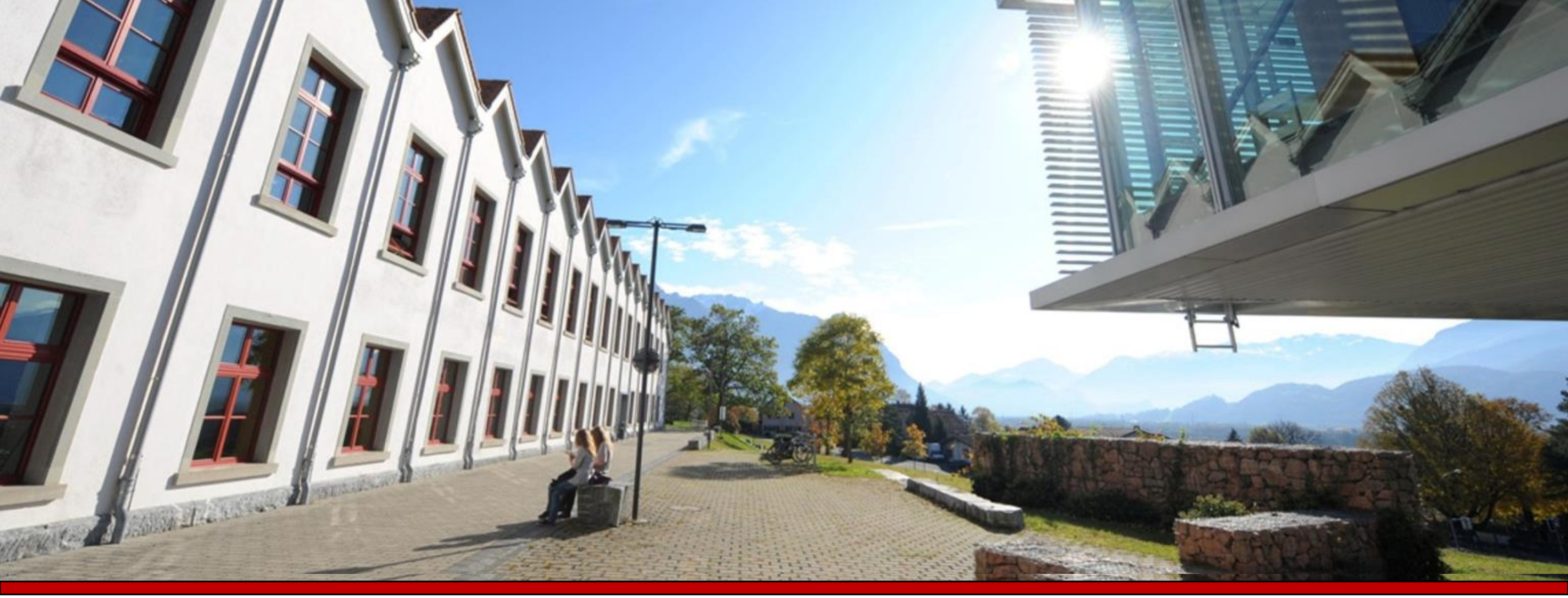


Boston – September 25th, 2024

APWG Symposium on Electronic Crime Research (eCrime)

“Hey Google, Remind me to be Phished” Exploiting the Notifications of the Google (AI) Assistant on Android for Social Engineering Attacks

Marie Weinz, Saskia Laura Schröer, Giovanni Apruzzese

UNIVERSITÄT
LIECHTENSTEIN

Backstory (1)

- October—November 2023

Backstory (1)

- October—November 2023
- Marie Weinz was experimenting with some phishing-related tools for her MSc. Thesis (which is not the topic of this paper/talk ☺)
- I recommended she looked into *GoPhish* and *ZPhisher*

GoPhish: https://getgophish.com
Zphisher: https://github.com/htr-tech/zphisher

Backstory (1)

- October—November 2023
- Marie Weinz was experimenting with some phishing-related tools for her MSc. Thesis (which is not the topic of this paper/talk ☺)
- I recommended she looked into *GoPhish* and *ZPhisher*
- I told her to send me some "phishing" emails using these tools

  (I, too, was curious to see how these tools worked!)

GoPhish: https://getgophish.com
Zphisher: https://github.com/htr-tech/zphisher

Backstory (2)

- December 4th, 2023
- I tell Marie to do some more tests on my Gmail accout

Backstory (2)

- December 4th, 2023
- I tell Marie to do some more tests on my Gmail accout

- December 5th, 2023 (11:12AM)
- Marie sends me one email

Backstory (2)

- December 4th, 2023
- I tell Marie to do some more tests on my Gmail accout

- December 5th, 2023 (11:12AM)
- Marie sends me one email

- December 5th, 2023 (11:55AM)
- I wake up and check my phone, cleaning some notifications.

Backstory (2)

- December 4th, 2023
- I tell Marie to do some more tests on my Gmail accout

- December 5th, 2023 (11:12AM)
- Marie sends me one email

- December 5th, 2023 (11:55AM)
- I wake up and check my phone, cleaning some notifications.

- December 5th, 2023 (11:59AM)
- I notice something weird…

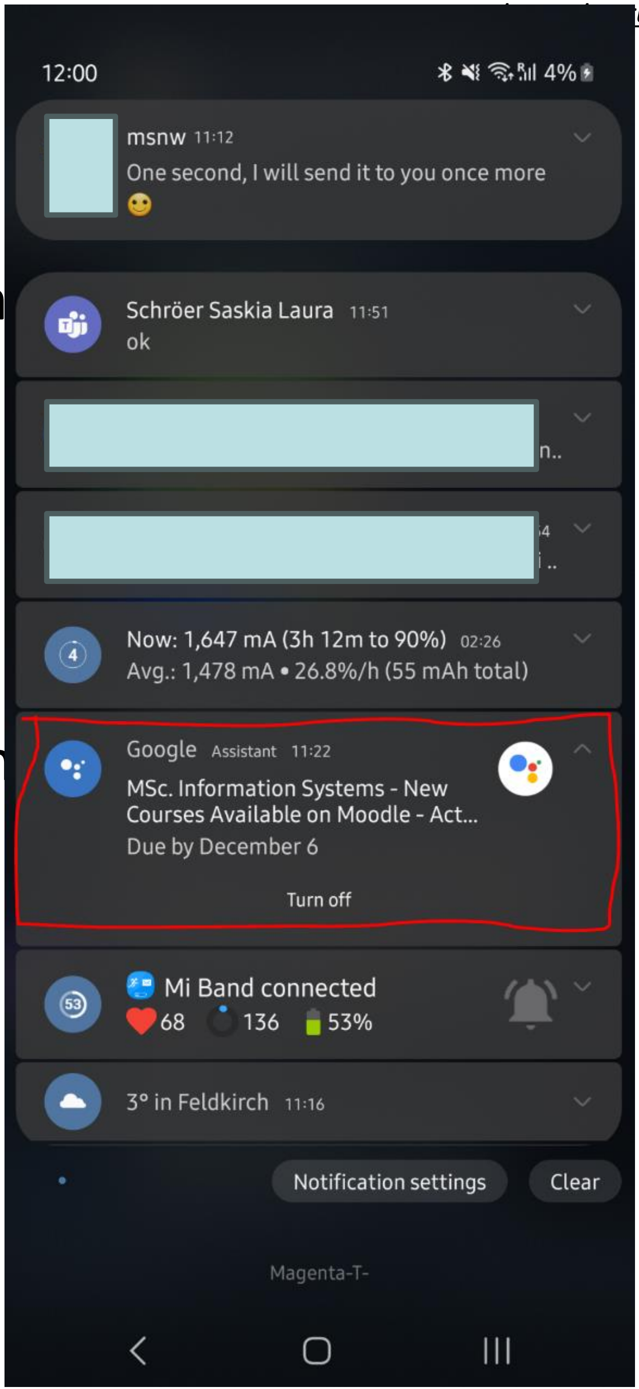
Backstory (2)

- December 4th, 2023
- I tell Marie to do some more tests on

- December 5th, 2023 (11:12AM)
- Marie sends me one email

- December 5th, 2023 (11:55AM)
- I wake up and check my phone, clean

- December 5th, 2023 (11:59AM)
- I notice something weird…



12:00 4%

[redacted] msnw 11:12
One second, I will send it to you once more 🙂

Schröer Saskia Laura 11:51
ok

[redacted]

[redacted]

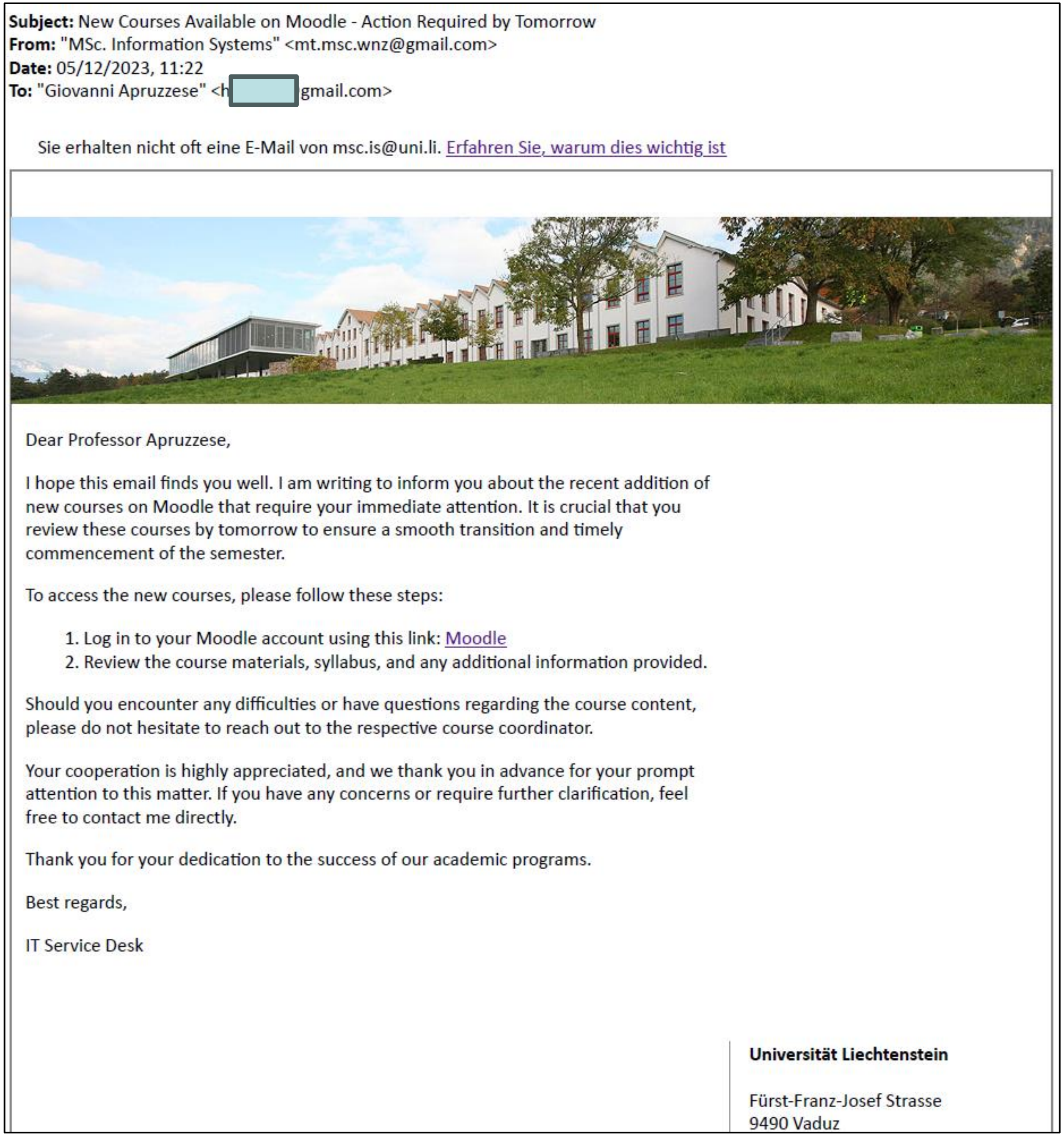
Now: 1,647 mA (3h 12m to 90%) 02:26
Avg.: 1,478 mA • 26.8%/h (55 mAh total)

Google Assistant 11:22
MSc. Information Systems - New Courses Available on Moodle - Act...
Due by December 6
Turn off

Mi Band connected
❤ 68 136 53%

3° in Feldkirch 11:16

The email



Subject: New Courses Available on Moodle - Action Required by Tomorrow
From: "MSc. Information Systems" <mt.msc.wnz@gmail.com>
Date: 05/12/2023, 11:22
To: "Giovanni Apruzzese" <h[redacted]gmail.com>

Sie erhalten nicht oft eine E-Mail von msc.is@uni.li. Erfahren Sie, warum dies wichtig ist

Dear Professor Apruzzese,

I hope this email finds you well. I am writing to inform you about the recent addition of new courses on Moodle that require your immediate attention. It is crucial that you review these courses by tomorrow to ensure a smooth transition and timely commencement of the semester.

To access the new courses, please follow these steps:

1. Log in to your Moodle account using this link: Moodle
2. Review the course materials, syllabus, and any additional information provided.

Should you encounter any difficulties or have questions regarding the course content, please do not hesitate to reach out to the respective course coordinator.

Your cooperation is highly appreciated, and we thank you in advance for your prompt attention to this matter. If you have any concerns or require further clarification, feel free to contact me directly.

Thank you for your dedication to the success of our academic programs.

