Apple iOS UI Access Permission Vulnerabilities

“iOS v6.0 – iOS v12.0.1!”

Benjamin Mejri (Kunz)
Vulnerability Laboratory
Evolution Security GmbH

What are UI Access Permission Vulnerabilities in iOS?

Characteristics:

- Allows access to sensitive data of idevice
- Pictures, Contacts, Mails, Messages & more
- Usage of a glitch or design error (not required!)
- Passcode Bypass – Yes & No?
- Unauthenticated access without passcode
- Manual Interaction
- No exploit code but local pocs

How to identify an UI Access Permission Vulnerability?

Physical Requirements

- Different idevices of the apple corporation
- Newst ios mobile operating system
- Default setup of the idevice configuration
- Testing environment (Research)
- ... motivation, a lot of time & some sticky fingers

Testing Environment on Research

Technical Requirements

- 2 Ways Decision
- Manual interaction – Be the player one
- Automated Fuzzing? Lego robot scores!

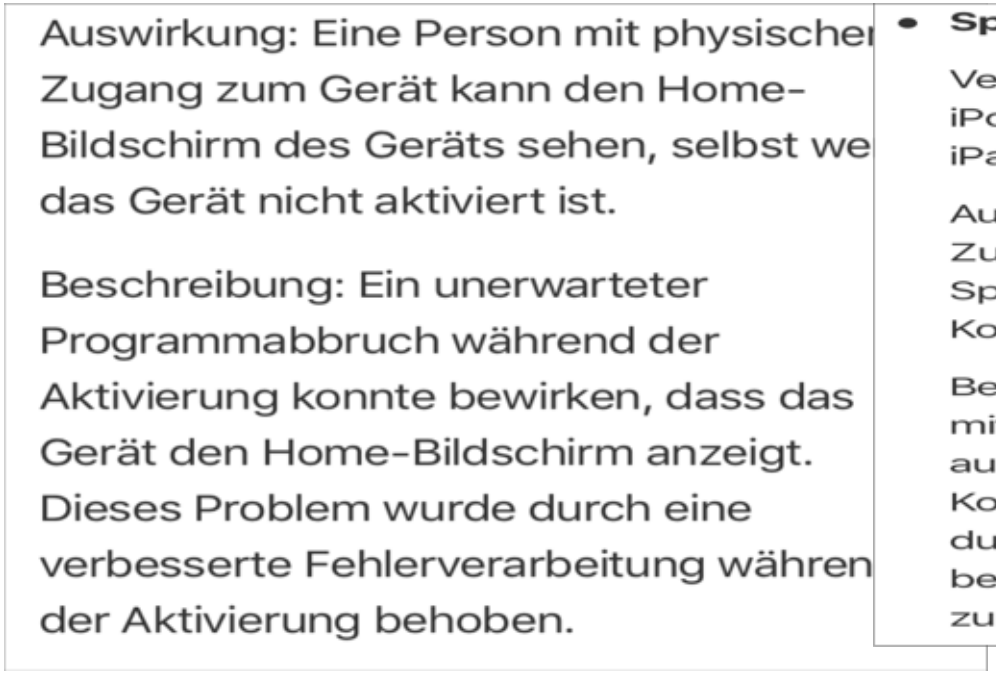
- Function mappings (Analyse the functions & usability style)
- Access privilege mappings (Analyse the app privileges)
- Research on new functions & and features (Be up2date)
- Use Faq, manuals and forums for questions & answers

Access Permissions & Physical Restrictions on Exploitation

- Vulnerability only with default setup exploitable
- Reasons: Siri, Voice Control, SMS Answer, Phone App
- Vulnerabilities in all cases local
- Physical idevice access required – hands on
- Automated expoitation & fuzzin hard - Reasons
- Passcode mostly partly bypassed
- some functions are restricted or non available
- Every idevice has other functions & features
- Touch Push, Button Functions & Commands

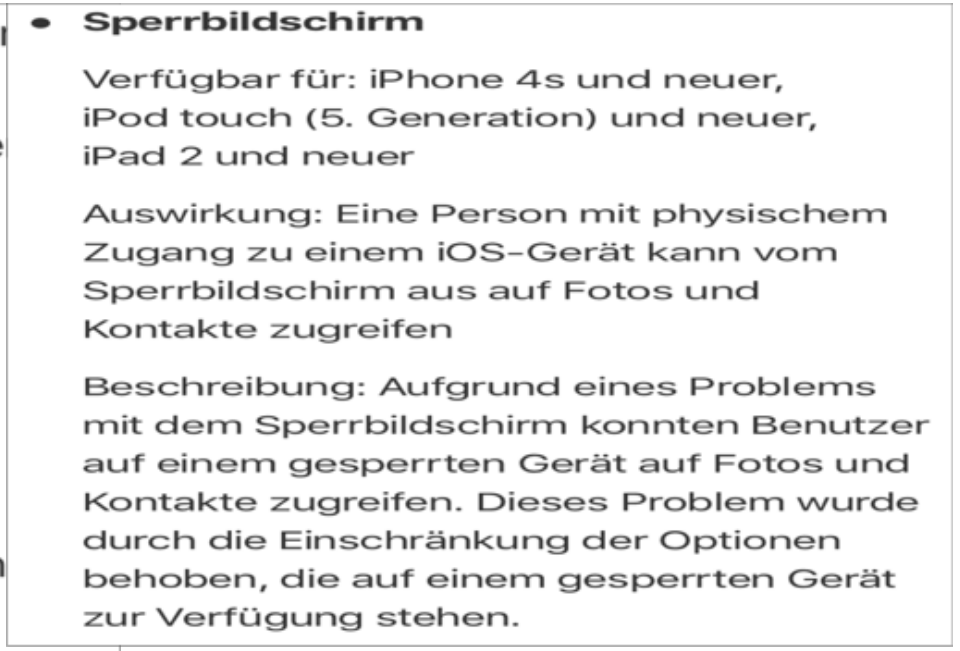
How Apple Cupertino resolves such type of Vulnerability?

- Temorarily prevention to exploit (Ex: API Redirect)
- If to late, acknowledgement after fix – no cve or bb
- Hotfix & Patch by monthly updates
- Resolved by new ios release version



Auswirkung: Eine Person mit physischer
Zugang zum Gerät kann den Home-
Bildschirm des Geräts sehen, selbst we
das Gerät nicht aktiviert ist.

Beschreibung: Ein unerwarteter
Programmabbruch während der
Aktivierung konnte bewirken, dass das
Gerät den Home-Bildschirm anzeigt.
Dieses Problem wurde durch eine
verbesserte Fehlerverarbeitung währen
der Aktivierung behoben.



- **Sperrbildschirm**

Verfügbar für: iPhone 4s und neuer,
iPod touch (5. Generation) und neuer,
iPad 2 und neuer

Auswirkung: Eine Person mit physischem
Zugang zu einem iOS-Gerät kann vom
Sperrbildschirm aus auf Fotos und
Kontakte zugreifen

Beschreibung: Aufgrund eines Problems
mit dem Sperrbildschirm konnten Benutzer
auf einem gesperrten Gerät auf Fotos und
Kontakte zugreifen. Dieses Problem wurde
durch die Einschränkung der Optionen
behoben, die auf einem gesperrten Gerät
zur Verfügung stehen.

iOS v6.0 - v6.1

Emergency Passcode Bypass

- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s, ipad & ipad 2 series


BASE DE 3G
00:00
66 %


BASE DE
02:06
51 %

What happened? What is possible?

