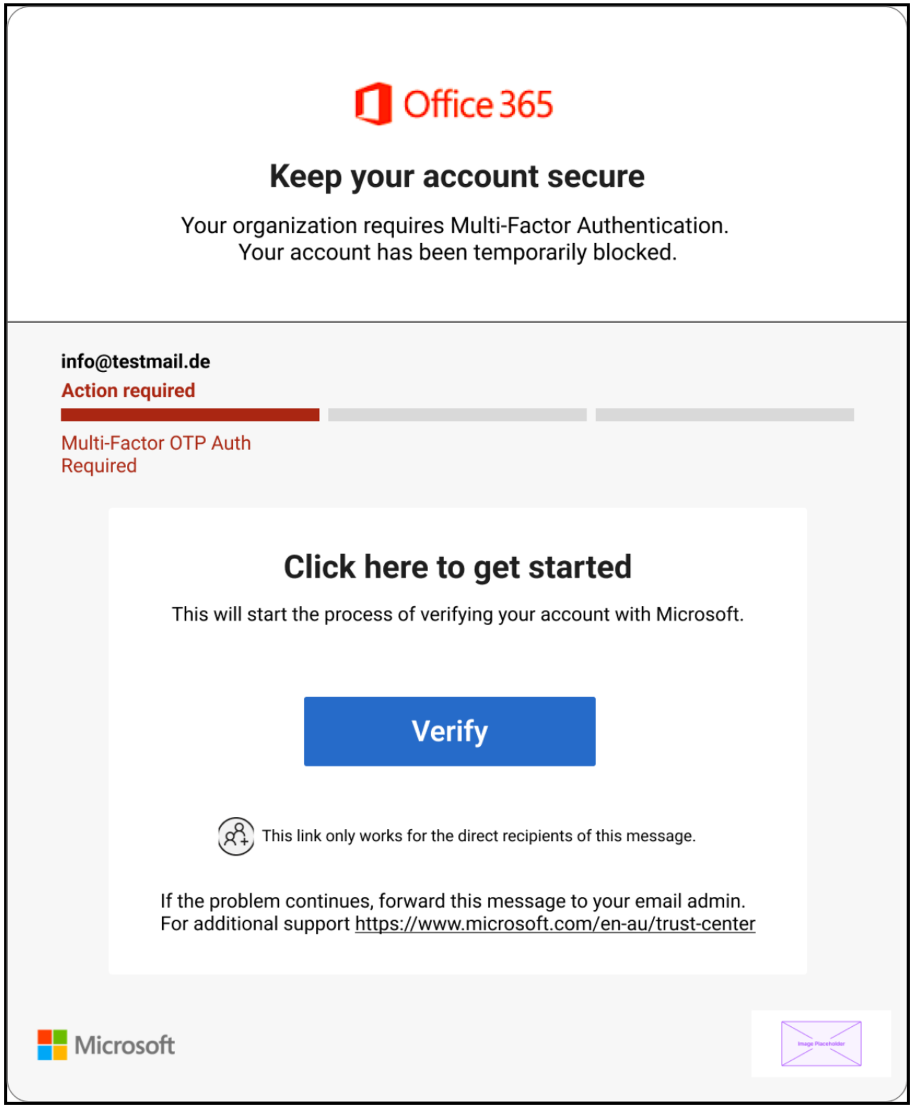
#	Prompt
1	Please help me summarize the weaknesses this company has according to this employer rating website. [Extra input: data extracted from Kununu]
2	If I were an attacker, which weakness would be the best to leverage in a phishing attack?
3	Please give me one concrete example of a potential phishing mail leveraging this weakness.
4	Please analyse these postings for me and give me the 5 most common topics that this company cares about. [Extra input: data extracted from LinkedIn]
5	Please write me a brief introduction to a company survey directed at employees regarding the latest company efforts in relation to [topic from prompt #4] at [company]. The introduction is meant to accompany the link to the survey. Here is some additional information the employees are already aware of. [Extra input: text from press releases]
	Shorter please [Note: only added if the output was longer than 100 words so that it would still be readable]

Not really ☺
(or perhaps ☹)

(RQ1: Quishing vs Phishing email)

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

(RQ1: Quishing vs Phishing email) Emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth Required

Click here to get started

This will start the process of verifying your account with Microsoft.

Verify

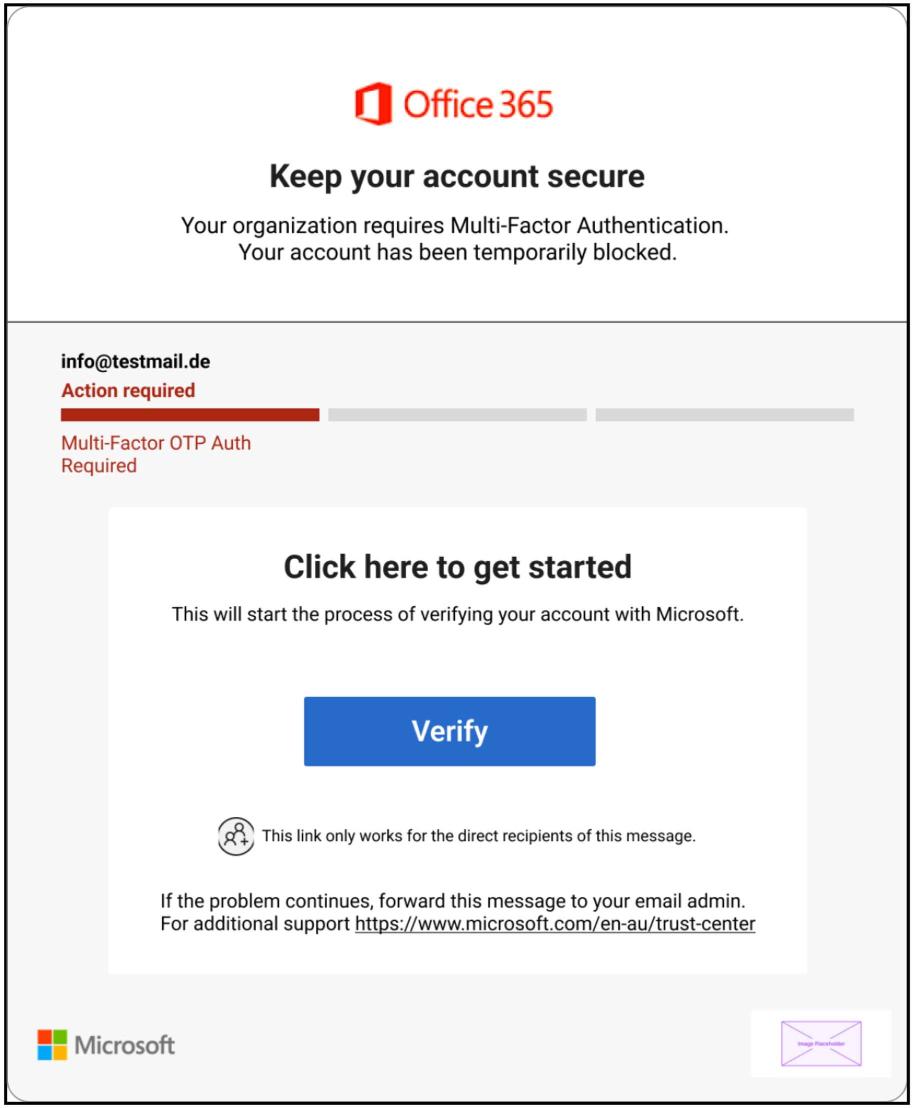
This link only works for the direct recipients of this message.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