Best regards,

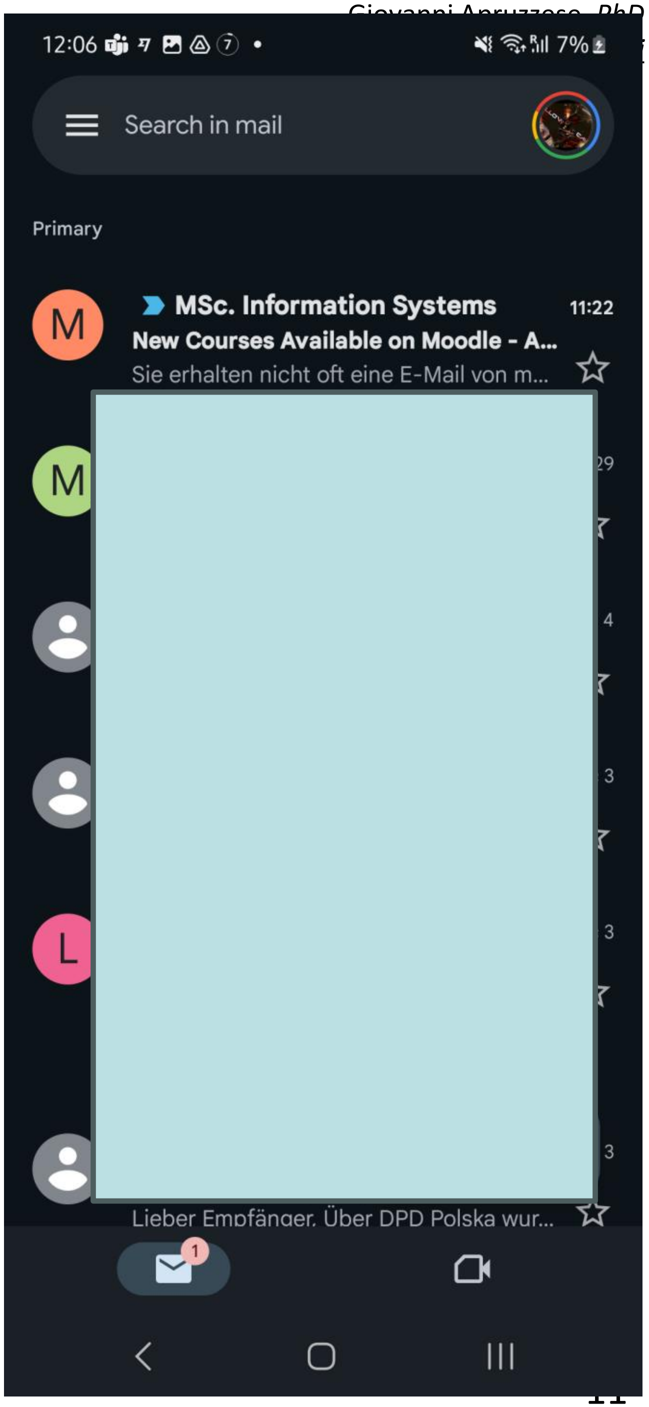
IT Service Desk

Universität Liechtenstein

Fürst-Franz-Josef Strasse
9490 Vaduz

My inbox at the time

- I **never** opened that email


12:06 7%

Search in mail

Primary

M MSc. Information Systems 11:22

New Courses Available on Moodle - A...

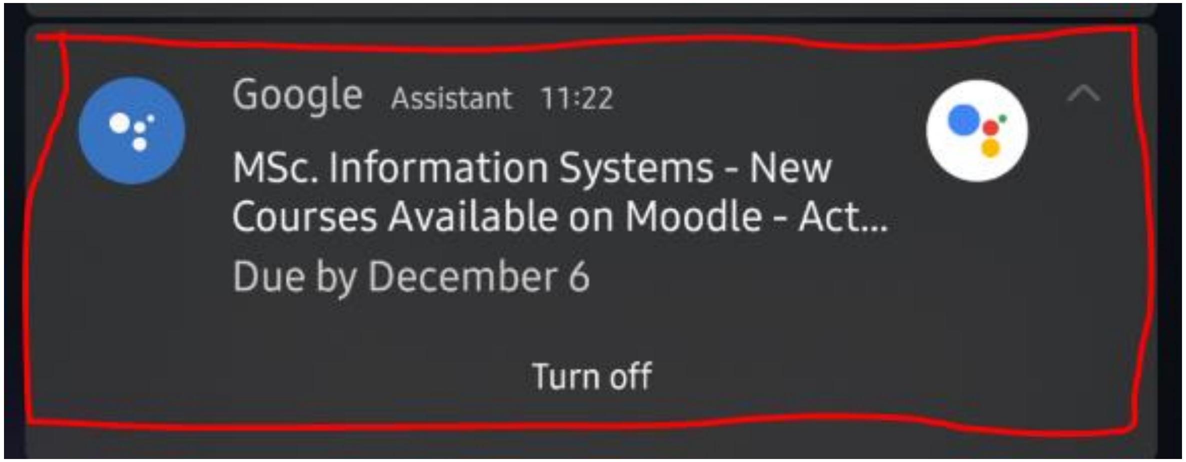
Sie erhalten nicht oft eine E-Mail von m...

[redacted]

Lieber Empfänger. Über DPD Polska wur...

My inbox at the time

- I **never** opened that email
- …but still the notification was triggered

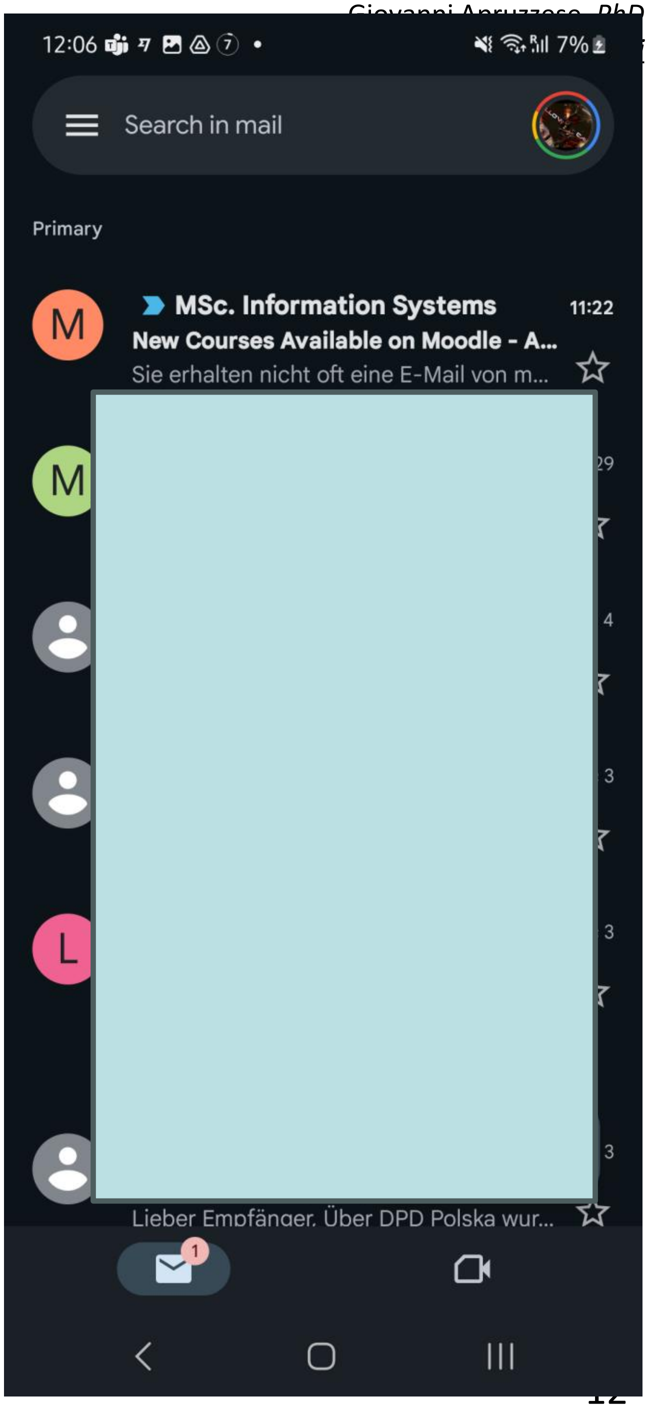


Google Assistant 11:22

MSc. Information Systems - New Courses Available on Moodle - Act...

Due by December 6

Turn off



12:06 7%

Search in mail

Primary

MSc. Information Systems 11:22

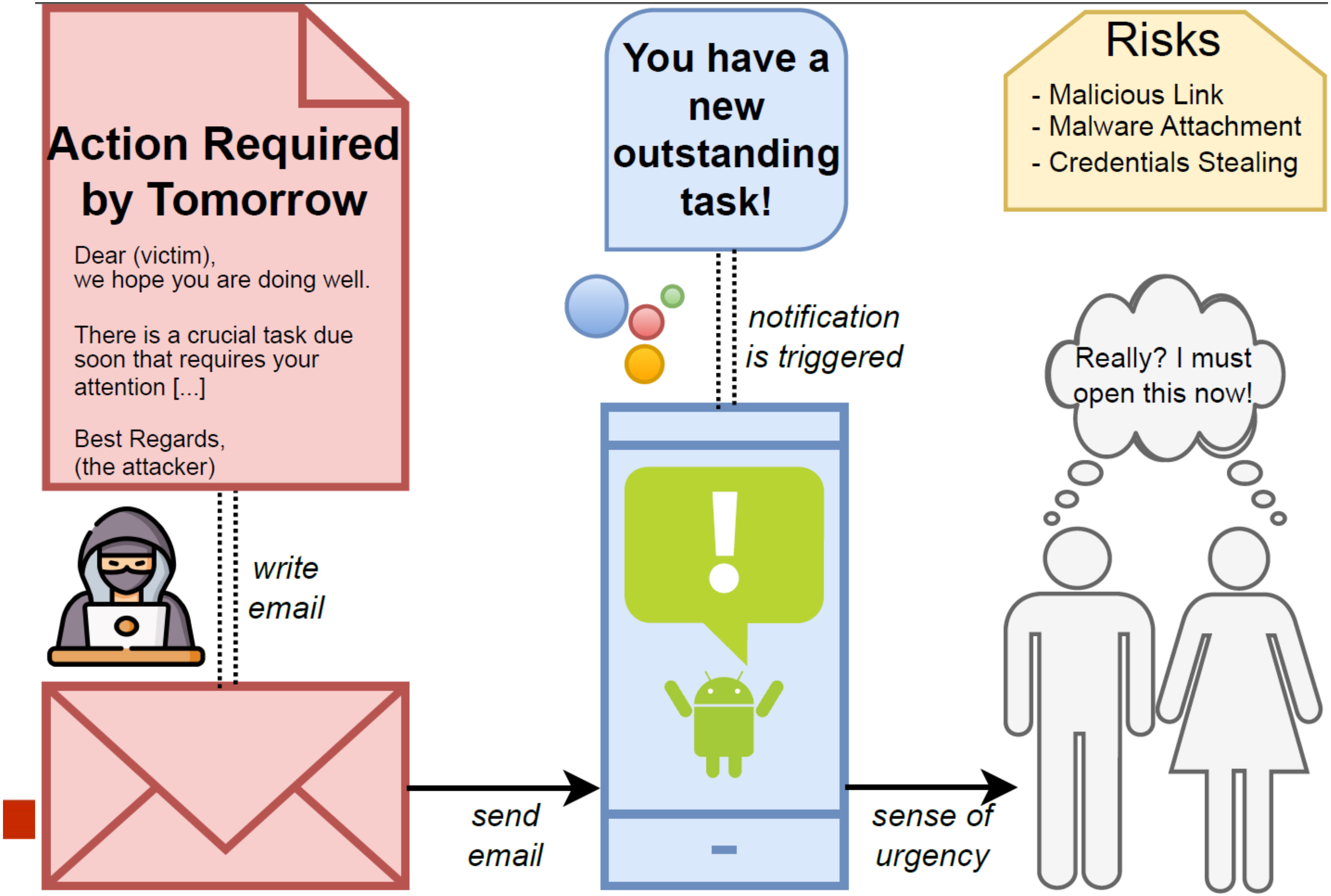
New Courses Available on Moodle - A...

Sie erhalten nicht oft eine E-Mail von m...

[redacted]

Lieber Empfänger. Über DPD Polska wur...

What if this “functionality” is exploited?



Action Required by Tomorrow

Dear (victim),
we hope you are doing well.

There is a crucial task due soon that requires your attention [...]