Technical Aspects

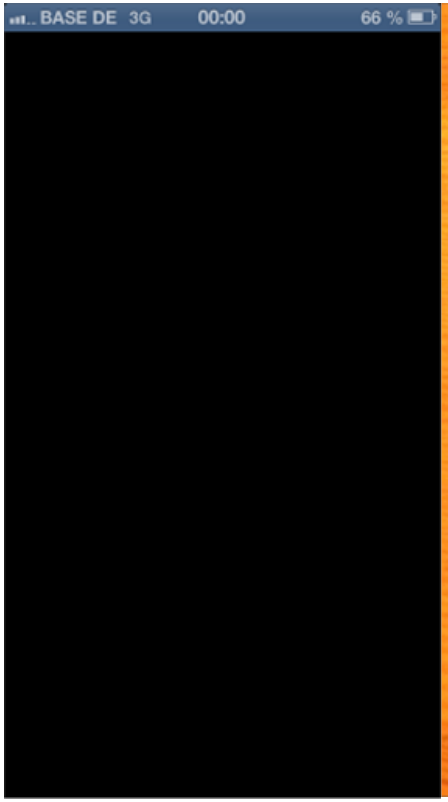
- Access privileges in phone app to call emergency
- (Own phone app mask)
- Glitch on Power when pushing a function in phone app
- Effect: App Merge – Emergency Mask to Phone Mask to Phone App
- Solution: No way to patch by manual interaction

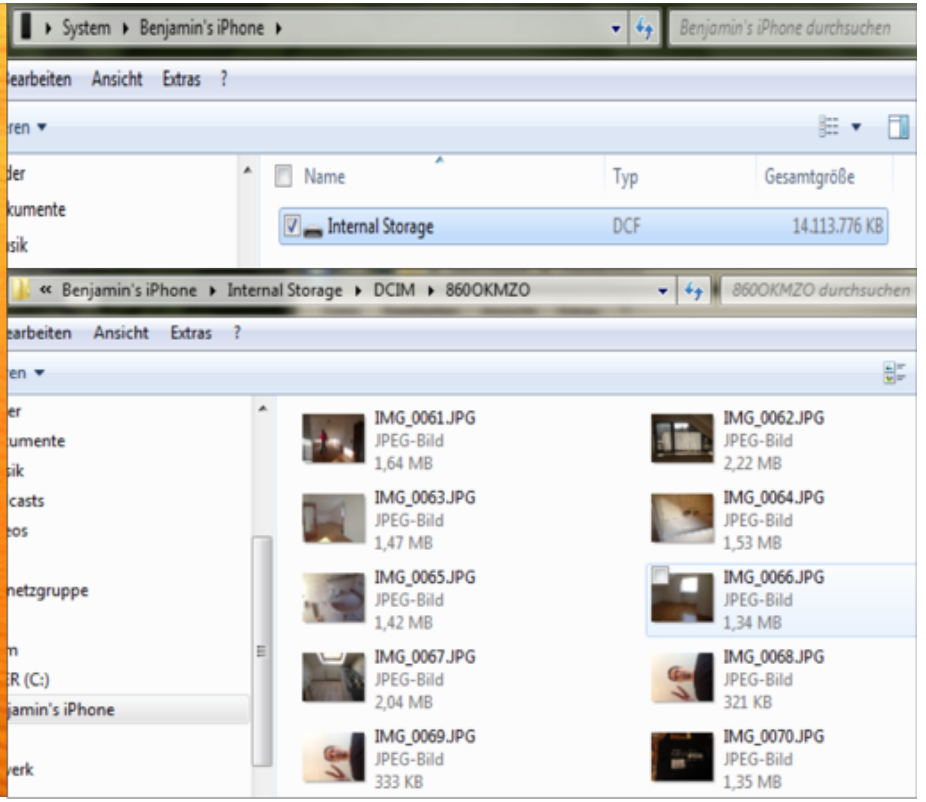
- Unauthenticated Access
- Photos, album, apps, data library, contacts, numbers & geo
- How? Through functions for access by the phone app
- Photo Share to Email App or Picture Upload Profile to Library

iOS v6.1.2

"Blackscreen mode" – Pushing twice home

- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s, ipad & ipad 2 series





What happened? What is possible?

Technical Aspects

- Access privileges in internal storage via usb (no pin no device confirm)

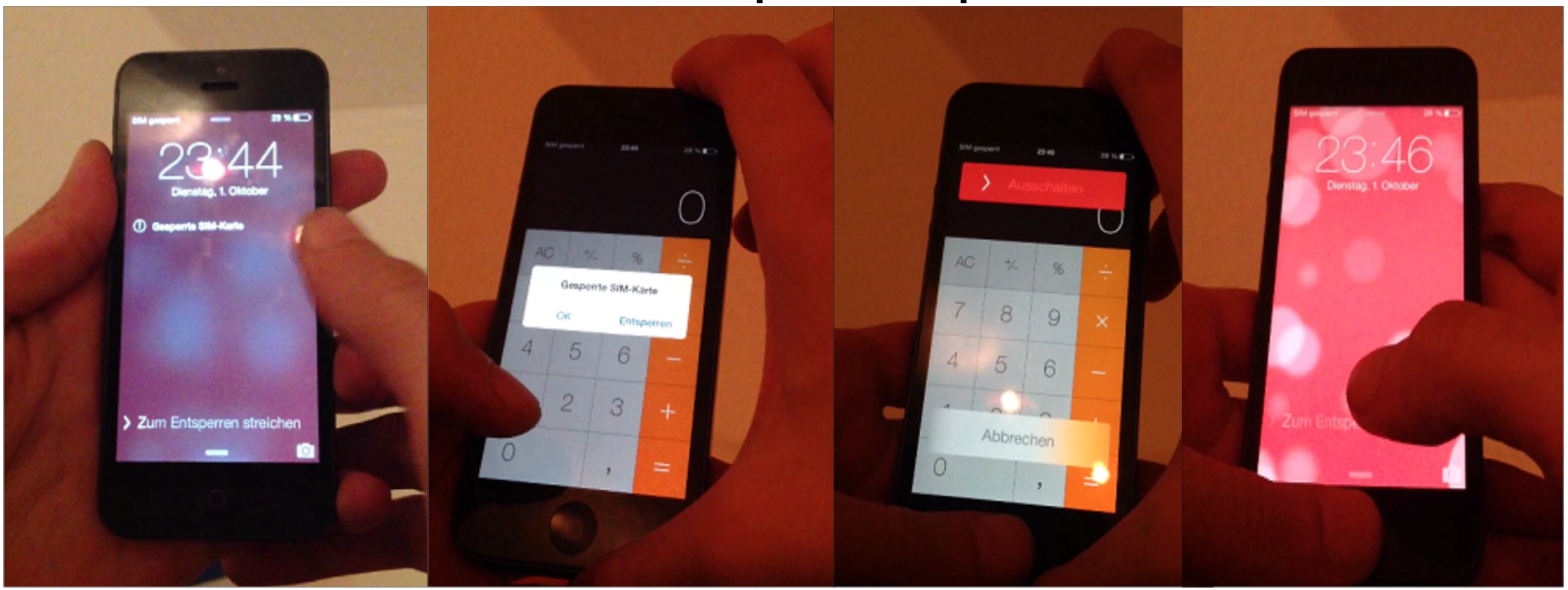
- Glitch on Power when pushing a function restart mode with home
- Effect: Black Screen – Internal Storage USB device access
- Solution: No way to patch by manual interaction

- Unauthenticated Access
- Internal storage und photo library or videos & geo data
- How? Through functions for access by the phone app when verified
- No other interaction possible – hard reset required with device reboot

iOS v7.0.1

Sim Lock Screen Bypass – Same trick

- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s, ipad & ipad 2 series



What happened? What is possible?