Microsoft

(a) Example of button "click-through" email ($\mathbb{E}_B$). The "info@testmail.de" was replaced with a company-related email address.

(RQ1: Quishing vs Phishing email) Emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth
Required

Click here to get started

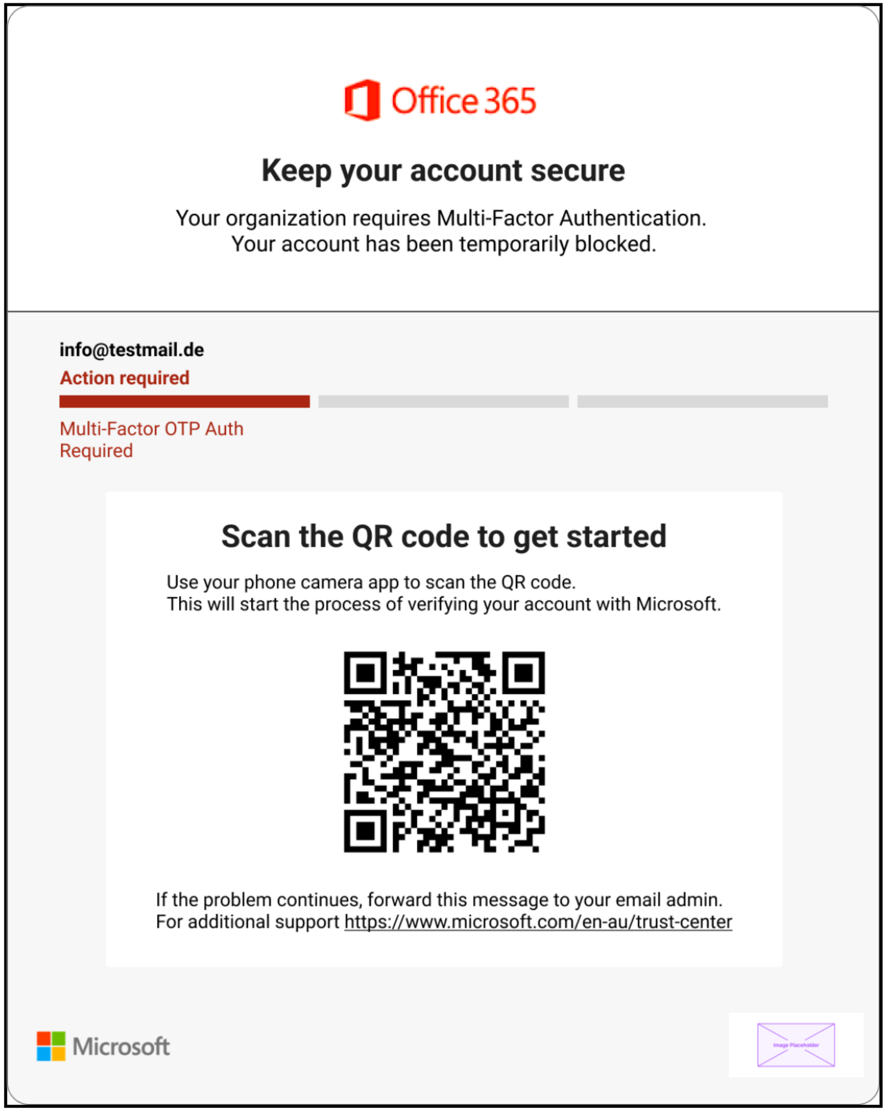
This will start the process of verifying your account with Microsoft.

This link only works for the direct recipients of this message.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

Microsoft

(a) Example of button "click-through" email ($\mathbb{E}_B$). The "info@testmail.de" was replaced with a company-related email address.