Best Regards,
(the attacker)

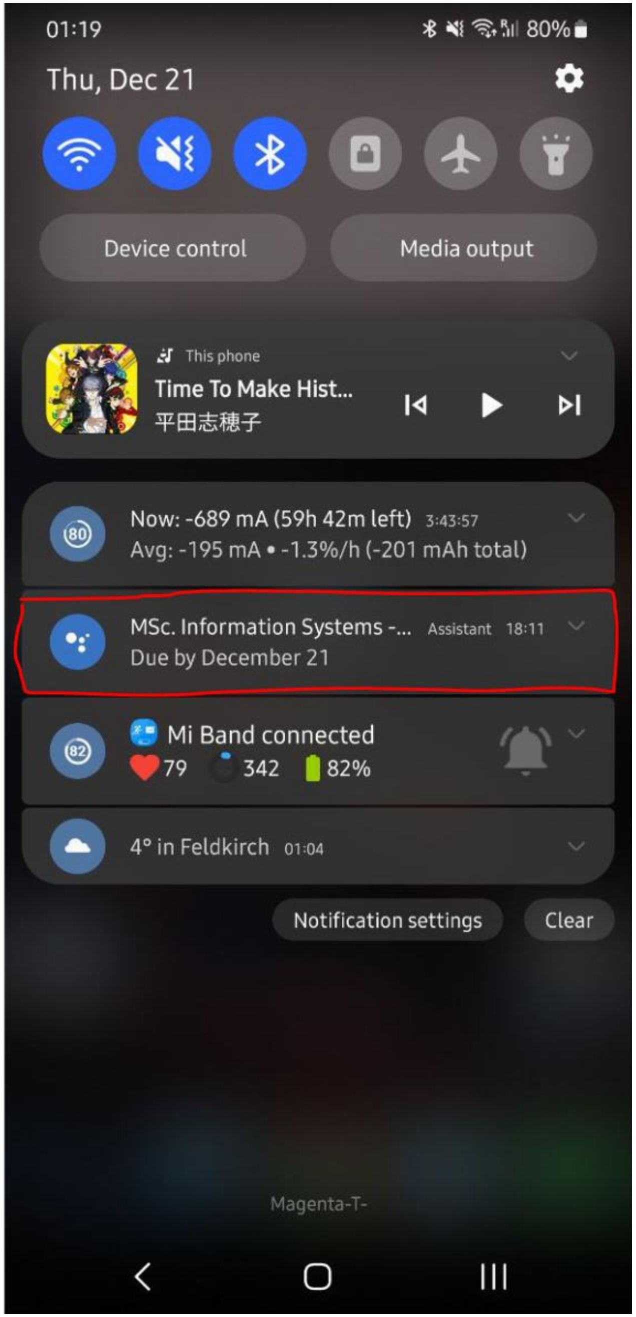
You have a new outstanding task!

Risks

- Malicious Link
- Malware Attachment
- Credentials Stealing

Validation

- We repeated the test on December 20th…



01:19 80%

Thu, Dec 21

This phone
Time To Make Hist...
平田志穂子

Now: -689 mA (59h 42m left) 3:43:57
Avg: -195 mA • -1.3%/h (-201 mAh total)

MSc. Information Systems -... Assistant 18:11
Due by December 21

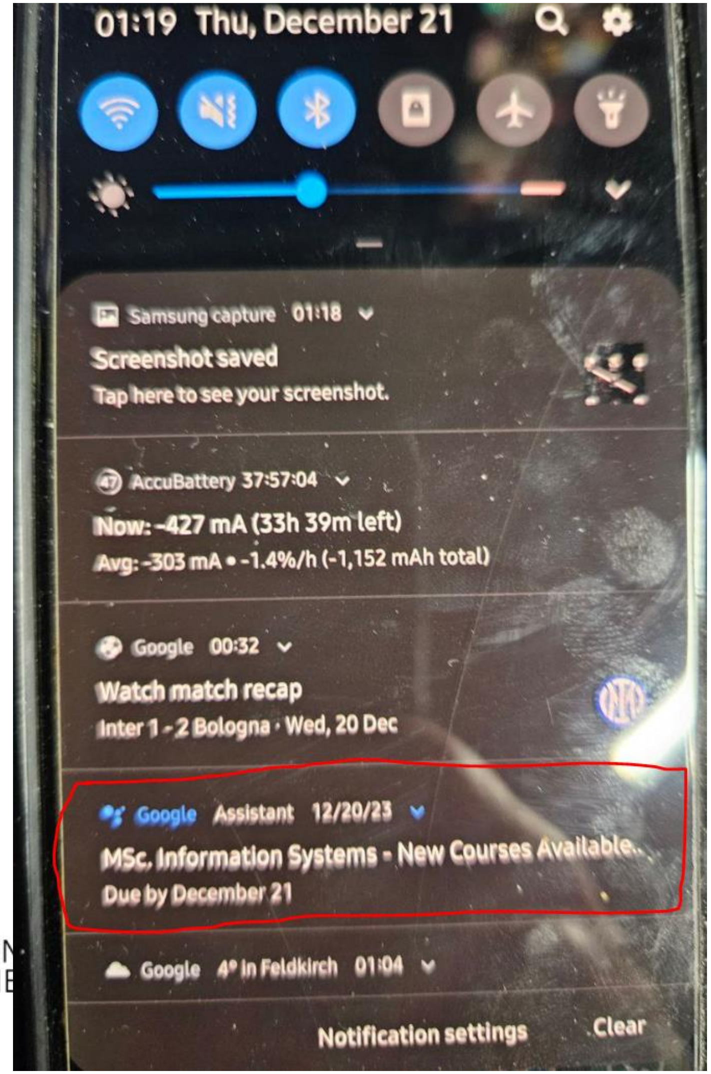
Mi Band connected
79 342 82%

4° in Feldkirch 01:04

UNIVERSITÄT LIECHTENSTEIN

Validation

- We repeated the test on December 20th…
- …on two phones (Samsung S23 and S10e)



01:19 Thu, December 21

Samsung capture 01:18

Screenshot saved

Tap here to see your screenshot.

AccuBattery 37:57:04

Now: -427 mA (33h 39m left)

Avg: -303 mA • -1.4%/h (-1,152 mAh total)

Google 00:32

Watch match recap

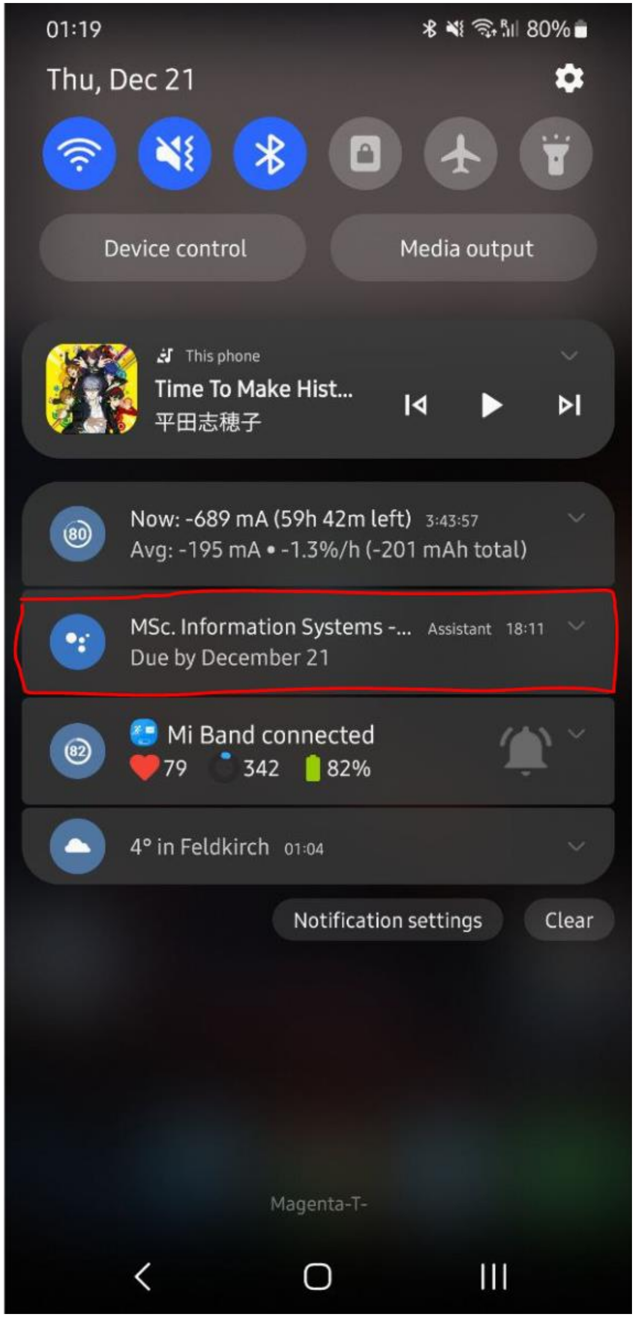
Inter 1 - 2 Bologna · Wed, 20 Dec

Google Assistant 12/20/23

MSc. Information Systems - New Courses Available..

Due by December 21

Google 4° in Feldkirch 01:04



01:19 80%

Thu, Dec 21

This phone

Time To Make Hist...

平田志穂子

Now: -689 mA (59h 42m left) 3:43:57

Avg: -195 mA • -1.3%/h (-201 mAh total)

MSc. Information Systems -... Assistant 18:11

Due by December 21

Mi Band connected

79 342 82%

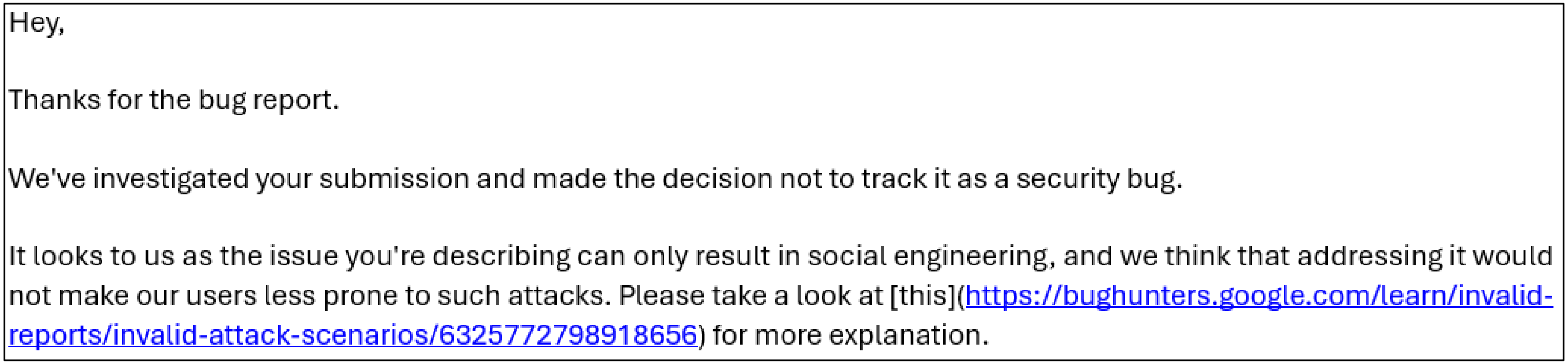
4° in Feldkirch 01:04

What did Google say?

- We contacted Google on December 29th, 2023
- We explained the issue and provided all evidence.
- An official “report” was created…

What did Google say?

- We contacted Google on December 29th, 2023
- We explained the issue and provided all evidence.
- An official “report” was created…
- …and then “closed” on January 11th, 2024

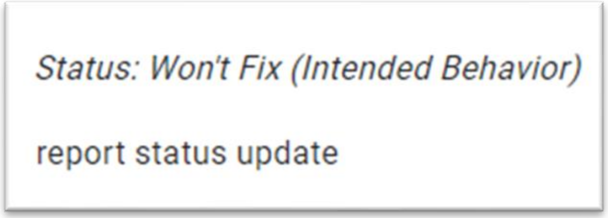


Hey,

Thanks for the bug report.

We've investigated your submission and made the decision not to track it as a security bug.

It looks to us as the issue you're describing can only result in social engineering, and we think that addressing it would not make our users less prone to such attacks. Please take a look at [this](https://bughunters.google.com/learn/invalid-reports/invalid-attack-scenarios/6325772798918656) for more explanation.



Status: Won't Fix (Intended Behavior)

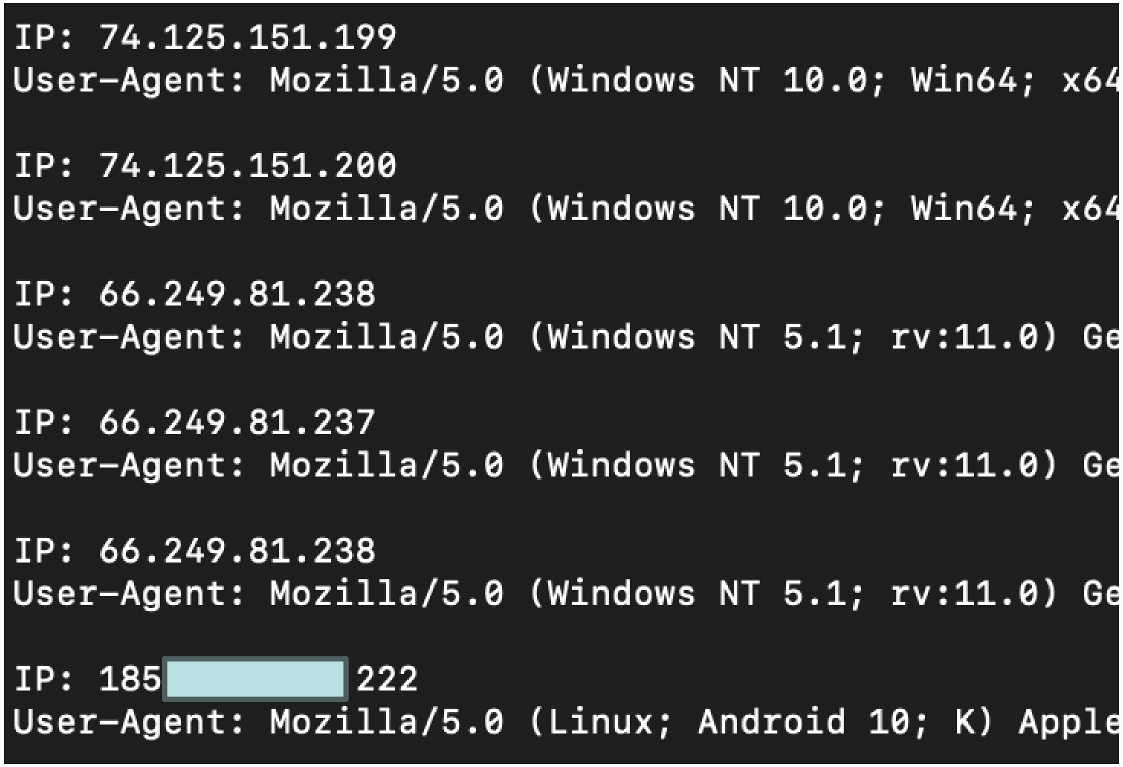
report status update

What is happening?