Technical Aspects

- Access privileges sim unlock not passcode

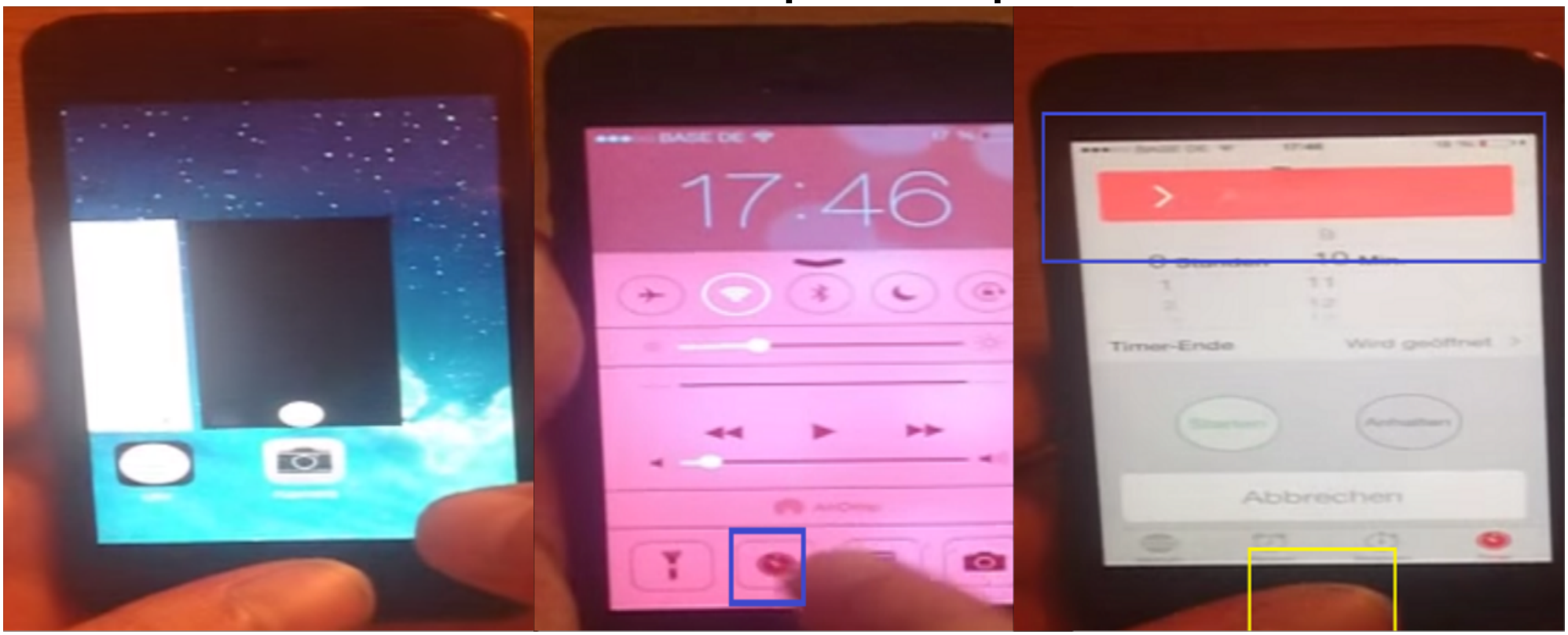
- Glitch on power when pushing app function to unlock with home
- Effect: Sim unlock
- Solution: Deactivate the control center in the locked mode (calculator)

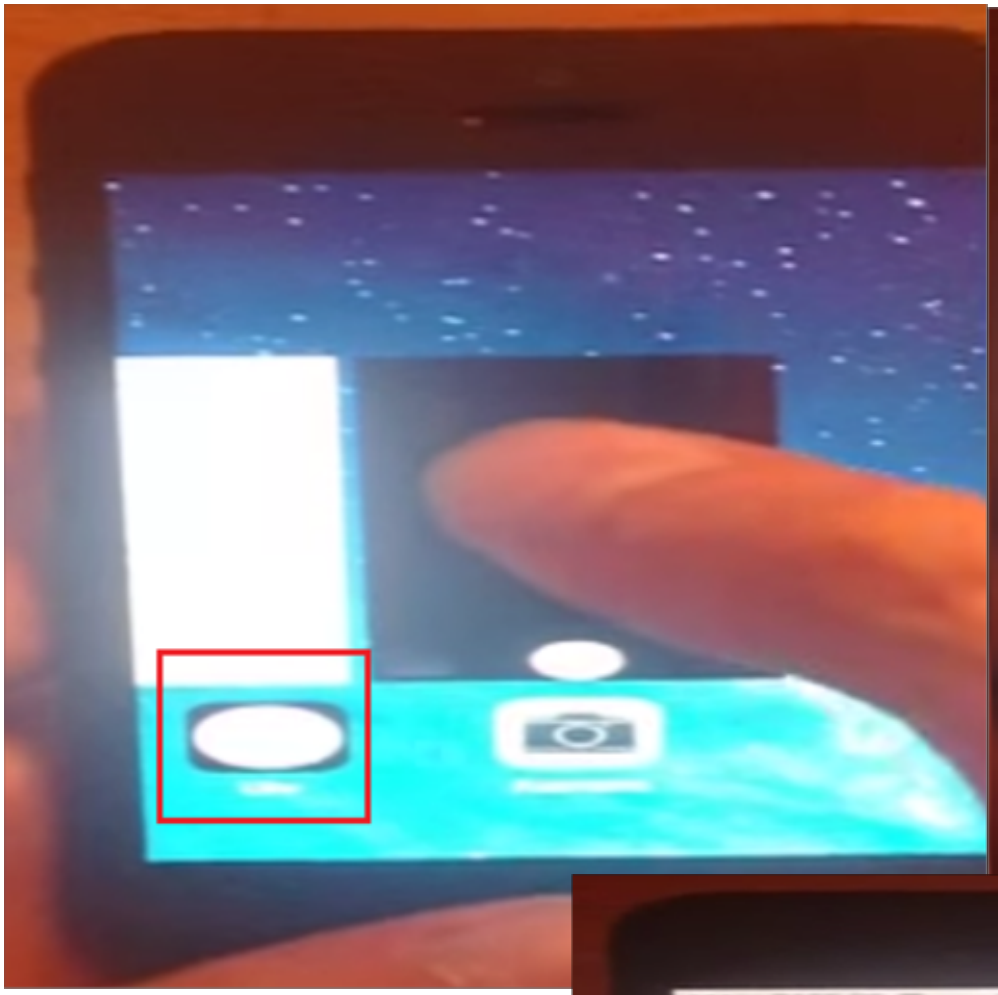
- Unauthenticated Access
- Unlock idevices
- How? Through functions for access by the shutdown in app function