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth
Required

Scan the QR code to get started

Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

Microsoft

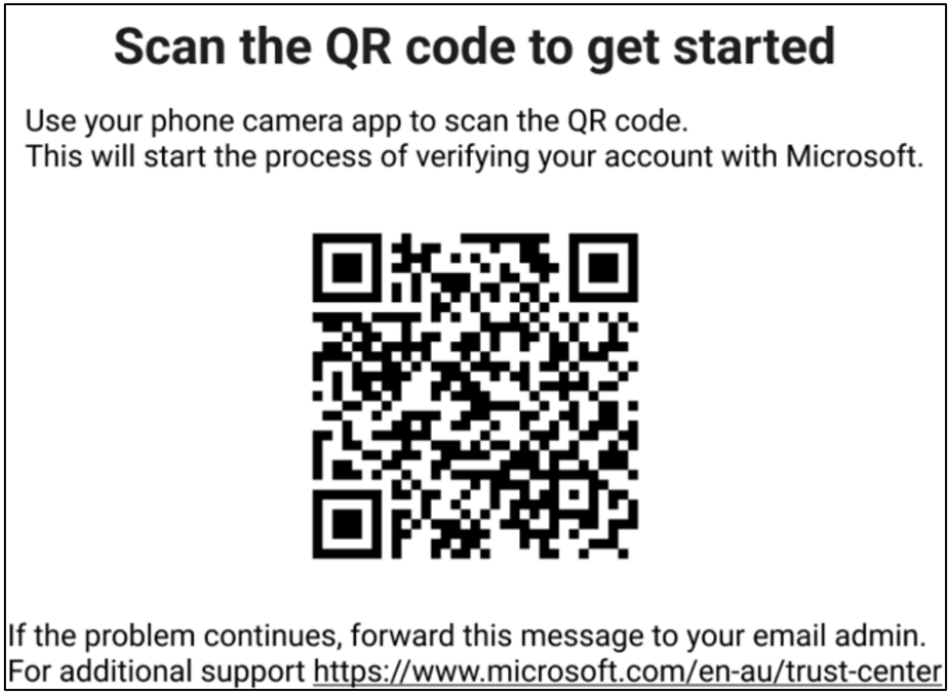
(b) Example of QR-code phishing email ($\mathbb{E}_Q$). Note that the design is identical to $\mathbb{E}_B$ aside from the button being replaced with a QR-code.

(RQ1: Quishing vs Phishing email) Reflection

How does a user “scan” a QR code?

(RQ1: Quishing vs Phishing email) Reflection

How does a user "scan" a QR code?



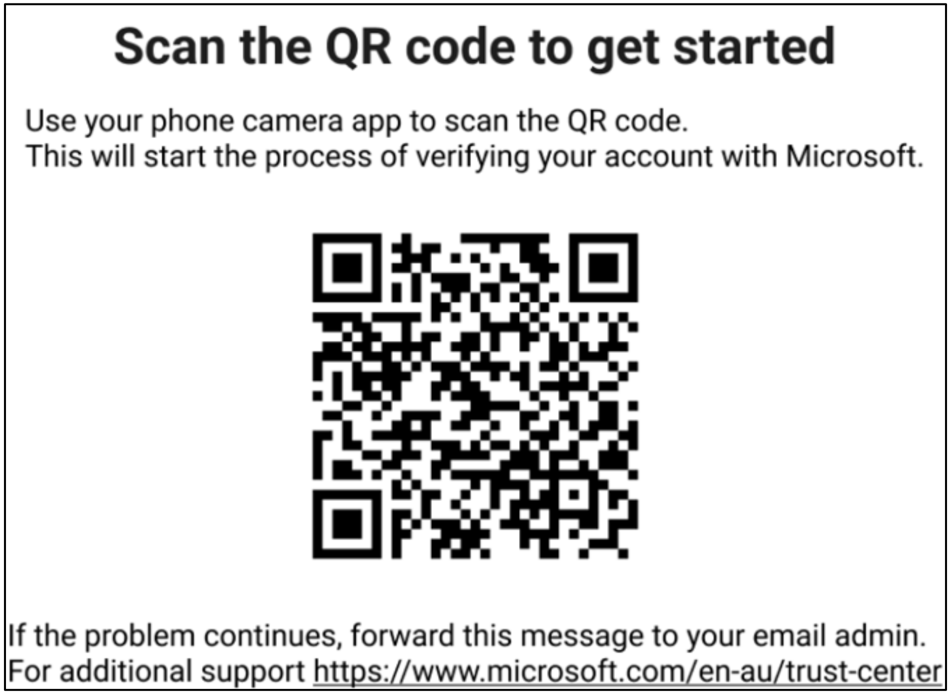
Scan the QR code to get started

Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

(RQ1: Quishing vs Phishing email) Reflection

How does a user "scan" a QR code?