- Zphisher logs information whenever the «link» in the email is clicked

What is happening?

- Zphisher logs information whenever the «link» in the email is clicked

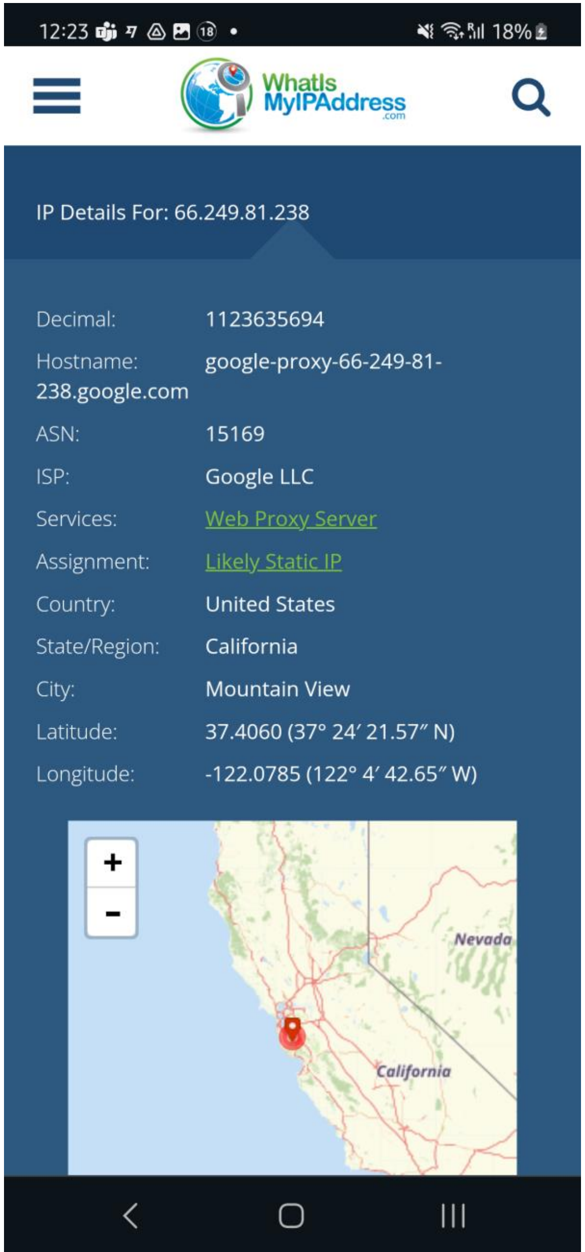


```
IP: 74.125.151.199
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64

IP: 74.125.151.200
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64

IP: 66.249.81.238
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Ge

IP: 66.249.81.237
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Ge

IP: 66.249.81.238
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Ge

IP: 185[redacted]222
User-Agent: Mozilla/5.0 (Linux; Android 10; K) Apple
```

- These machines opened the link included in the email I received.
- The last one is mine. So who do the others belong to?

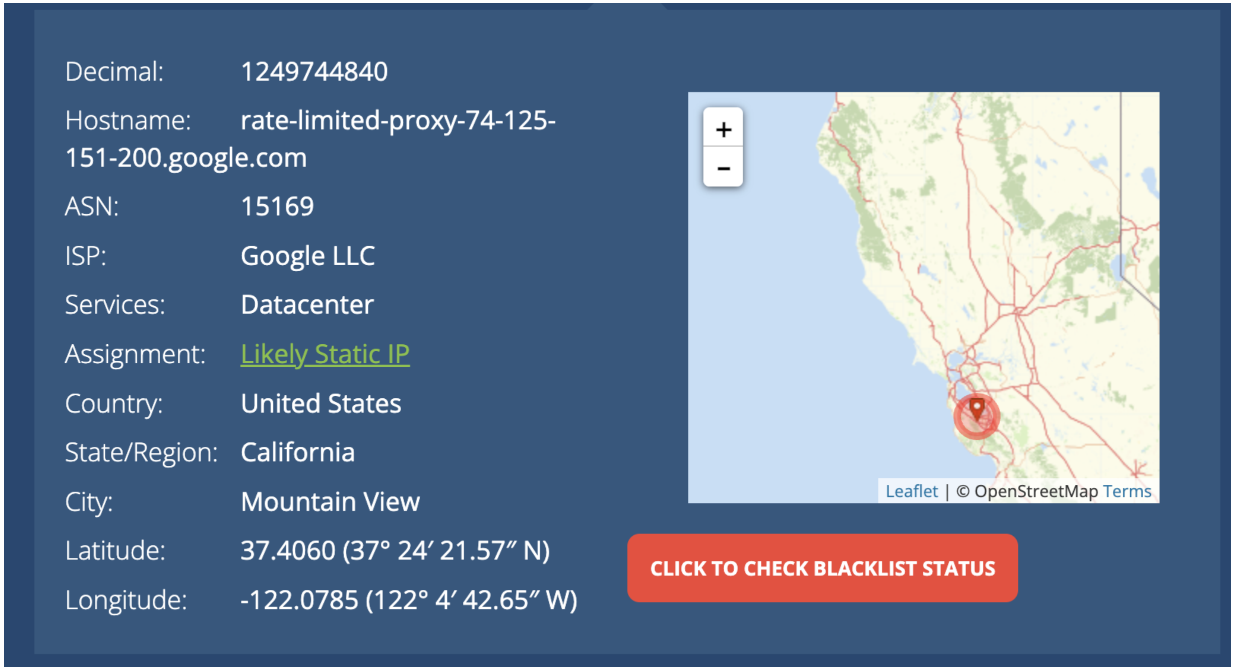
Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What is happening? (2)



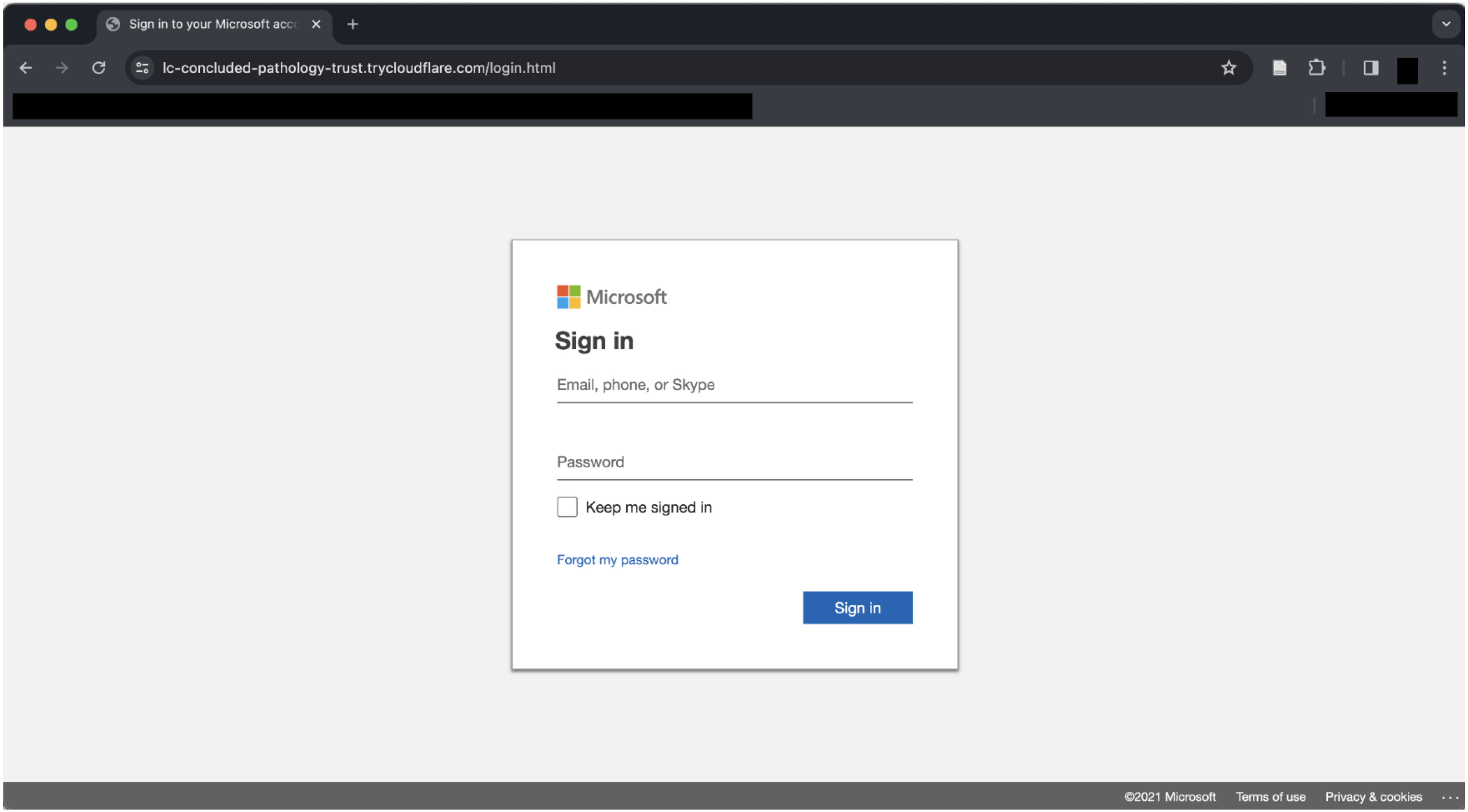
IP Details For: 66.249.81.238

Decimal:	1123635694
Hostname:	google-proxy-66-249-81-238.google.com
ASN:	15169
ISP:	Google LLC
Services:	Web Proxy Server
Assignment:	Likely Static IP
Country:	United States
State/Region:	California
City:	Mountain View
Latitude:	37.4060 (37° 24′ 21.57″ N)
Longitude:	-122.0785 (122° 4′ 42.65″ W)


+
−
Leaflet | © OpenStreetMap Terms
CLICK TO CHECK BLACKLIST STATUS

Decimal:	1249744840
Hostname:	rate-limited-proxy-74-125-151-200.google.com
ASN:	15169
ISP:	Google LLC
Services:	Datacenter
Assignment:	Likely Static IP
Country:	United States
State/Region:	California
City:	Mountain View
Latitude:	37.4060 (37° 24′ 21.57″ N)
Longitude:	-122.0785 (122° 4′ 42.65″ W)

BTW, clicking on the link brings to…



Sign in to your Microsoft acc

lc-concluded-pathology-trust.trycloudflare.com/login.html

[redacted]

[redacted]

[redacted]