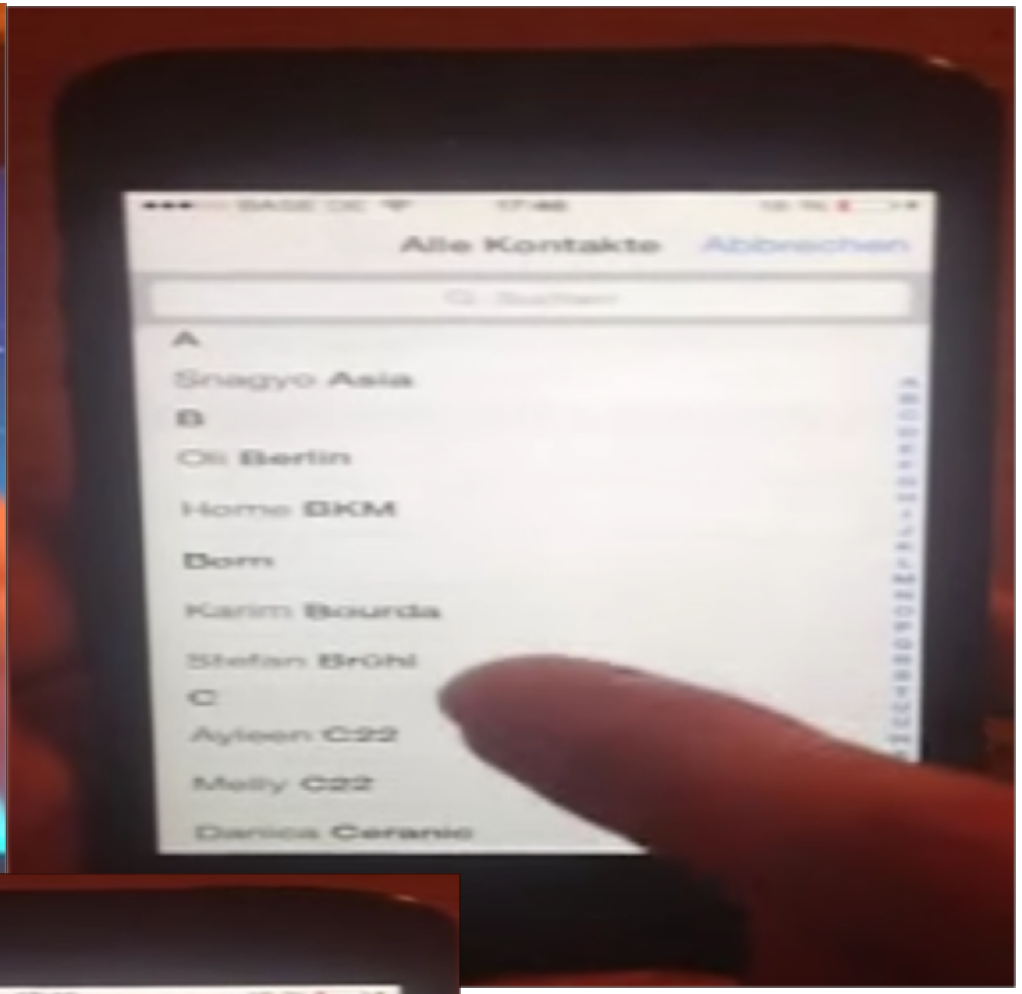
iOS v7.1.1

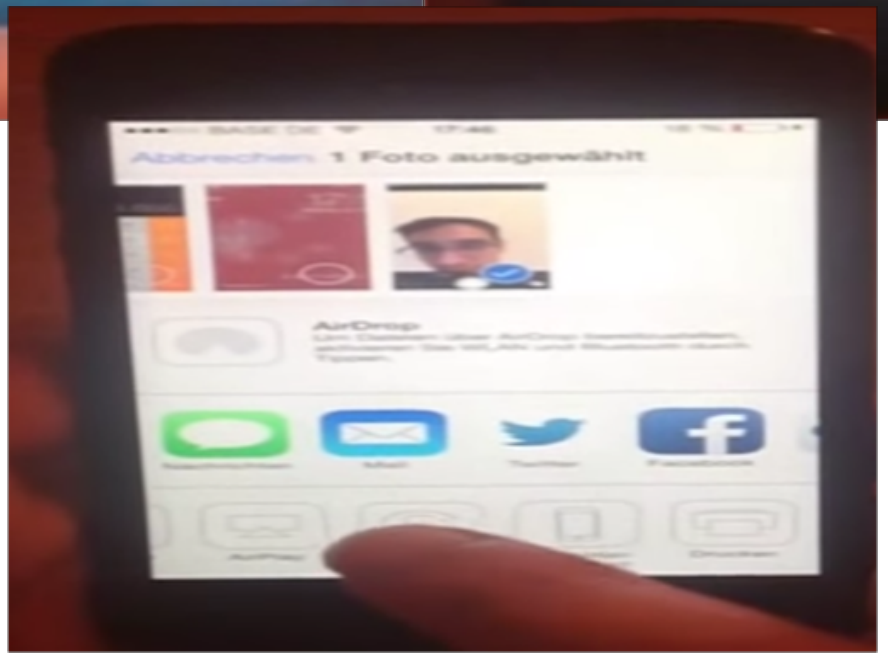
Timer Passcode Bypass – Home & Shutdown

- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s, ipad & ipad 2 series






Alle Kontakte
Abbrechen
A
B
C


Abbrechen 1 Foto ausgewählt
AirDrop

What happened? What is possible?

Technical Aspects

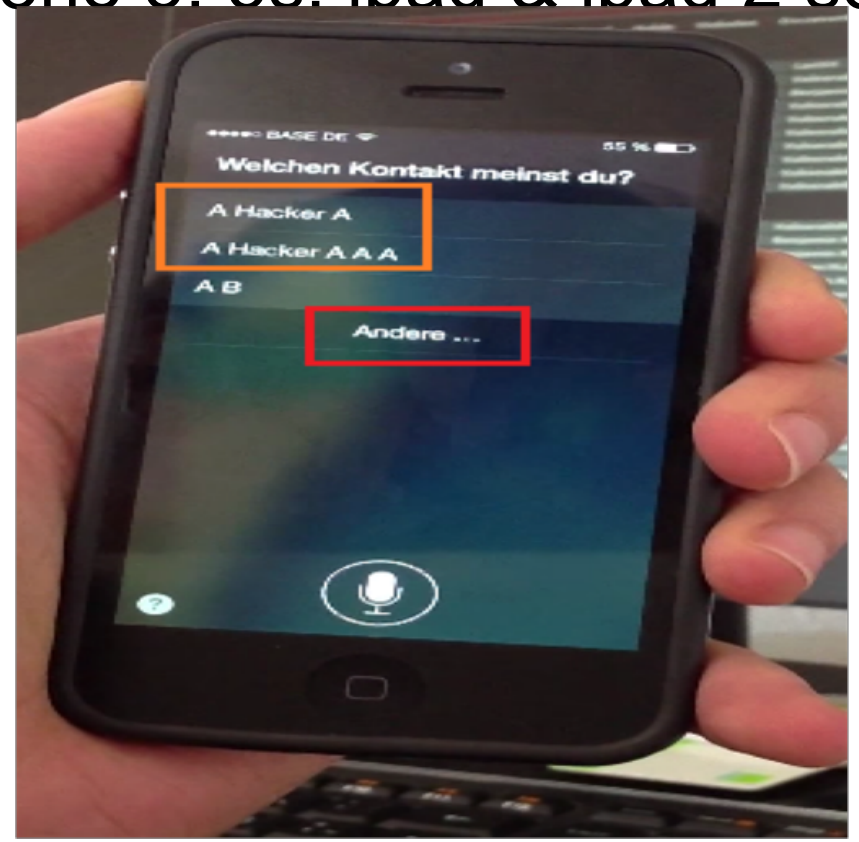
- Access privileges in timer app to home function by control center
-
- Glitch on Power when pushing a function in phone app with timer
- Effect: App Merge – Timer to Camera to Phone Mask to Phone App
- Solution: Deactivate the control center in the locked mode (timer app)

- Unauthenticated Access
- Photos, album, apps, data library, contacts, numbers & geo data
- How? Through functions for access by the timer app
- Photo Share to Email App or Picture Upload Profile to Library

iOS v7.1.1

Passcode Bypass – Siri to Contacts

- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s, ipad & ipad 2 series



What happened? What is possible?

Technical Aspects

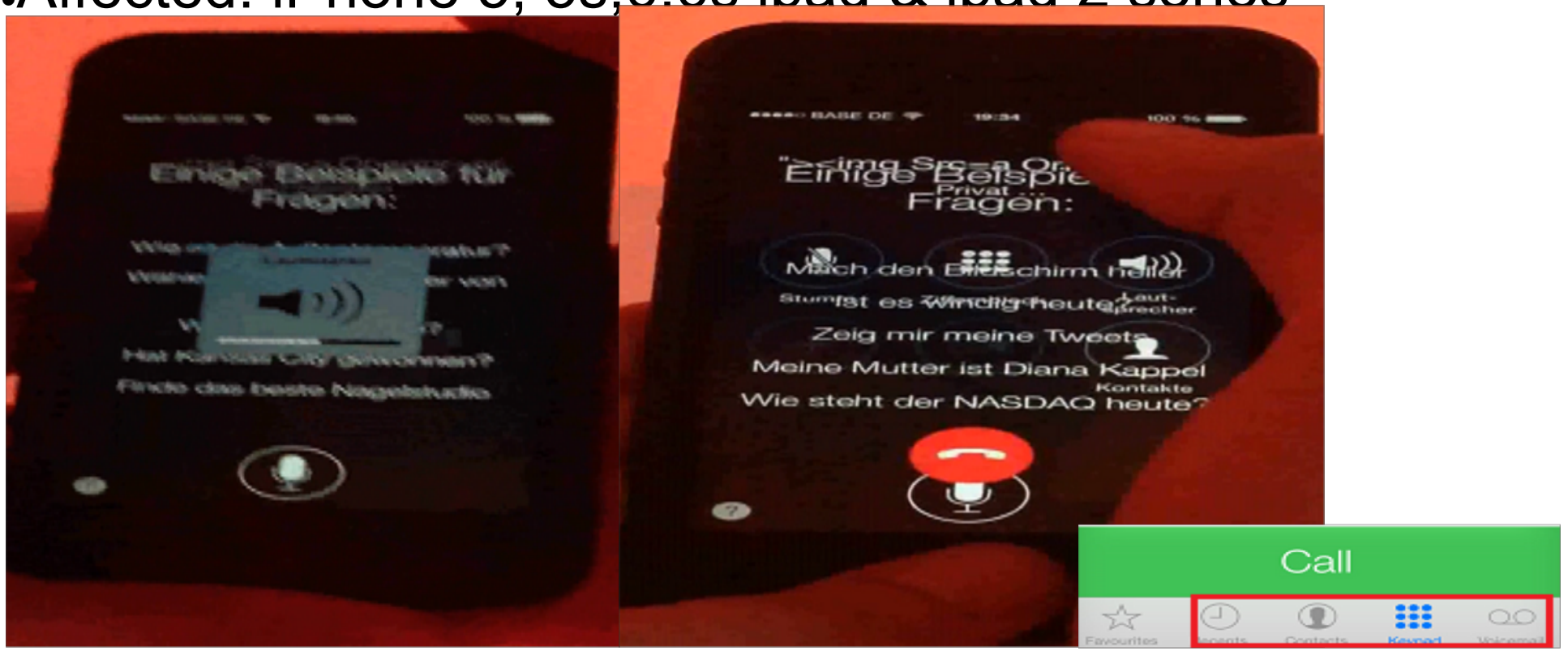
- Access privileges in siri app to contact function
-
- Missing passcode permission to list idevice contacts
- Effect: Siri to contacts to profile
- Solution: Deactivate siri in the locked mode