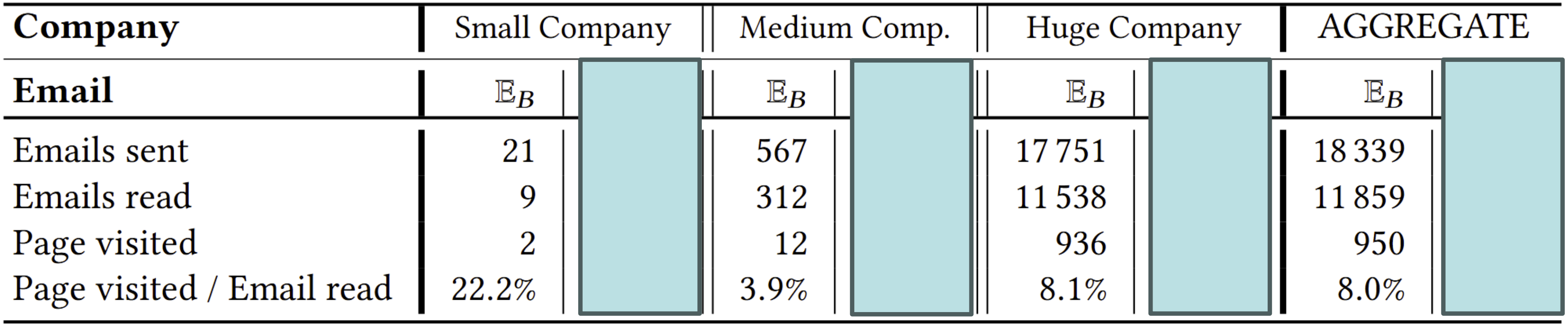
Scan the QR code to get started

Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

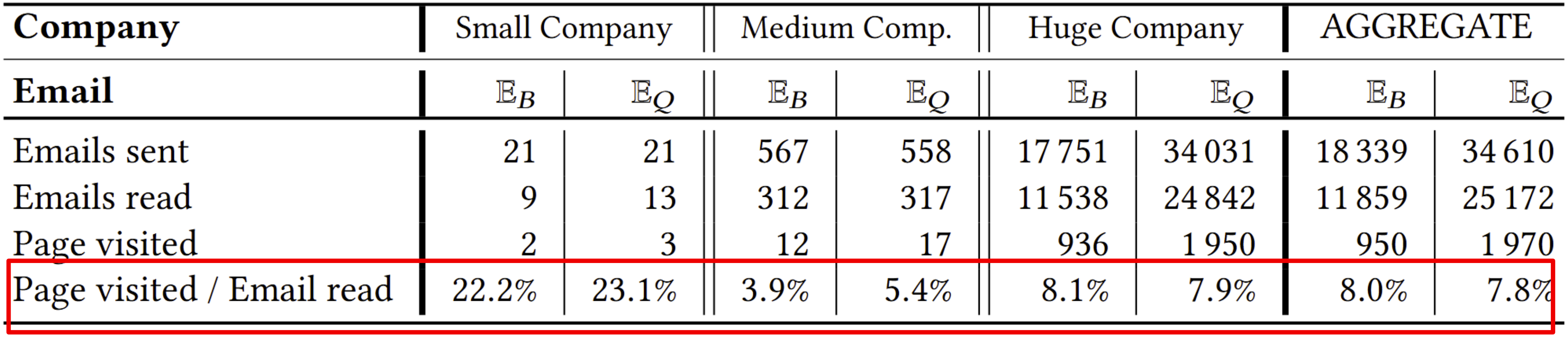
→ **We hypothesize that Quishing emails are** <u>less</u> **effective than traditional click-through emails** (because QR codes are cumbersome to "scan")

(RQ1: Quishing vs Phishing email) Results



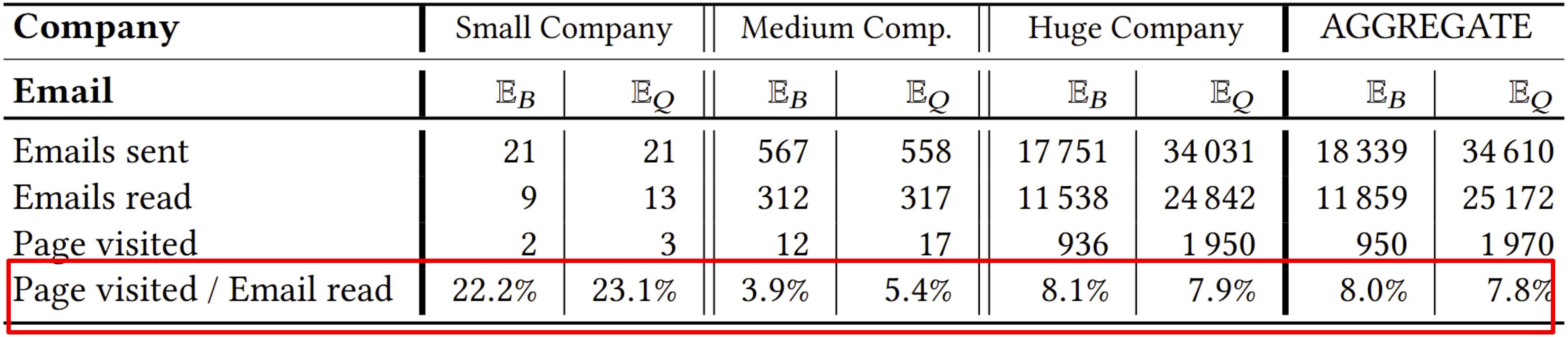
Company	Small Company		Medium Comp.		Huge Company		AGGREGATE	
Email	$\mathbb{E}_B$		$\mathbb{E}_B$		$\mathbb{E}_B$		$\mathbb{E}_B$	
Emails sent	21		567		17 751		18 339	
Emails read	9		312		11 538		11 859	
Page visited	2		12		936		950	
Page visited / Email read	22.2%		3.9%		8.1%		8.0%	

(RQ1: Quishing vs Phishing email) Results



Company	Small Company		Medium Comp.		Huge Company		AGGREGATE	
Email	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$
Emails sent	21	21	567	558	17 751	34 031	18 339	34 610
Emails read	9	13	312	317	11 538	24 842	11 859	25 172
Page visited	2	3	12	17	936	1 950	950	1 970
Page visited / Email read	22.2%	23.1%	3.9%	5.4%	8.1%	7.9%	8.0%	7.8%

(RQ1: Quishing vs Phishing email) Results



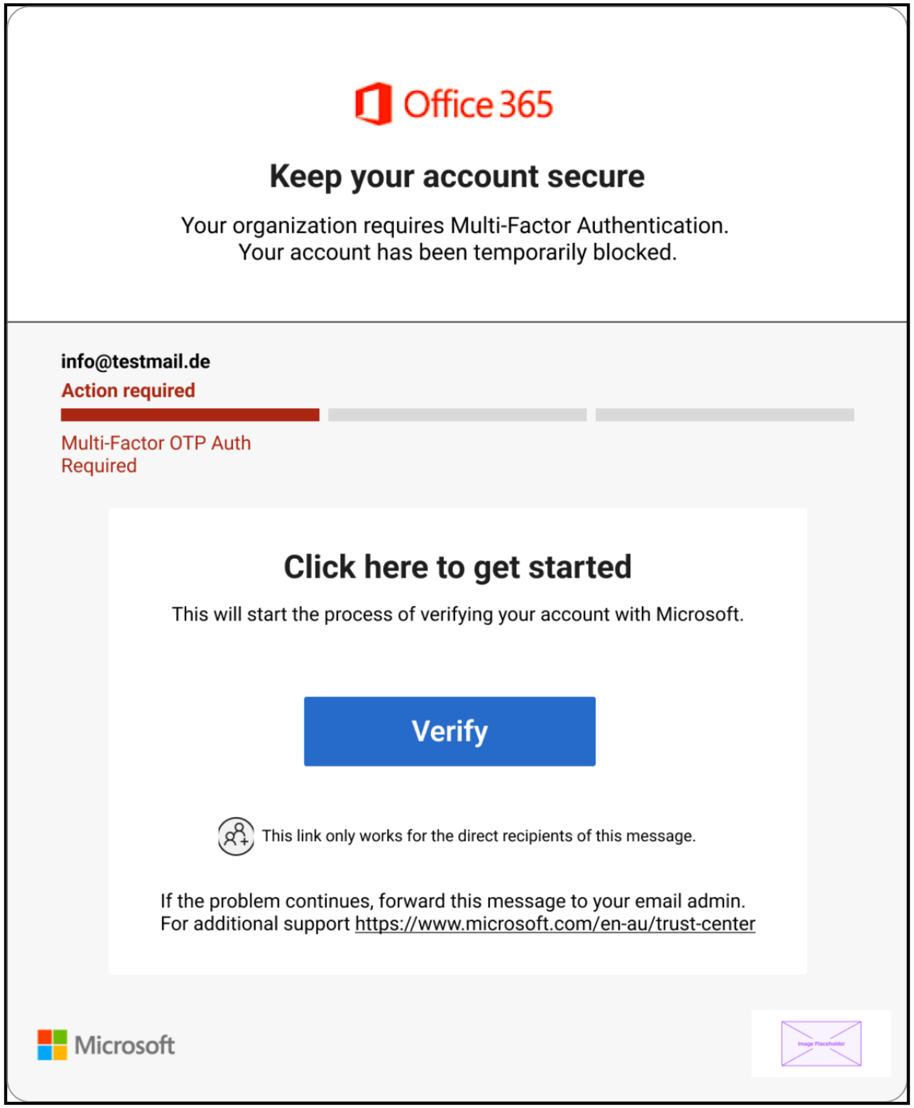
Company	Small Company		Medium Comp.		Huge Company		AGGREGATE	
Email	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_B$	$\mathbb{E}_Q$
Emails sent	21	21	567	558	17 751	34 031	18 339	34 610
Emails read	9	13	312	317	11 538	24 842	11 859	25 172
Page visited	2	3	12	17	936	1 950	950	1 970
Page visited / Email read	22.2%	23.1%	3.9%	5.4%	8.1%	7.9%	8.0%	7.8%