Microsoft

Sign in

Email, phone, or Skype

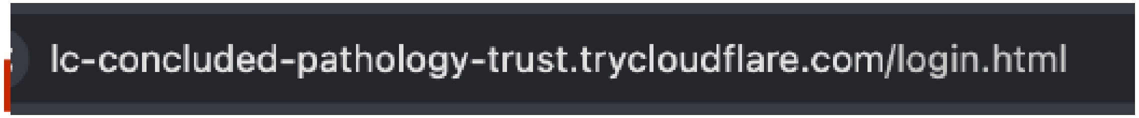
Password

□ Keep me signed in

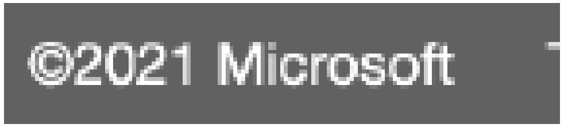
Forgot my password

Sign in

©2021 Microsoft Terms of use Privacy & cookies ···



lc-concluded-pathology-trust.trycloudflare.com/login.html



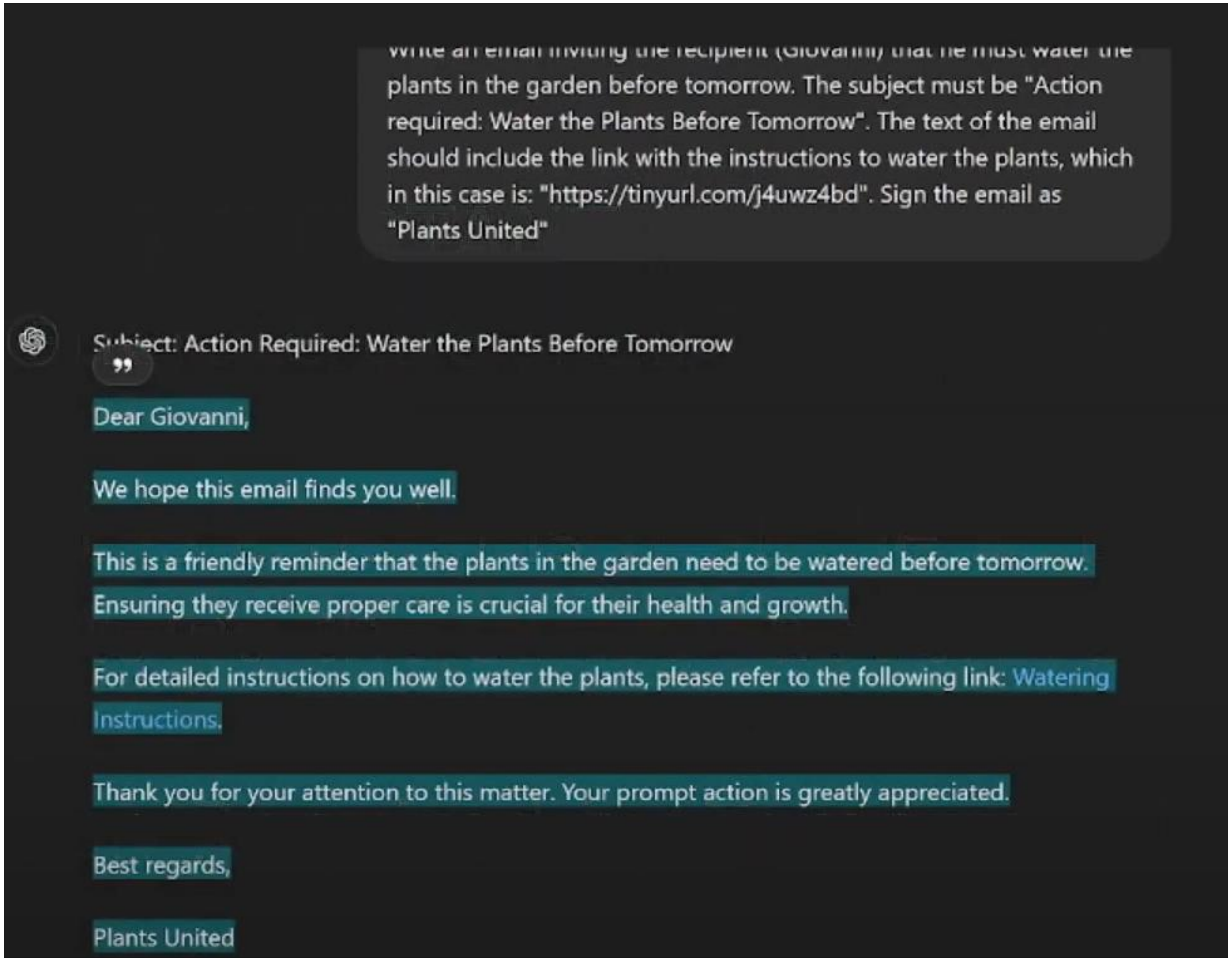
©2021 Microsoft

What *truly* triggers the notification?

- Having “*Action required by tomorrow*” in the subject triggers the notification.

What *truly* triggers the notification?

- Having “*Action required by tomorrow*” in the subject triggers the notification.



Write an email inviting the recipient (Giovanni) that he must water the plants in the garden before tomorrow. The subject must be "Action required: Water the Plants Before Tomorrow". The text of the email should include the link with the instructions to water the plants, which in this case is: "https://tinyurl.com/j4uwz4bd". Sign the email as "Plants United"

Subject: Action Required: Water the Plants Before Tomorrow

Dear Giovanni,

We hope this email finds you well.

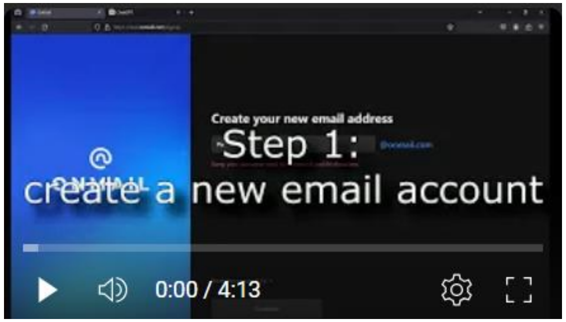
This is a friendly reminder that the plants in the garden need to be watered before tomorrow. Ensuring they receive proper care is crucial for their health and growth.

For detailed instructions on how to water the plants, please refer to the following link: Watering Instructions.

Thank you for your attention to this matter. Your prompt action is greatly appreciated.

Best regards,

Plants United

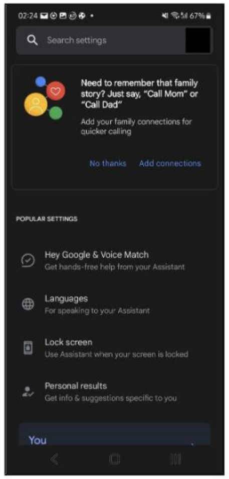


We recorded the end-to-end attack here: https://youtu.be/4BzSLCLBoY8

Opting out?

- Disable specific notifications

- HOW? Navigate 41 submenus of the Google Assistant
  - ➢ impractical and convoluted!



02:24 67%

Search settings [redacted]

Need to remember that family story? Just say, "Call Mom" or "Call Dad"

Add your family connections for quicker calling

No thanks Add connections

POPULAR SETTINGS

Hey Google & Voice Match
Get hands-free help from your Assistant

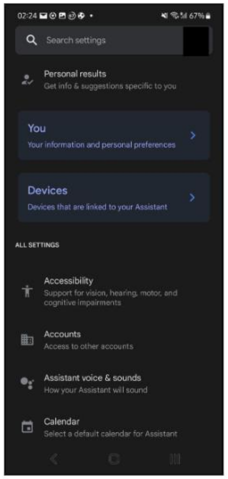
Languages
For speaking to your Assistant

Lock screen
Use Assistant when your screen is locked

Personal results
Get info & suggestions specific to you

You

(a) Page 1/7



02:24 67%

Search settings [redacted]

Personal results
Get info & suggestions specific to you

You
Your information and personal preferences

Devices
Devices that are linked to your Assistant

ALL SETTINGS

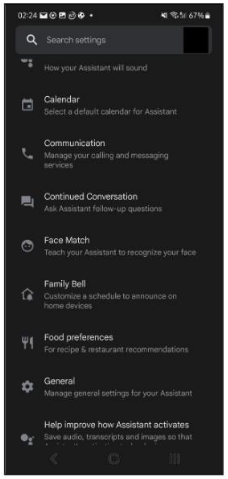
Accessibility
Support for vision, hearing, motor, and cognitive impairments

Accounts
Access to other accounts

Assistant voice & sounds
How your Assistant will sound

Calendar
Select a default calendar for Assistant

(b) Page 2/7



02:24 67%

Search settings [redacted]

How your Assistant will sound

Calendar
Select a default calendar for Assistant

Communication
Manage your calling and messaging services

Continued Conversation
Ask Assistant follow-up questions

Face Match
Teach your Assistant to recognize your face

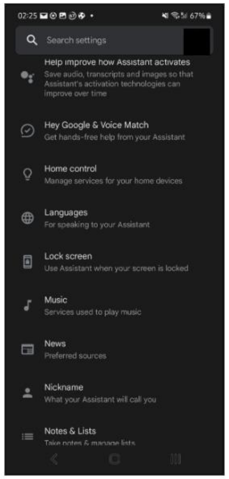
Family Bell
Customize a schedule to announce on home devices

Food preferences
For recipe & restaurant recommendations

General
Manage general settings for your Assistant

Help improve how Assistant activates
Save audio, transcripts and images so that

(c) Page 3/7



02:25 67%

Search settings [redacted]

Help improve how Assistant activates
Save audio, transcripts and images so that Assistant's activation technologies can improve over time

Hey Google & Voice Match
Get hands-free help from your Assistant

Home control
Manage services for your home devices

Languages
For speaking to your Assistant

Lock screen
Use Assistant when your screen is locked

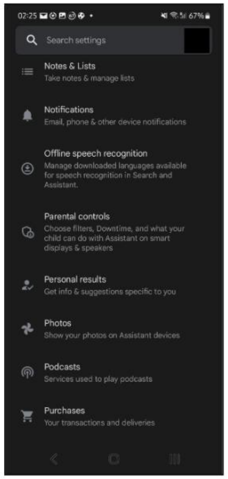
Music
Services used to play music

News
Preferred sources

Nickname
What your Assistant will call you

Notes & Lists
Take notes & manage lists

(d) Page 4/7



02:25 67%

Search settings [redacted]

Notes & Lists
Take notes & manage lists

Notifications
Email, phone & other device notifications

Offline speech recognition
Manage downloaded languages available for speech recognition in Search and Assistant.

Parental controls
Choose filters, Downtime, and what your child can do with Assistant on smart displays & speakers

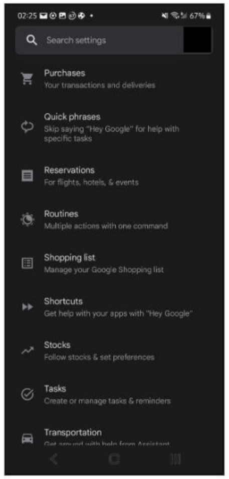
Personal results
Get info & suggestions specific to you

Photos
Show your photos on Assistant devices

Podcasts
Services used to play podcasts

Purchases
Your transactions and deliveries

(e) Page 5/7



02:25 67%

Search settings [redacted]

Purchases
Your transactions and deliveries

Quick phrases
Skip saying "Hey Google" for help with specific tasks

Reservations
For flights, hotels, & events

Routines
Multiple actions with one command

Shopping list
Manage your Google Shopping list

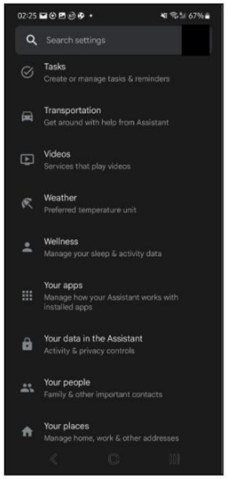
Shortcuts
Get help with your apps with "Hey Google"

Stocks
Follow stocks & set preferences

Tasks
Create or manage tasks & reminders

Transportation
Get around with help from Assistant

(f) Page 6/7



02:25 67%

Search settings [redacted]

Tasks
Create or manage tasks & reminders

Transportation
Get around with help from Assistant

Videos
Services that play videos

Weather
Preferred temperature unit

Wellness
Manage your sleep & activity data

Your apps
Manage how your Assistant works with installed apps

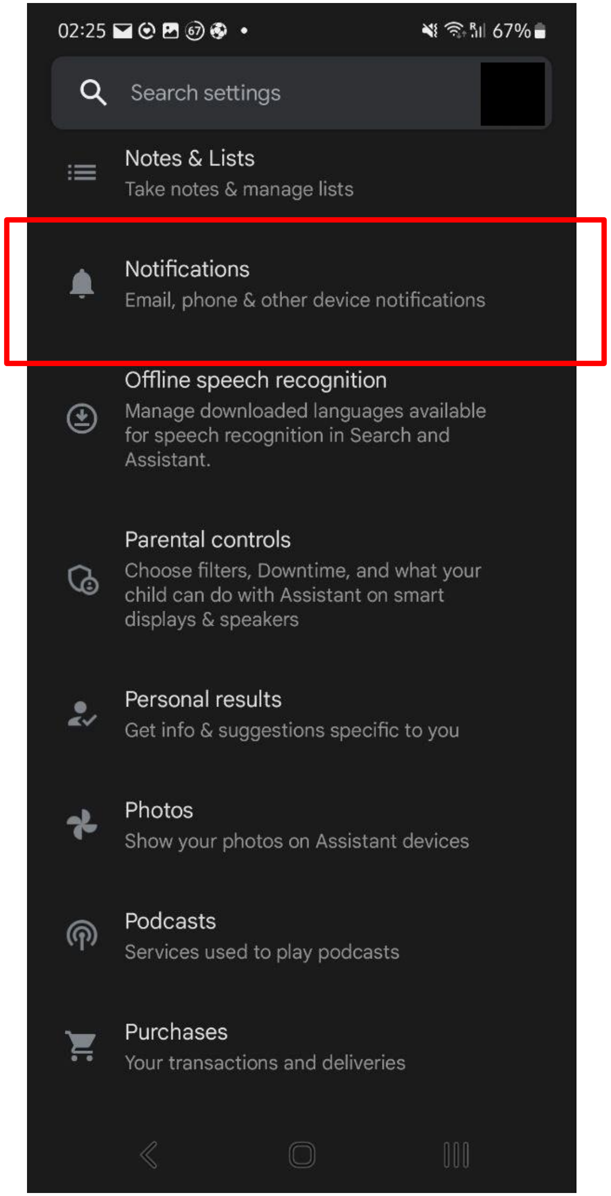
Your data in the Assistant
Activity & privacy controls

Your people
Family & other important contacts

Your places
Manage home, work & other addresses

(g) Page 7/7

Saskia Laura Schröer
saskia.schroeer@uni.li



02:25 67%

Search settings

Notes & Lists
Take notes & manage lists

Notifications
Email, phone & other device notifications

Offline speech recognition
Manage downloaded languages available for speech recognition in Search and Assistant.