- Unauthenticated Access
- Photos, album, apps, data library, contacts, numbers & geo data
- How? Through functions for access by the siri app
- Contacts to Profile to Picture to App or Profile to Library

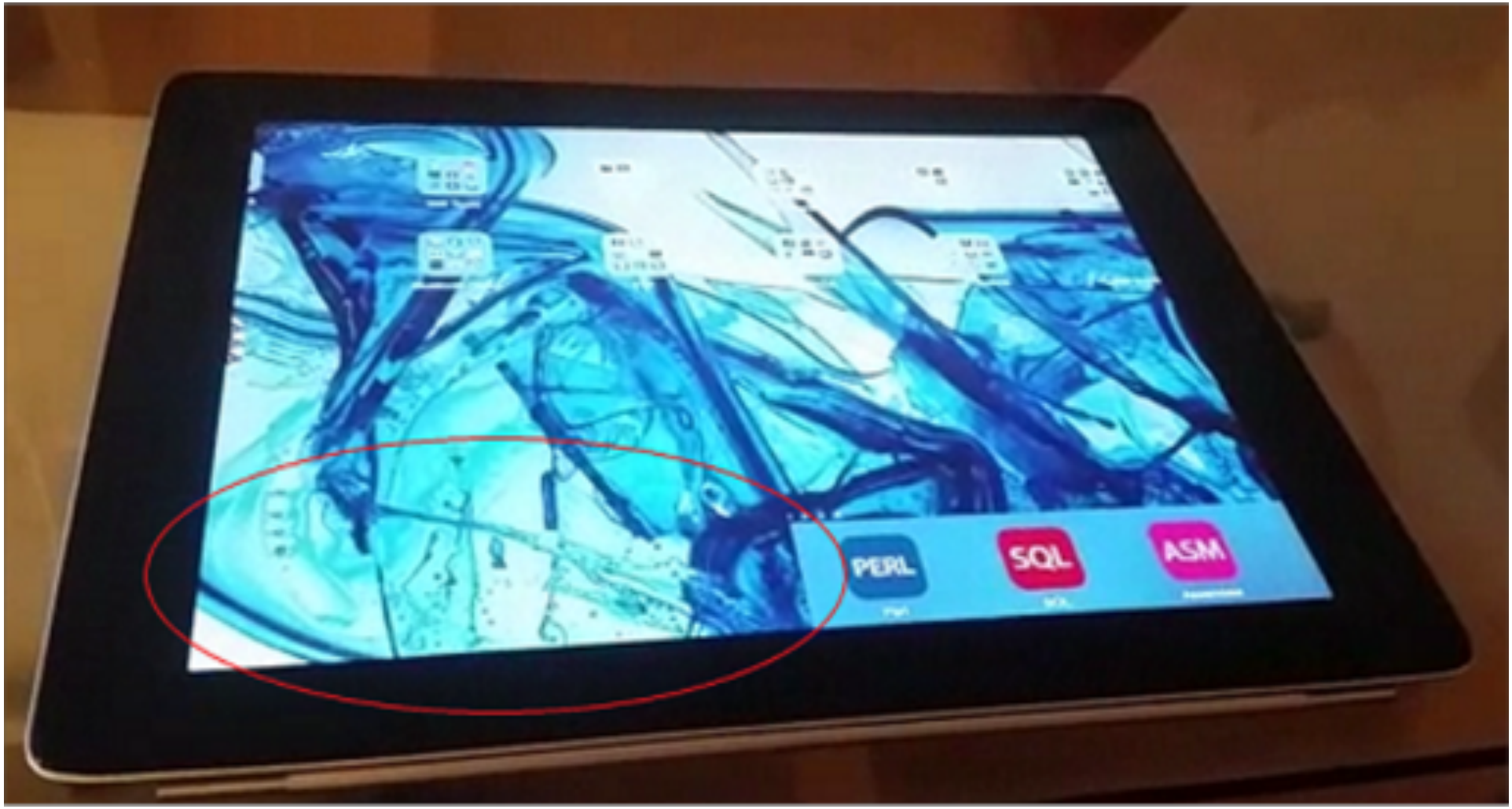
iOS v8.0

Passcode Bypass – Siri merge in phone app

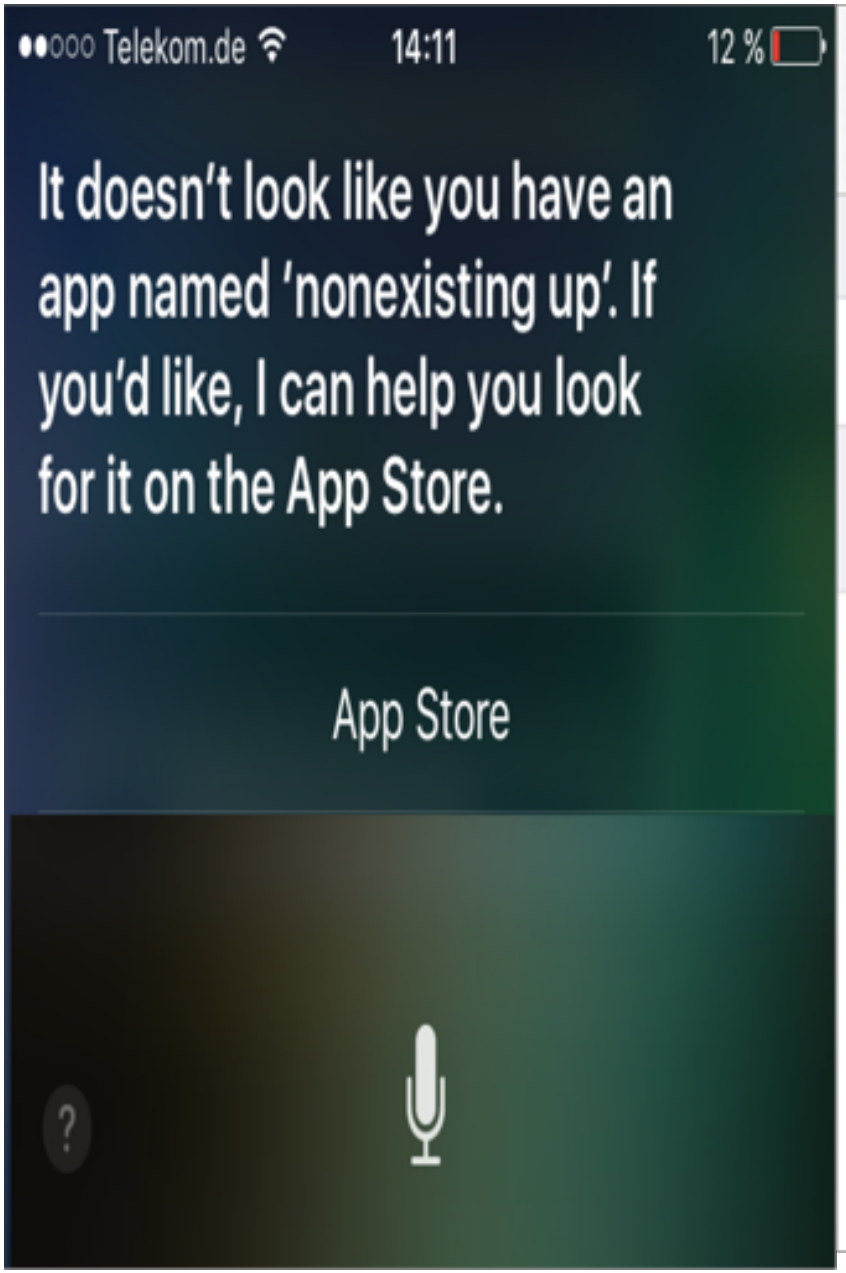
- Requirements: Physical access & default setup
- Affected: iPhone 5, 5s,6,6s ipad & ipad 2 series