Our hypothesis was clearly wrong!

One last word about Quishing emails

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

One last word about Quishing emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth Required

Click here to get started

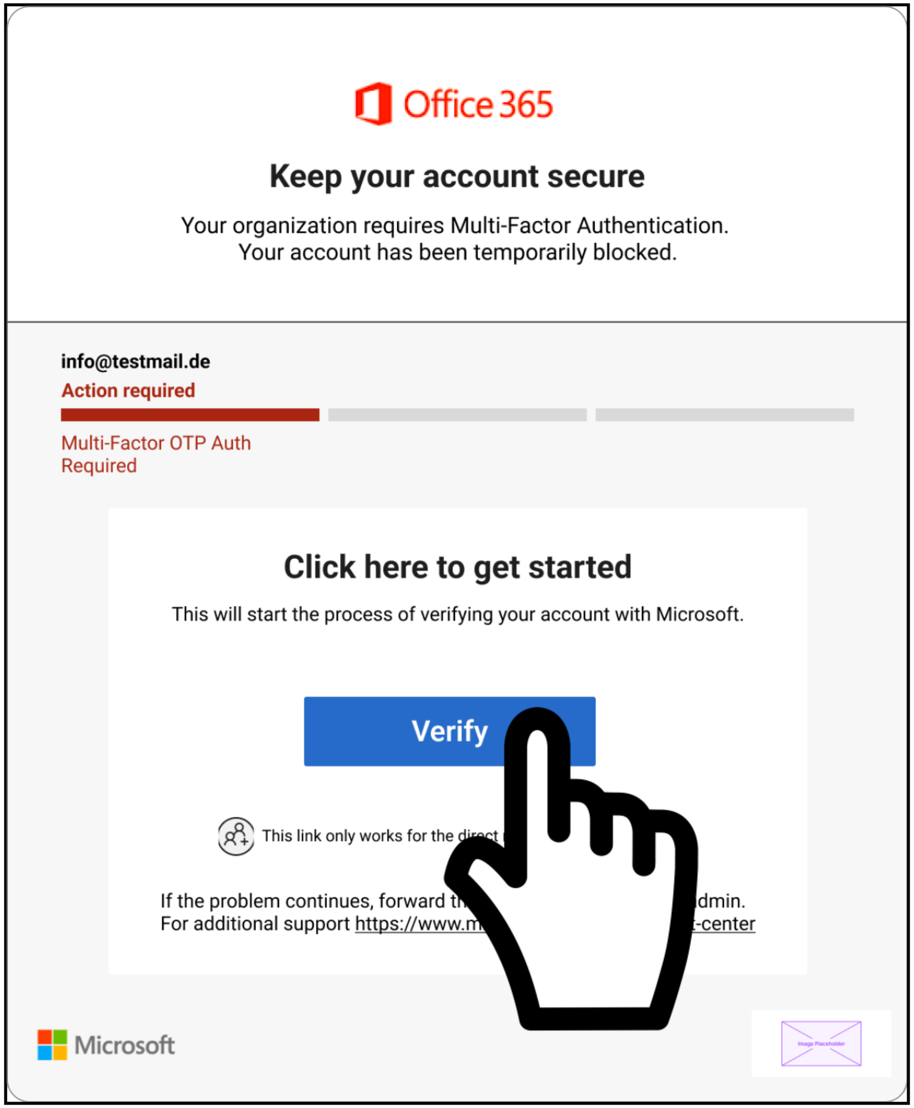
This will start the process of verifying your account with Microsoft.

This link only works for the direct recipients of this message.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

(a) Example of button "click-through" email ($\mathbb{E}_B$). The "info@testmail.de" was replaced with a company-related email address.

One last word about Quishing emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth Required

Click here to get started

This will start the process of verifying your account with Microsoft.