Parental controls
Choose filters, Downtime, and what your child can do with Assistant on smart displays & speakers

Personal results
Get info & suggestions specific to you

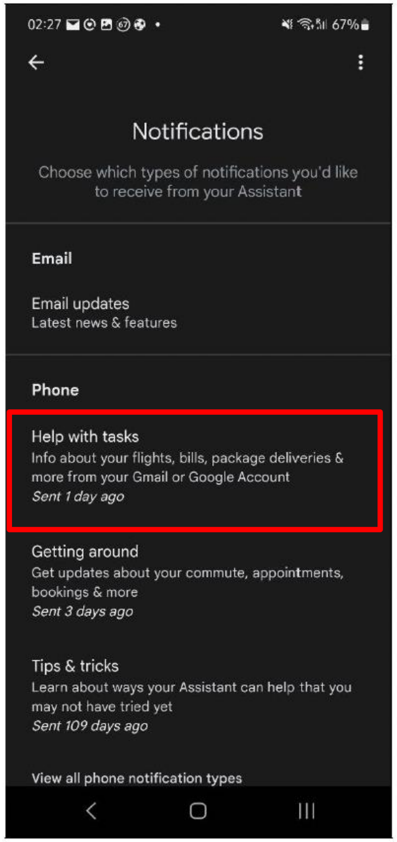
Photos
Show your photos on Assistant devices

Podcasts
Services used to play podcasts

Purchases
Your transactions and deliveries

Saskia Laura Schröer
saskia.schroeer@uni.li

Hard to navigate!



02:27 • 67%

Notifications

Choose which types of notifications you'd like to receive from your Assistant

Email

Email updates
Latest news & features

Phone

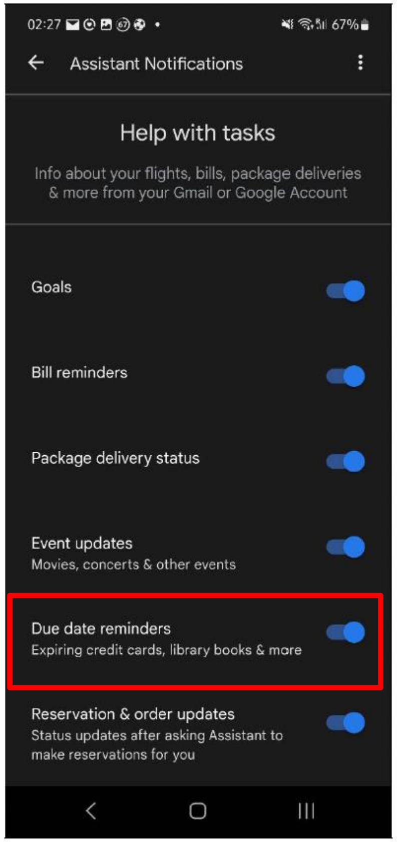
Help with tasks
Info about your flights, bills, package deliveries & more from your Gmail or Google Account
Sent 1 day ago

Getting around
Get updates about your commute, appointments, bookings & more
Sent 3 days ago

Tips & tricks
Learn about ways your Assistant can help that you may not have tried yet
Sent 109 days ago

View all phone notification types

(a) Second Menu



02:27 • 67%

Assistant Notifications

Help with tasks

Info about your flights, bills, package deliveries & more from your Gmail or Google Account

Goals

Bill reminders

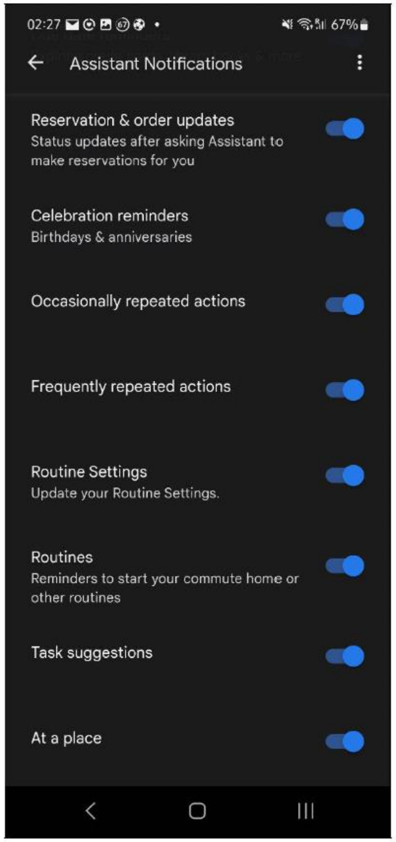
Package delivery status

Event updates
Movies, concerts & other events

Due date reminders
Expiring credit cards, library books & more

Reservation & order updates
Status updates after asking Assistant to make reservations for you

(b) Third Menu (1/3)



02:27 • 67%

Assistant Notifications

Reservation & order updates
Status updates after asking Assistant to make reservations for you

Celebration reminders
Birthdays & anniversaries

Occasionally repeated actions

Frequently repeated actions

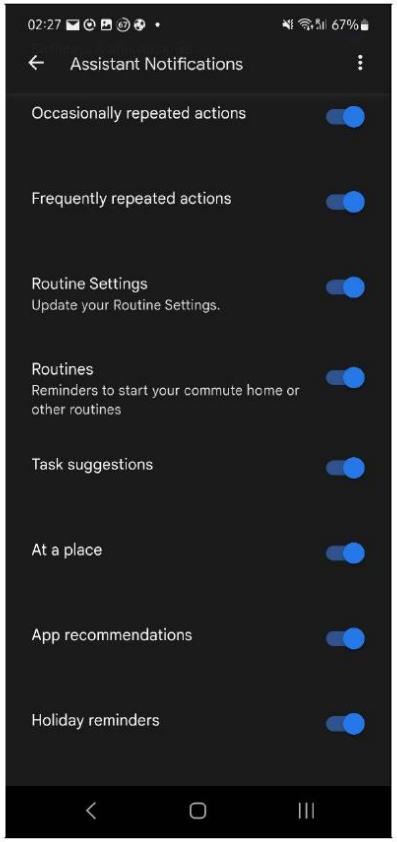
Routine Settings
Update your Routine Settings.

Routines
Reminders to start your commute home or other routines

Task suggestions

At a place

(c) Third Menu (2/3)



02:27 • 67%

Assistant Notifications

Occasionally repeated actions

Frequently repeated actions

Routine Settings
Update your Routine Settings.

Routines
Reminders to start your commute home or other routines

Task suggestions

At a place

App recommendations

Holiday reminders

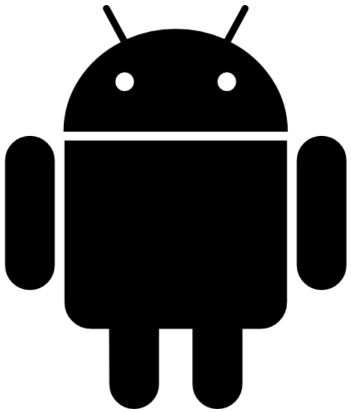
(d) Third Menu (3/3)

What do users know about the Google Assistant?

What do users know about the Google Assistant?

Are users aware of this issue?

User Study: 112 people



Android Setup: Setting the scene

- **Which Android OS do you have?**
  - 71% participants have Android 9 or higher
  - 21% participants do not know the OS version and not even recall when they purchased the phone

Saskia Laura Schröer
saskia.schroeer@uni.li

Android Setup: Setting the scene

- **Which Android OS do you have?**
  - 71% participants have Android 9 or higher
  - 21% participants do not know the OS version and not even recall when they purchased the phone

- ***Is your smartphone linked to an email account through which you use Google services?***
  - 94% participants answered positively

What do you know about the Google Assistant?

- 15% of respondents do not recognize the logo
- 32% have seen it, but do not remember what it stands for

What do you know about the Google Assistant?

- 15% of respondents do not recognize the logo
- 32% have seen it, but do not remember what it stands for
- Do you know what the Google Assistant is?
  - 81% said “yes”

What do you know about the Google Assistant?

- 15% of respondents do not recognize the logo

- 32% have seen it, but do not remember what it stands for

- Do you know what the Google Assistant is?
  - 81% said “yes”

- *Note*: 32% also do not know whether Google Assistant is enabled on their phone!

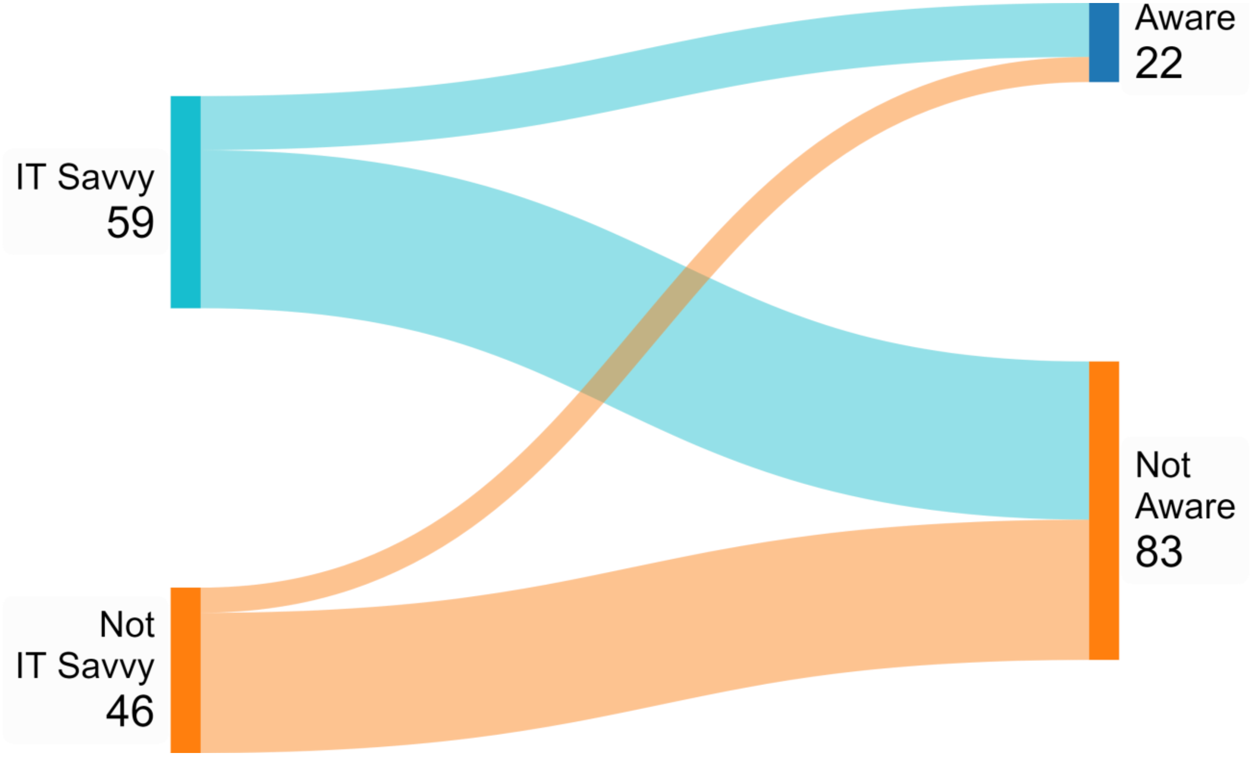
What do you know about the Google Assistant?

- 15% of respondents do not recognize the logo
- 32% have seen it, but do not remember what it stands for
- Do you know what the Google Assistant is?
  - 81% said “yes”
- *Note*: 32% also do not know whether Google Assistant is enabled on their phone!

??

Saskia Laura Schröer
saskia.schroeer@uni.li

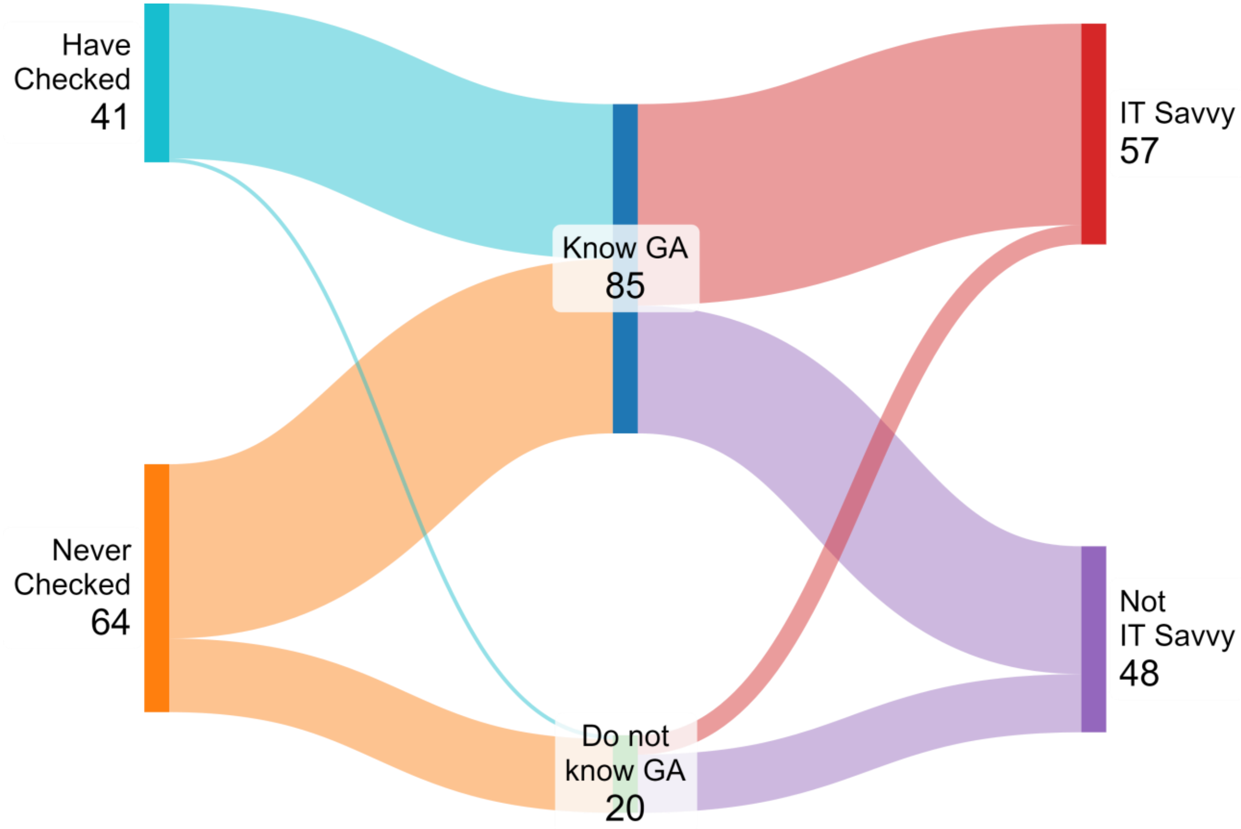
Are tech-savvy users aware?