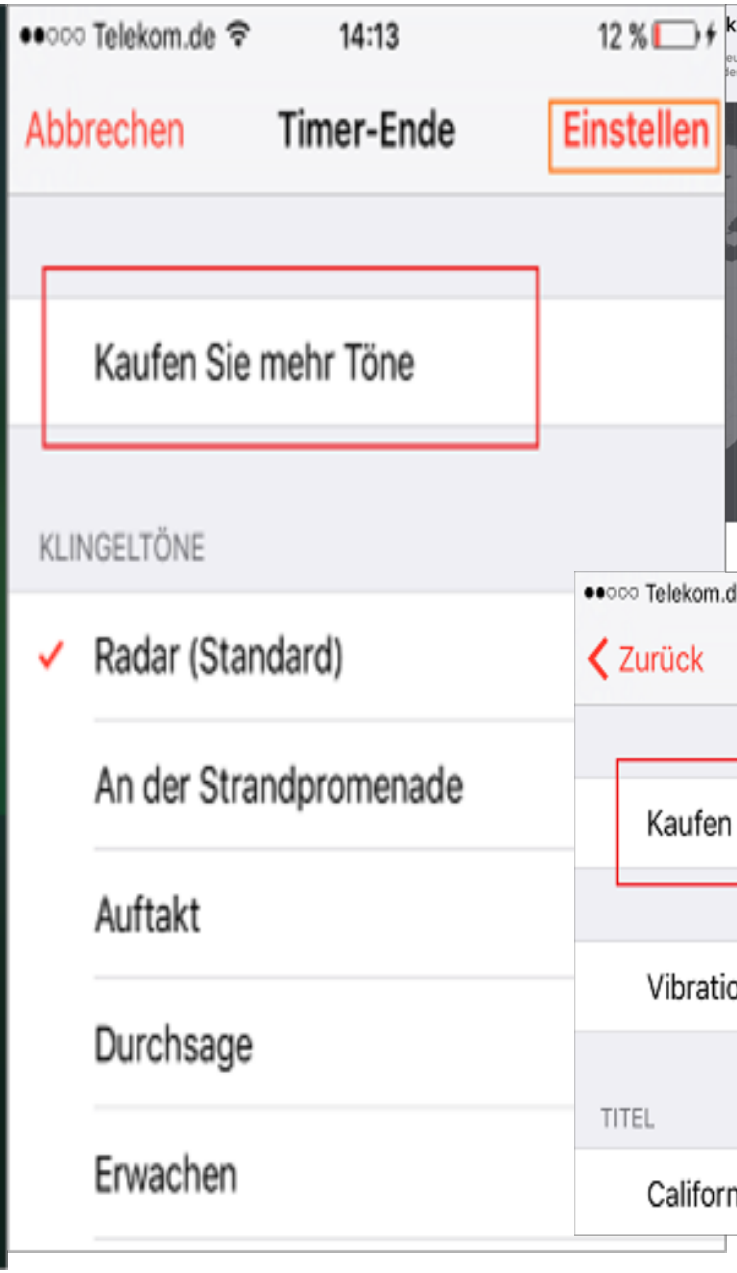


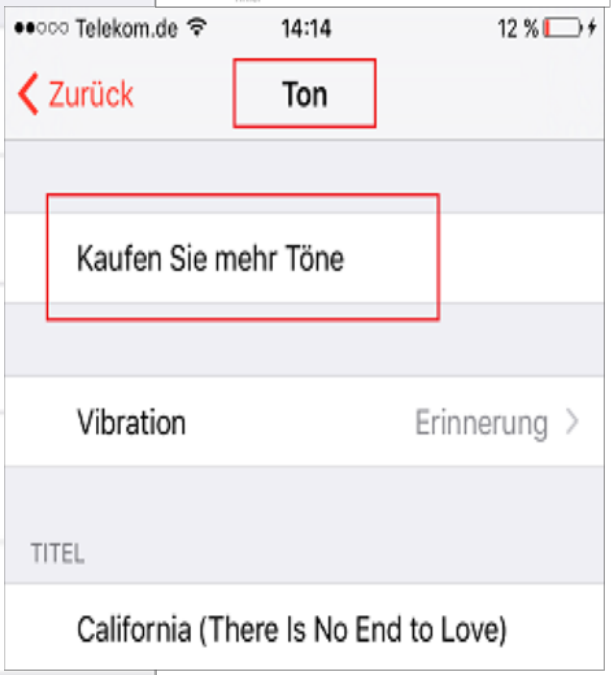
iOS v9.0 - v9.2.1



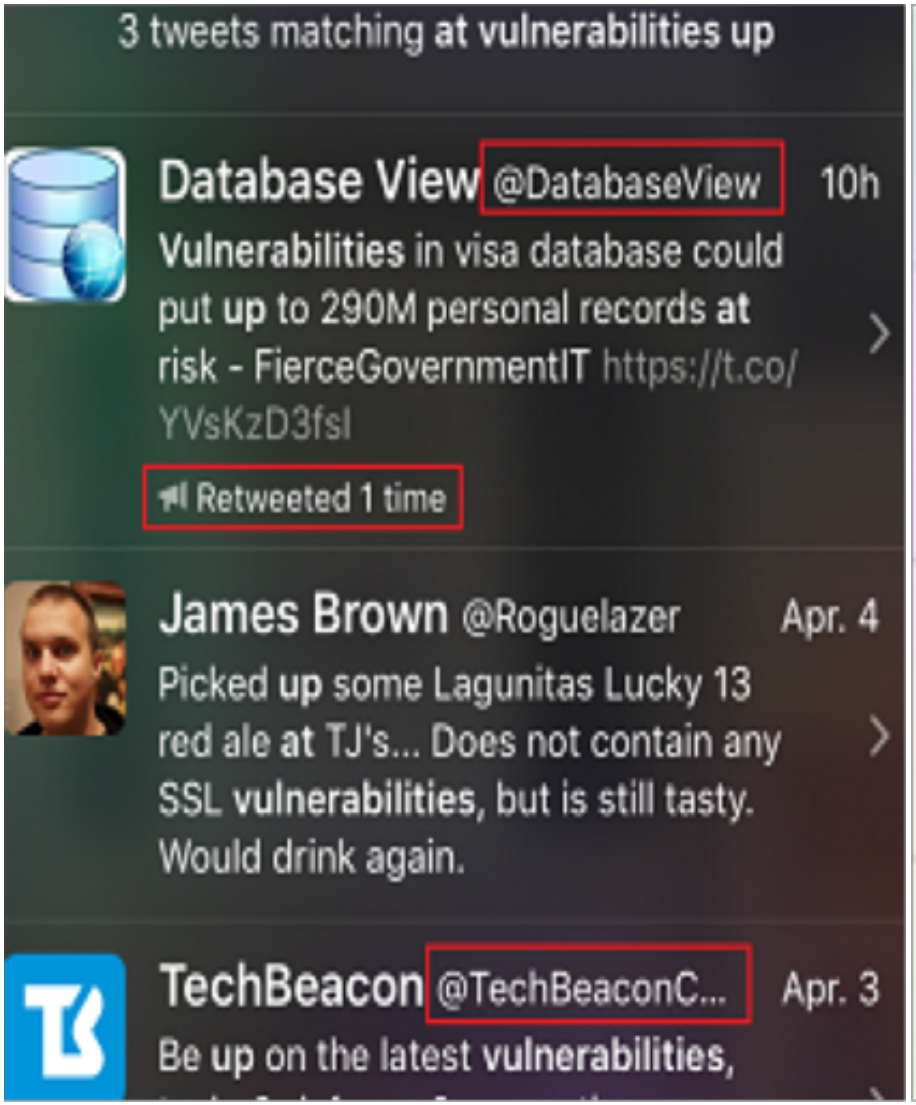
iOS v9.2.1 - v9.3.1

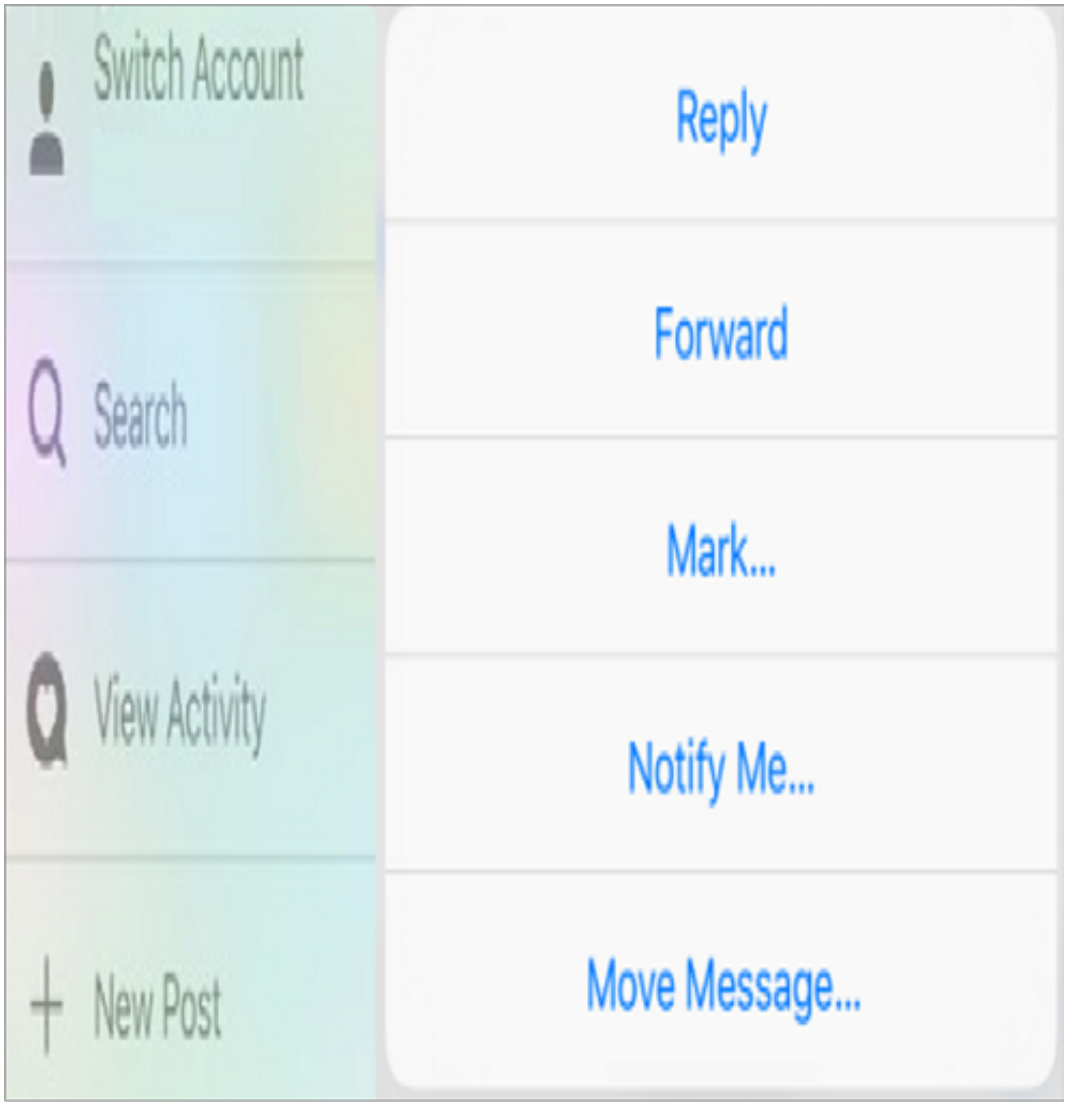






iOS v9.2.1 - v9.3.1

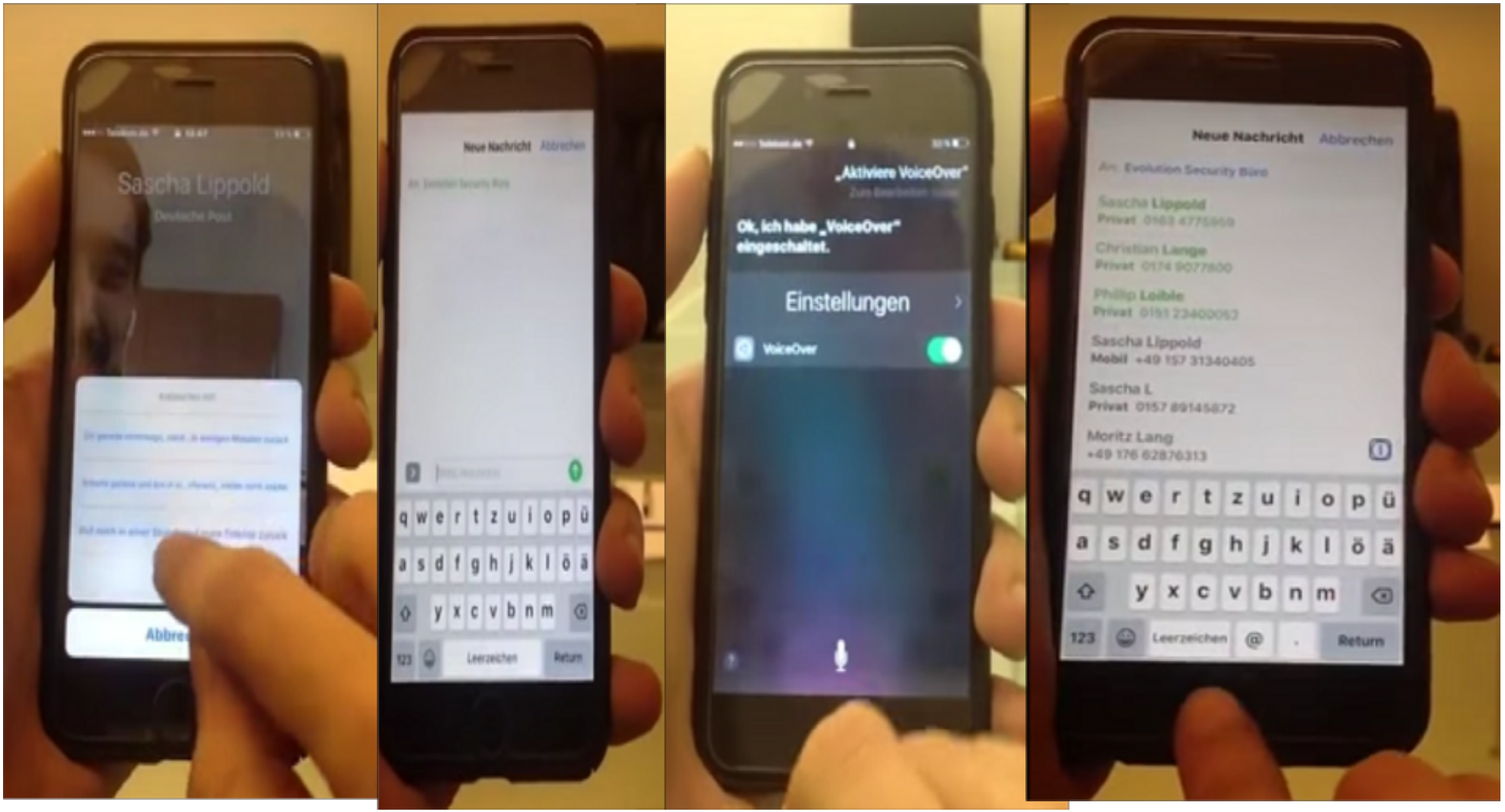




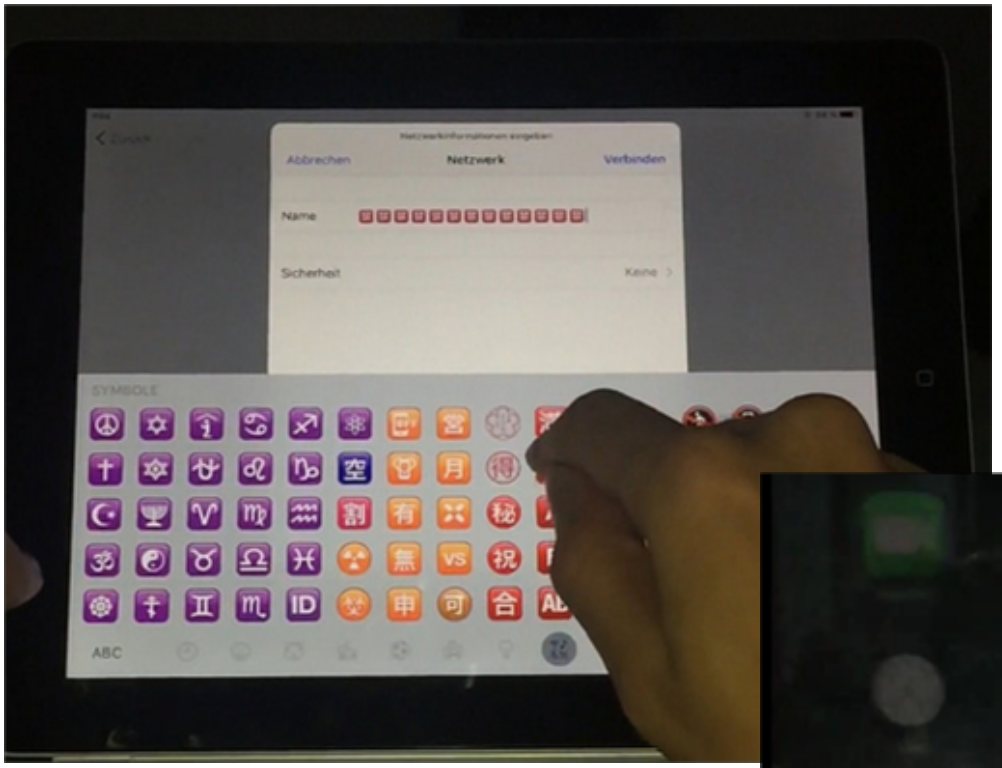
iOS v10.0