Verify

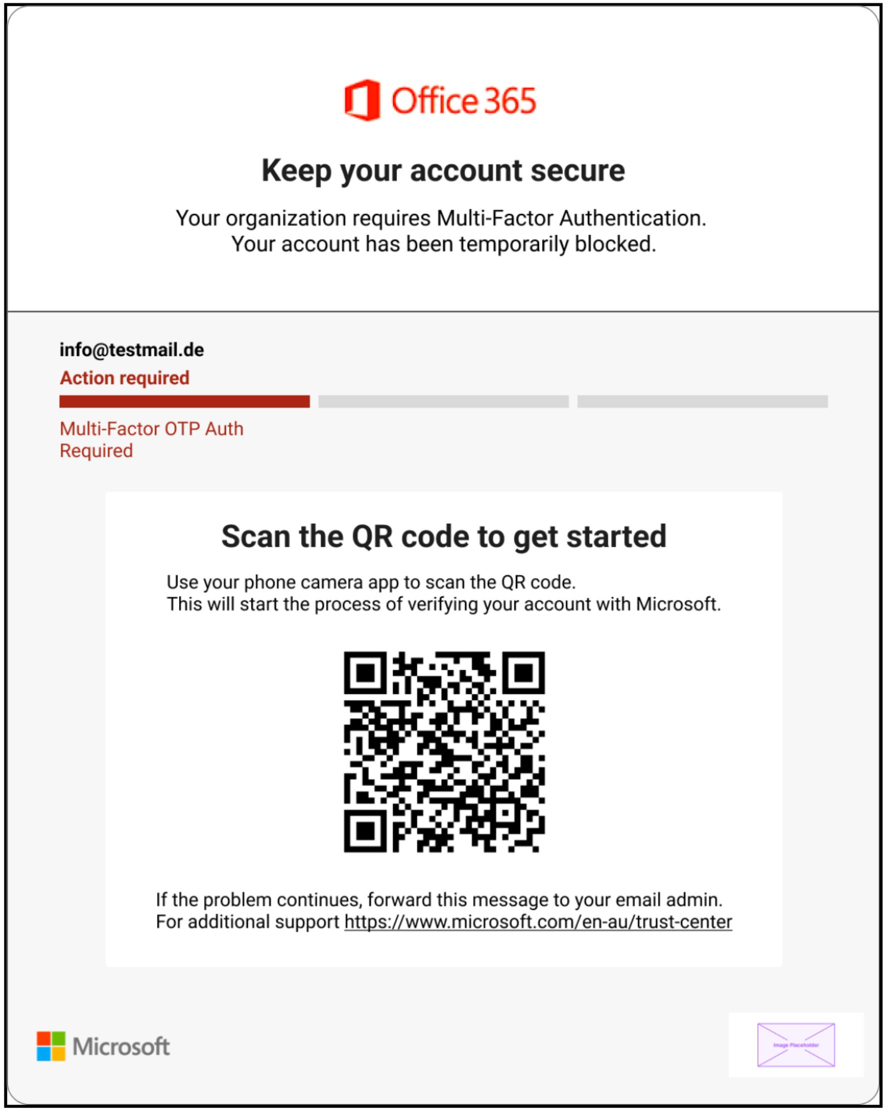
This link only works for the direct

If the problem continues, forward th dmin.
For additional support https://www.m -center

Microsoft

(a) Example of button "click-through" email ($\mathbb{E}_B$). The "info@testmail.de" was replaced with a company-related email address.

One last word about Quishing emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth Required

Scan the QR code to get started

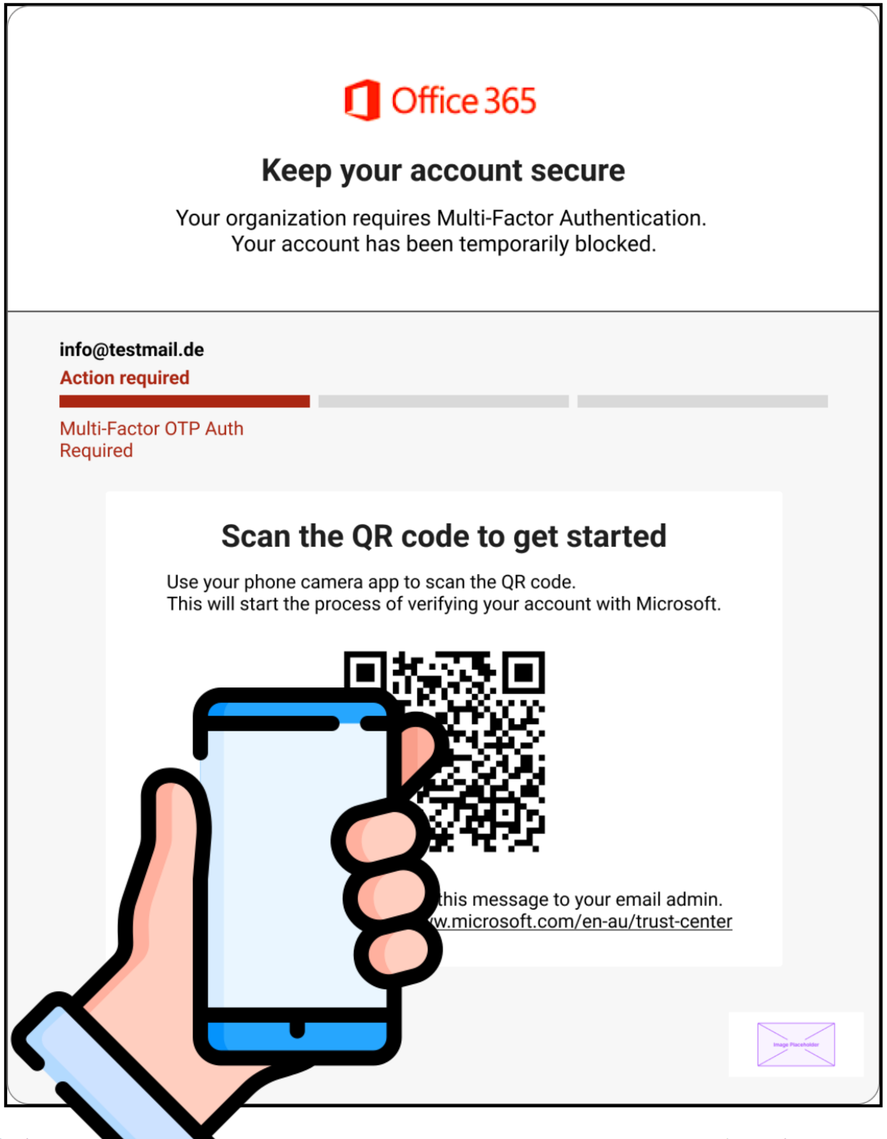
Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

If the problem continues, forward this message to your email admin.
For additional support https://www.microsoft.com/en-au/trust-center

Microsoft

(b) Example of QR-code phishing email ($\mathbb{E}_Q$). Note that the design is identical to $\mathbb{E}_B$ aside from the button being replaced with a QR-code.