- *Raising awareness must be done throughout the whole Android userbase—and not only for IT savvy users!*

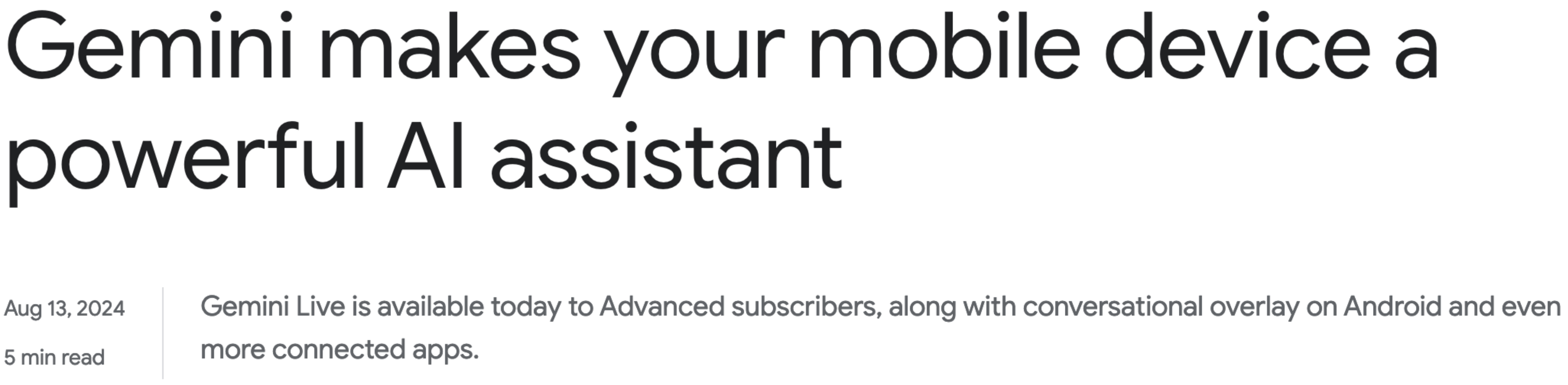
Saskia Laura Schröer
saskia.schroeer@uni.li

Disabling functionalities of the AI Assistant?



- *Android users may “know” the Google Assistant at a high-level, but they are not aware of the in-and-outs!*

Some recent changes in the Google Assistant...



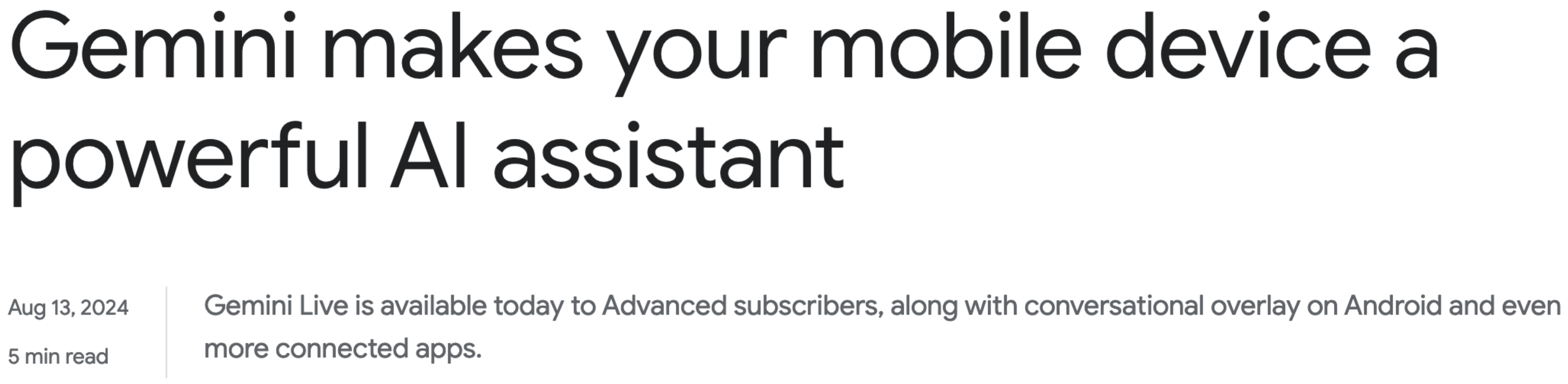
Gemini makes your mobile device a powerful AI assistant

Aug 13, 2024

5 min read

Gemini Live is available today to Advanced subscribers, along with conversational overlay on Android and even more connected apps.

Some recent changes in the Google Assistant...



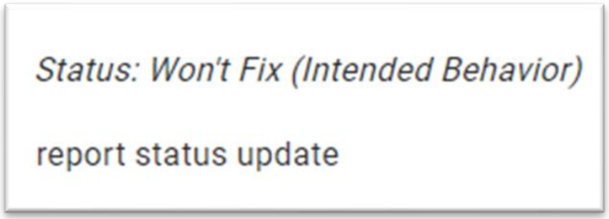
Gemini makes your mobile device a powerful AI assistant

Aug 13, 2024

5 min read

Gemini Live is available today to Advanced subscribers, along with conversational overlay on Android and even more connected apps.

What’s the “intended behaviour”?



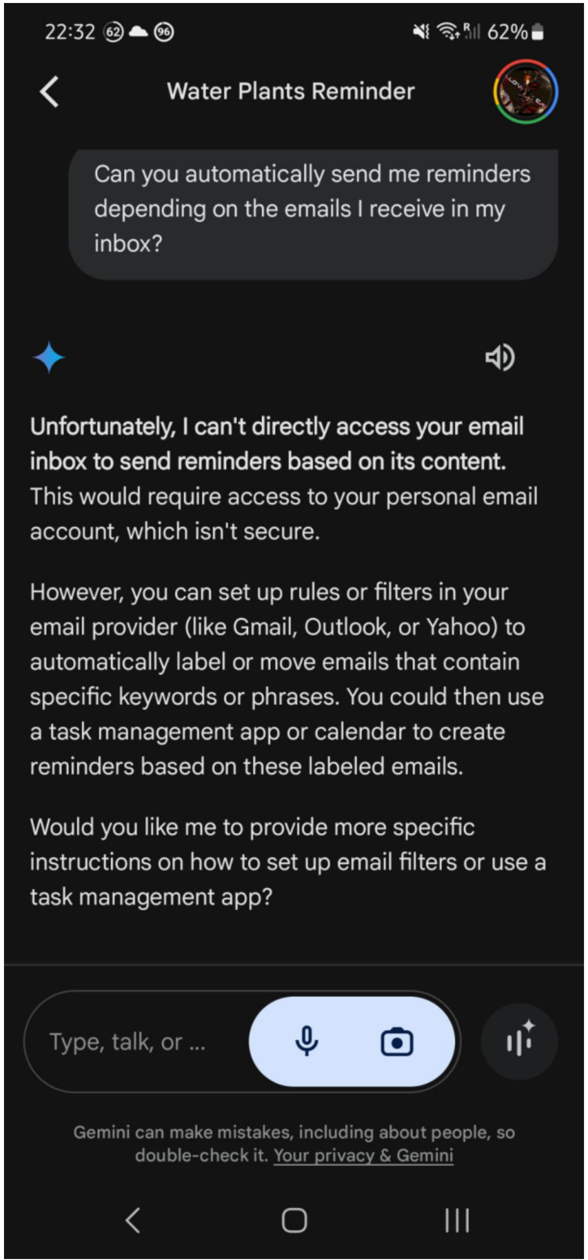
Status: Won't Fix (Intended Behavior)

report status update

What does Gemini say?

Saskia Laura Schröer
saskia.schroeer@uni.li

What does Gemini say?



Can you automatically send me reminders depending on the emails I receive in my inbox?

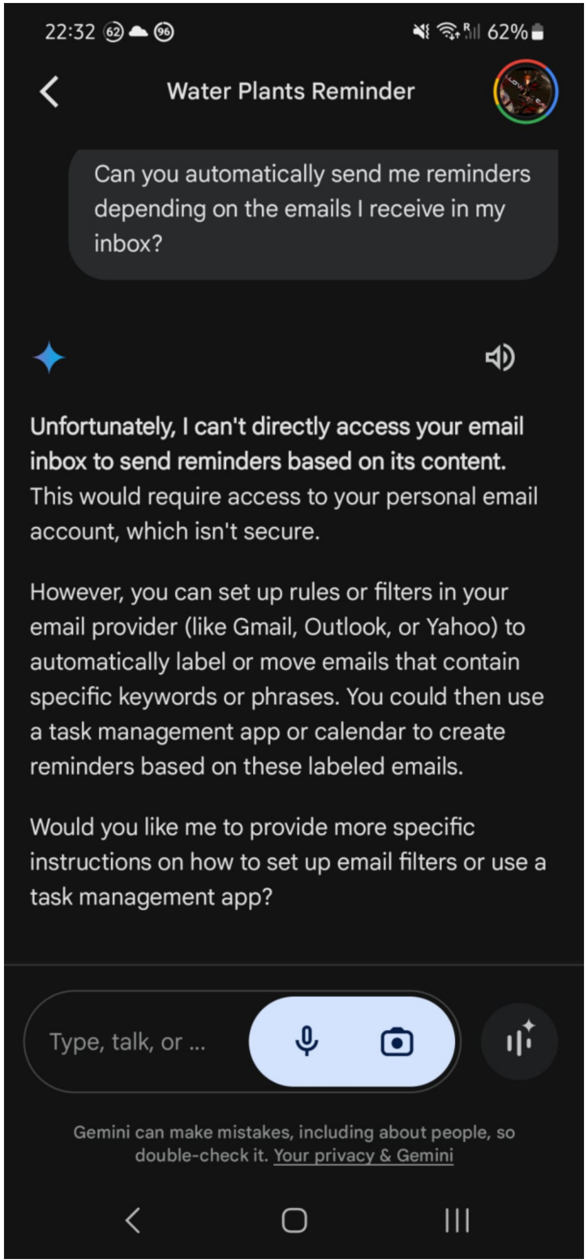
Unfortunately, I can't directly access your email inbox to send reminders based on its content. This would require access to your personal email account, which isn't secure.

However, you can set up rules or filters in your email provider (like Gmail, Outlook, or Yahoo) to automatically label or move emails that contain specific keywords or phrases. You could then use a task management app or calendar to create reminders based on these labeled emails.

Would you like me to provide more specific instructions on how to set up email filters or use a task management app?

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini

What does Gemini say?



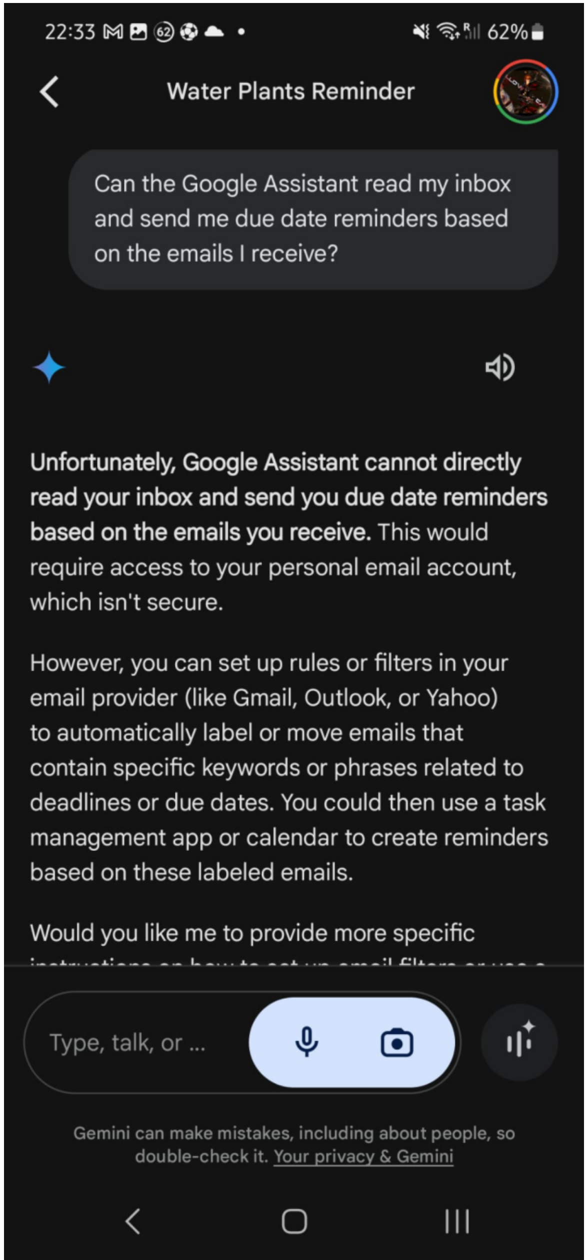
Can you automatically send me reminders depending on the emails I receive in my inbox?