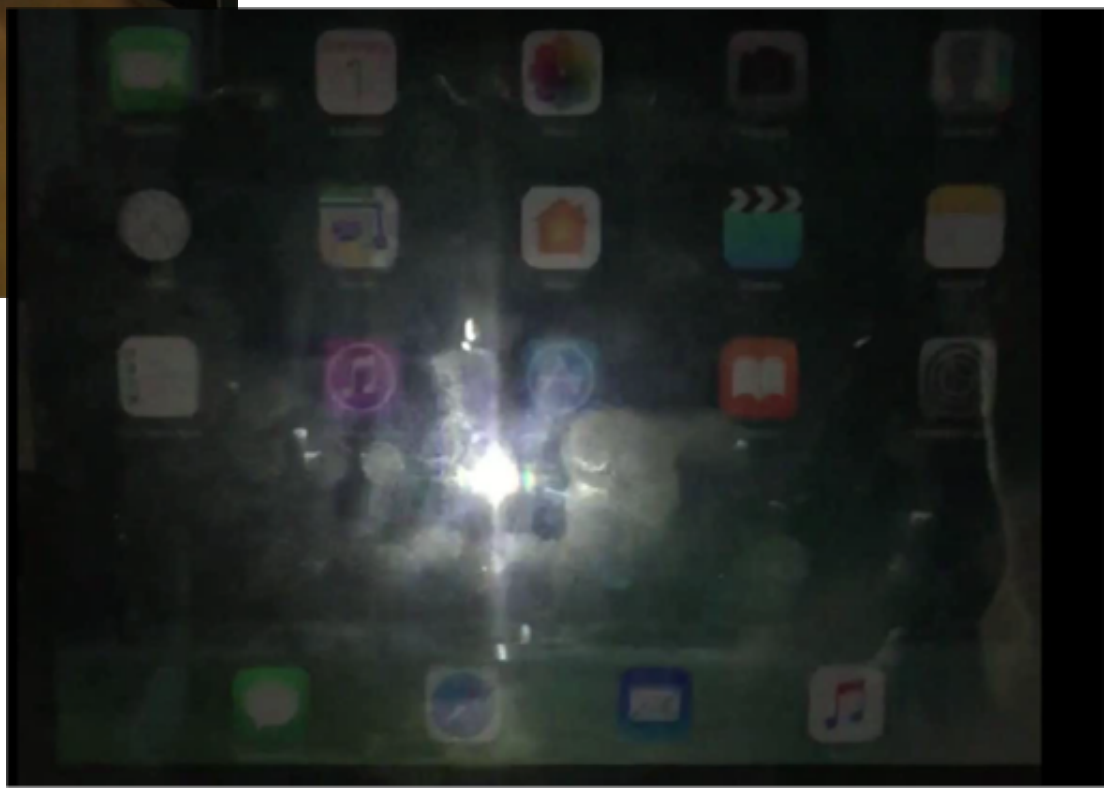

Code eingeben
Abbrechen
Kopieren
Nachschlagen
Teilen ...
Fotoalben und die Namen der auf dem Gerät
installierten Apps (also allgemein deine
Nachrichten
Mail
Zu „Notizen“ hinzufügen
Twitter
Kopieren
iCloud Drive
Mehr

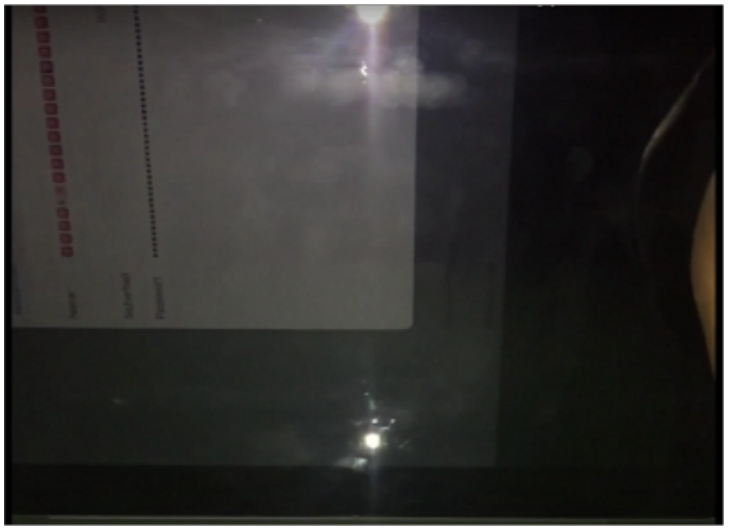
iOS v10.1


Sascha Lippold
Neue Nachricht
Abbrechen