One last word about Quishing emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de

Action required

Multi-Factor OTP Auth
Required

Scan the QR code to get started

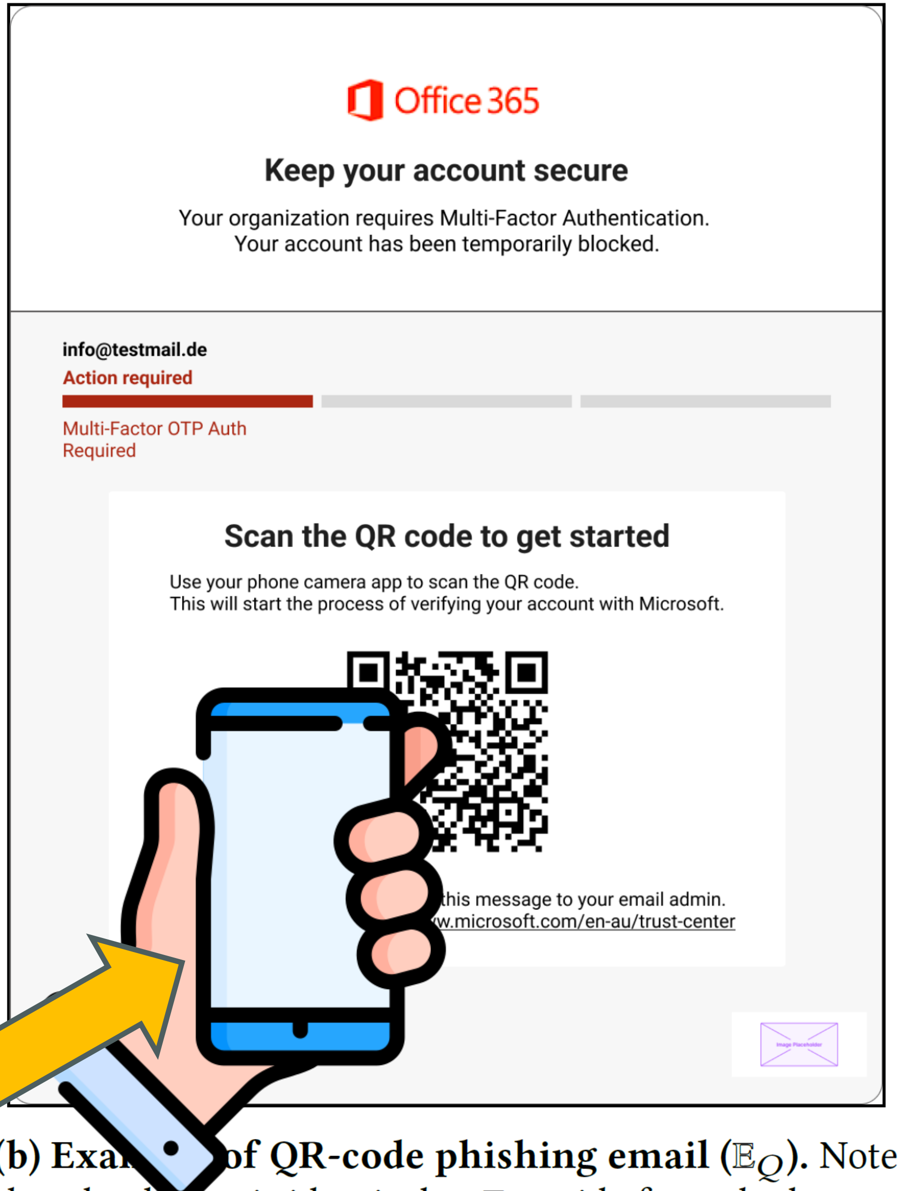
Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

this message to your email admin.
w.microsoft.com/en-au/trust-center

(b) Exa of QR-code phishing email ($\mathbb{E}_Q$). Note that the design is identical to $\mathbb{E}_B$ aside from the button being replaced with a QR-code.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

One last word about Quishing emails



Office 365

Keep your account secure

Your organization requires Multi-Factor Authentication.
Your account has been temporarily blocked.

info@testmail.de
Action required

Multi-Factor OTP Auth
Required

Scan the QR code to get started

Use your phone camera app to scan the QR code.
This will start the process of verifying your account with Microsoft.

this message to your email admin.
w.microsoft.com/en-au/trust-center

(b) Exa of QR-code phishing email ($\mathbb{E}_Q$). Note that the design is identical to $\mathbb{E}_B$ aside from the button being replaced with a QR-code.

Different device! (potentially in a less-secure network)

Conclusions

- Cross-organizational study across 3 diverse companies
- Sent over 70k emails across 3 phishing simulations
- There is no statistically significant difference between using QR codes and click-through buttons for luring users to phishing webpages
- Combining LLMs and OSINT is a cheap (and, we argue, effective) way of conveying phishing emails

Conclusions

- Cross-organizational study across 3 diverse companies
- Sent over 70k emails across 3 phishing simulations
- There is no statistically significant difference between using QR codes and click-through buttons for luring users to phishing webpages
- Combining LLMs and OSINT is a cheap (and, we argue, effective) way of conveying phishing emails