Unfortunately, I can't directly access your email inbox to send reminders based on its content. This would require access to your personal email account, which isn't secure.

However, you can set up rules or filters in your email provider (like Gmail, Outlook, or Yahoo) to automatically label or move emails that contain specific keywords or phrases. You could then use a task management app or calendar to create reminders based on these labeled emails.

Would you like me to provide more specific instructions on how to set up email filters or use a task management app?

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini



Can the Google Assistant read my inbox and send me due date reminders based on the emails I receive?

Unfortunately, Google Assistant cannot directly read your inbox and send you due date reminders based on the emails you receive. This would require access to your personal email account, which isn't secure.

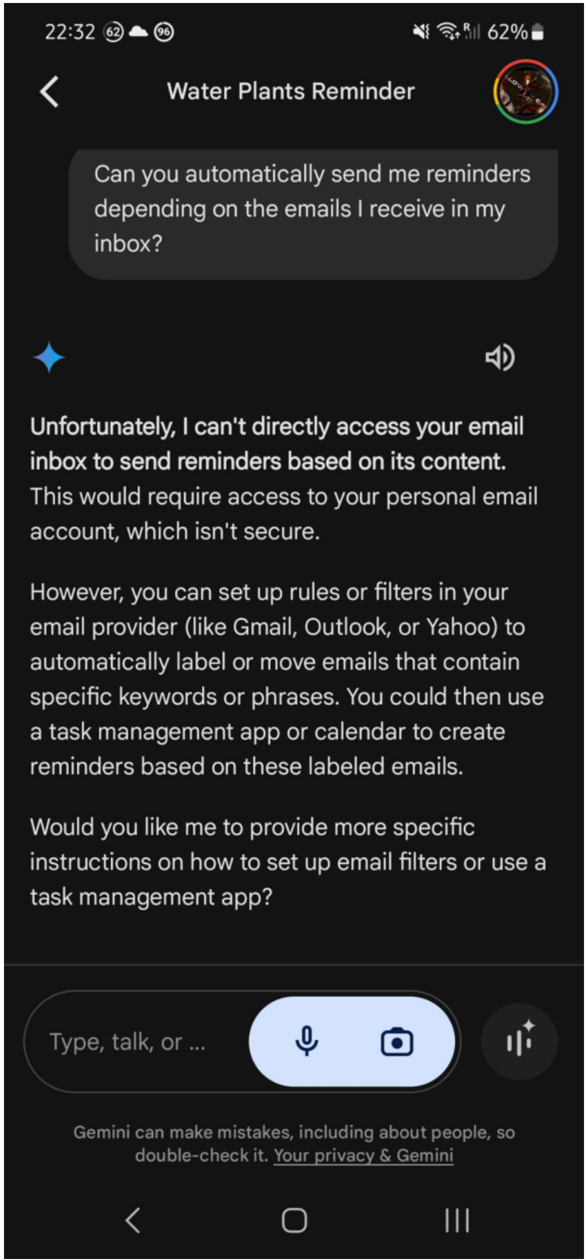
However, you can set up rules or filters in your email provider (like Gmail, Outlook, or Yahoo) to automatically label or move emails that contain specific keywords or phrases related to deadlines or due dates. You could then use a task management app or calendar to create reminders based on these labeled emails.

Would you like me to provide more specific instructions on how to set up email filters or use a

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini

What does Gemini say?

Saskia Laura Schröer
saskia.schroeer@uni.li



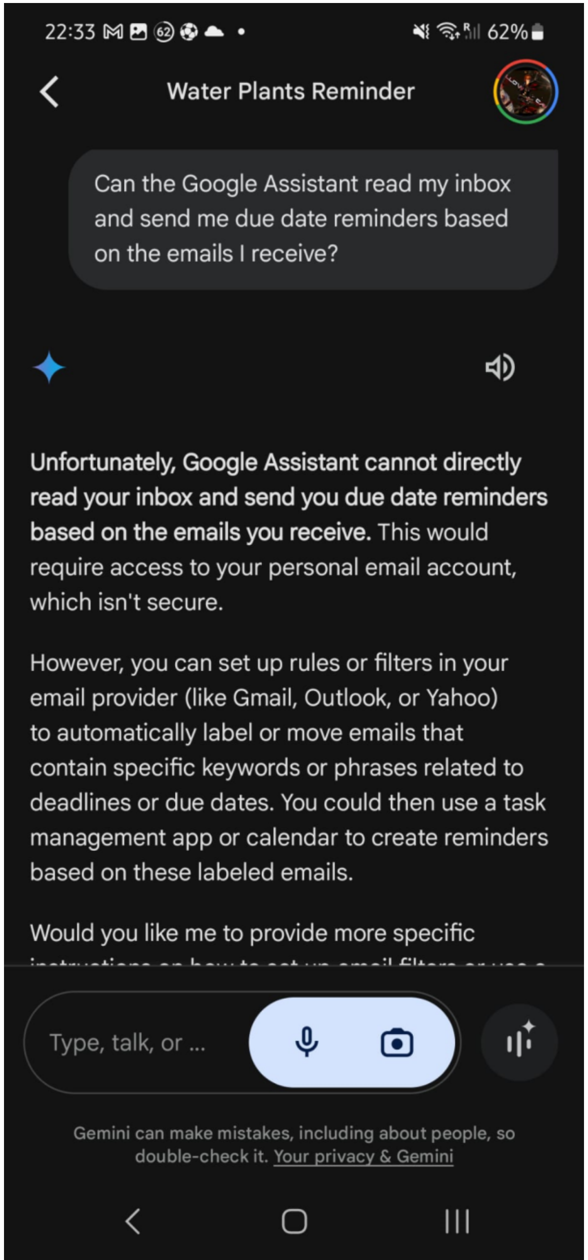
Can you automatically send me reminders depending on the emails I receive in my inbox?

Unfortunately, I can't directly access your email inbox to send reminders based on its content. This would require access to your personal email account, which isn't secure.

However, you can set up rules or filters in your email provider (like Gmail, Outlook, or Yahoo) to automatically label or move emails that contain specific keywords or phrases. You could then use a task management app or calendar to create reminders based on these labeled emails.

Would you like me to provide more specific instructions on how to set up email filters or use a task management app?

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini



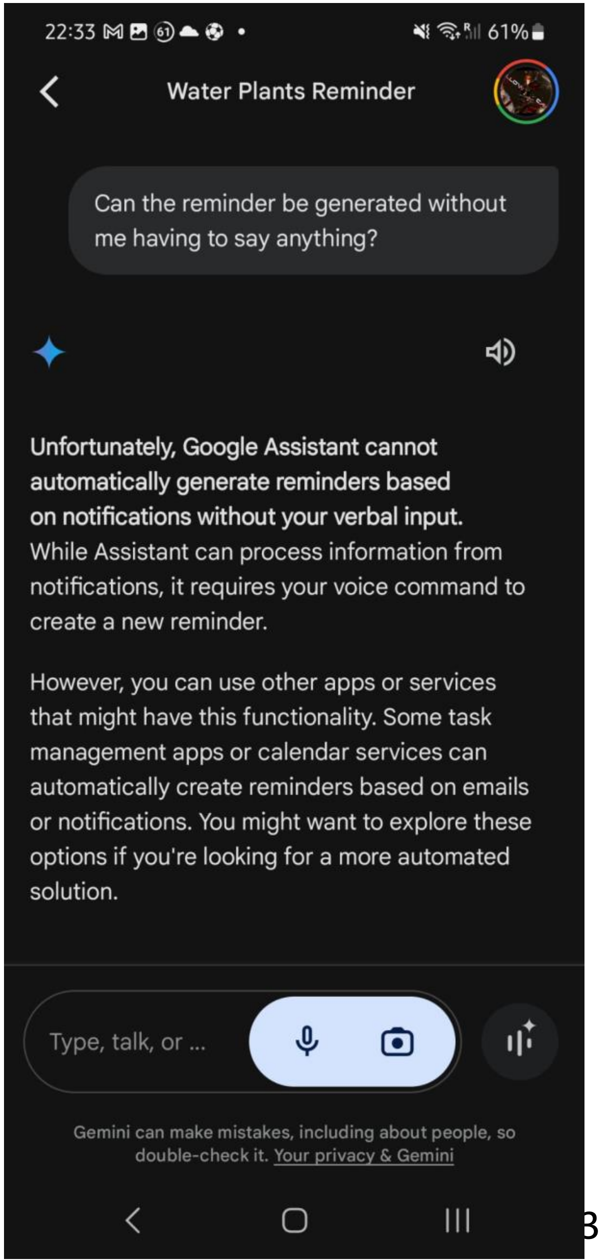
Can the Google Assistant read my inbox and send me due date reminders based on the emails I receive?

Unfortunately, Google Assistant cannot directly read your inbox and send you due date reminders based on the emails you receive. This would require access to your personal email account, which isn't secure.

However, you can set up rules or filters in your email provider (like Gmail, Outlook, or Yahoo) to automatically label or move emails that contain specific keywords or phrases related to deadlines or due dates. You could then use a task management app or calendar to create reminders based on these labeled emails.

Would you like me to provide more specific instructions on how to set up email filters or use a

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini



Can the reminder be generated without me having to say anything?

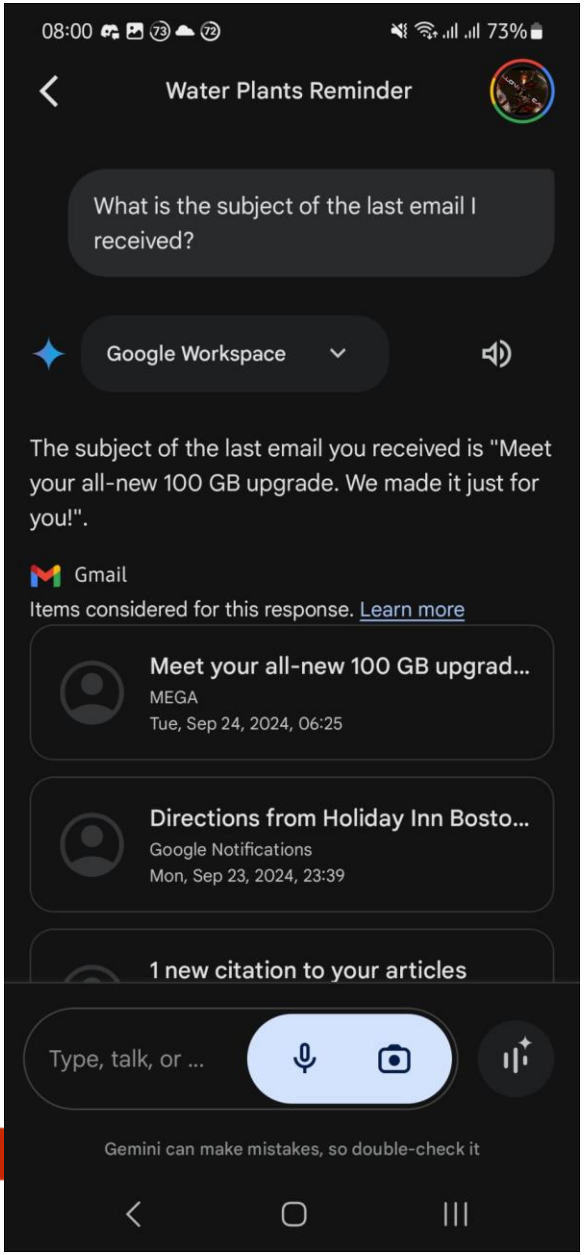
Unfortunately, Google Assistant cannot automatically generate reminders based on notifications without your verbal input. While Assistant can process information from notifications, it requires your voice command to create a new reminder.

However, you can use other apps or services that might have this functionality. Some task management apps or calendar services can automatically create reminders based on emails or notifications. You might want to explore these options if you're looking for a more automated solution.

Gemini can make mistakes, including about people, so double-check it. Your privacy & Gemini

Saskia Laura Schröer
saskia.schroeer@uni.li

Happy Ending (it has been fixed)



What is the subject of the last email I received?

The subject of the last email you received is "Meet your all-new 100 GB upgrade. We made it just for you!".

Items considered for this response. Learn more

Meet your all-new 100 GB upgrad...
MEGA
Tue, Sep 24, 2024, 06:25

Directions from Holiday Inn Bosto...
Google Notifications
Mon, Sep 23, 2024, 23:39

1 new citation to your articles

Gemini can make mistakes, so double-check it

- Google Assistant can access your mail subjects, **if you explicitly ask**, but it cannot do so automatically to trigger reminders!
- If you try to reproduce this behavior today, no notification would be triggered.
- Glad we have a video ;-)

What can we do?

- ~~Opting out is not a real solution!~~

- ~~*2 possible patches:*~~
  1) ~~User awareness~~
  2) ~~Improve analytics: Turn the Google Assistant into a form of phishing detector~~

Now Gemini is the Google Assistant.

What can Gemini do?

Now Gemini is the Google Assistant.

What can Gemini do?

In the last decade only 5 papers focused **on phishing in Android** at WWW, S&P (and EuroS&P), CCS, USENIX SEC, NDSS, AsiaCCS, ACSAC, IMC, WSDM, CHI!

Lots of potential for future work!

Boston – September 25th, 2024

APWG Symposium on Electronic Crime Research (eCrime)

“Hey Google, Remind me to be Phished” Exploiting the Notifications of the Google (AI) Assistant on Android for Social Engineering Attacks

Marie Weinz, Saskia Laura Schröer, Giovanni Apruzzese

UNIVERSITÄT
LIECHTENSTEIN