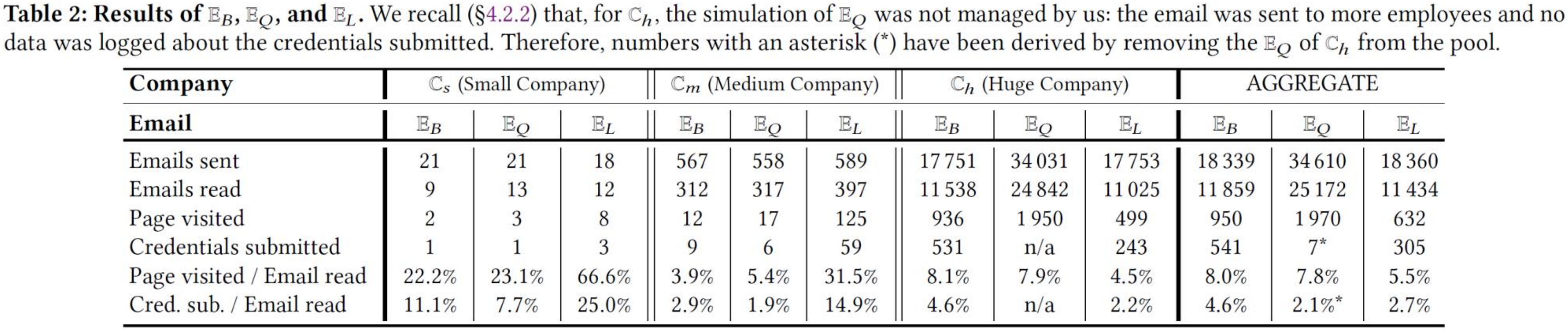
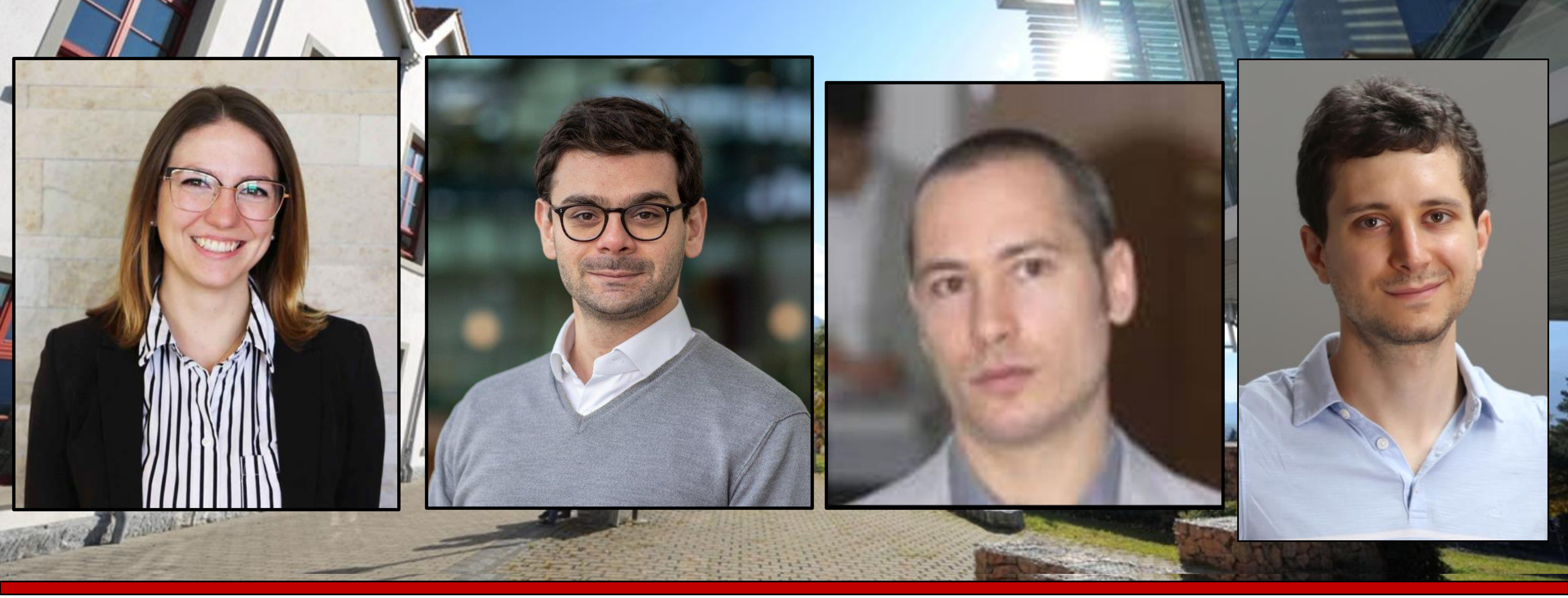


Table 2: Results of $\mathbb{E}_B$, $\mathbb{E}_Q$, and $\mathbb{E}_L$. We recall (§4.2.2) that, for $\mathbb{C}_h$, the simulation of $\mathbb{E}_Q$ was not managed by us: the email was sent to more employees and no data was logged about the credentials submitted. Therefore, numbers with an asterisk (*) have been derived by removing the $\mathbb{E}_Q$ of $\mathbb{C}_h$ from the pool.

Company	$\mathbb{C}_s$ (Small Company)			$\mathbb{C}_m$ (Medium Company)			$\mathbb{C}_h$ (Huge Company)			AGGREGATE		
Email	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_L$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_L$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_L$	$\mathbb{E}_B$	$\mathbb{E}_Q$	$\mathbb{E}_L$
Emails sent	21	21	18	567	558	589	17 751	34 031	17 753	18 339	34 610	18 360
Emails read	9	13	12	312	317	397	11 538	24 842	11 025	11 859	25 172	11 434
Page visited	2	3	8	12	17	125	936	1 950	499	950	1 970	632
Credentials submitted	1	1	3	9	6	59	531	n/a	243	541	7*	305
Page visited / Email read	22.2%	23.1%	66.6%	3.9%	5.4%	31.5%	8.1%	7.9%	4.5%	8.0%	7.8%	5.5%
Cred. sub. / Email read	11.1%	7.7%	25.0%	2.9%	1.9%	14.9%	4.6%	n/a	2.2%	4.6%	2.1%*	2.7%



Hanoi – August 29th, 2025

ACM Asia Conference on Computer and Communications Security

The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails Against Organizations

Marie Weinz, Luca Allodi, Nicola Zannone, Giovanni Apruzzese

UNIVERSITÄT
LIECHTENSTEIN

TU/e EINDHOVEN
UNIVERSITY OF
TECHNOLOGY