„Aktiviere VoiceOver"
Ok, ich habe „VoiceOver" eingeschaltet.
Einstellungen
VoiceOver
Neue Nachricht
Abbrechen
Sascha Lippold
Christian Lange
Philip Leible
Sascha Lippold
Mobil +49 157 31340405
Sascha L
Privat 0157 89145872
Moritz Lang
+49 176 62876313
Leerzeichen
Return

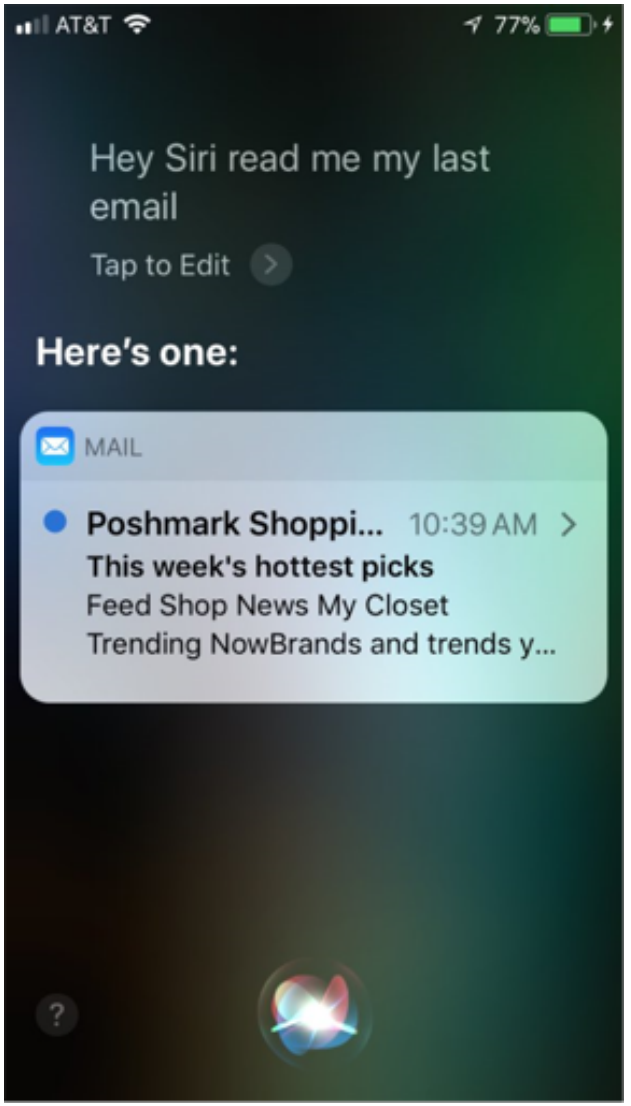
iOS v10.1 – v10.2



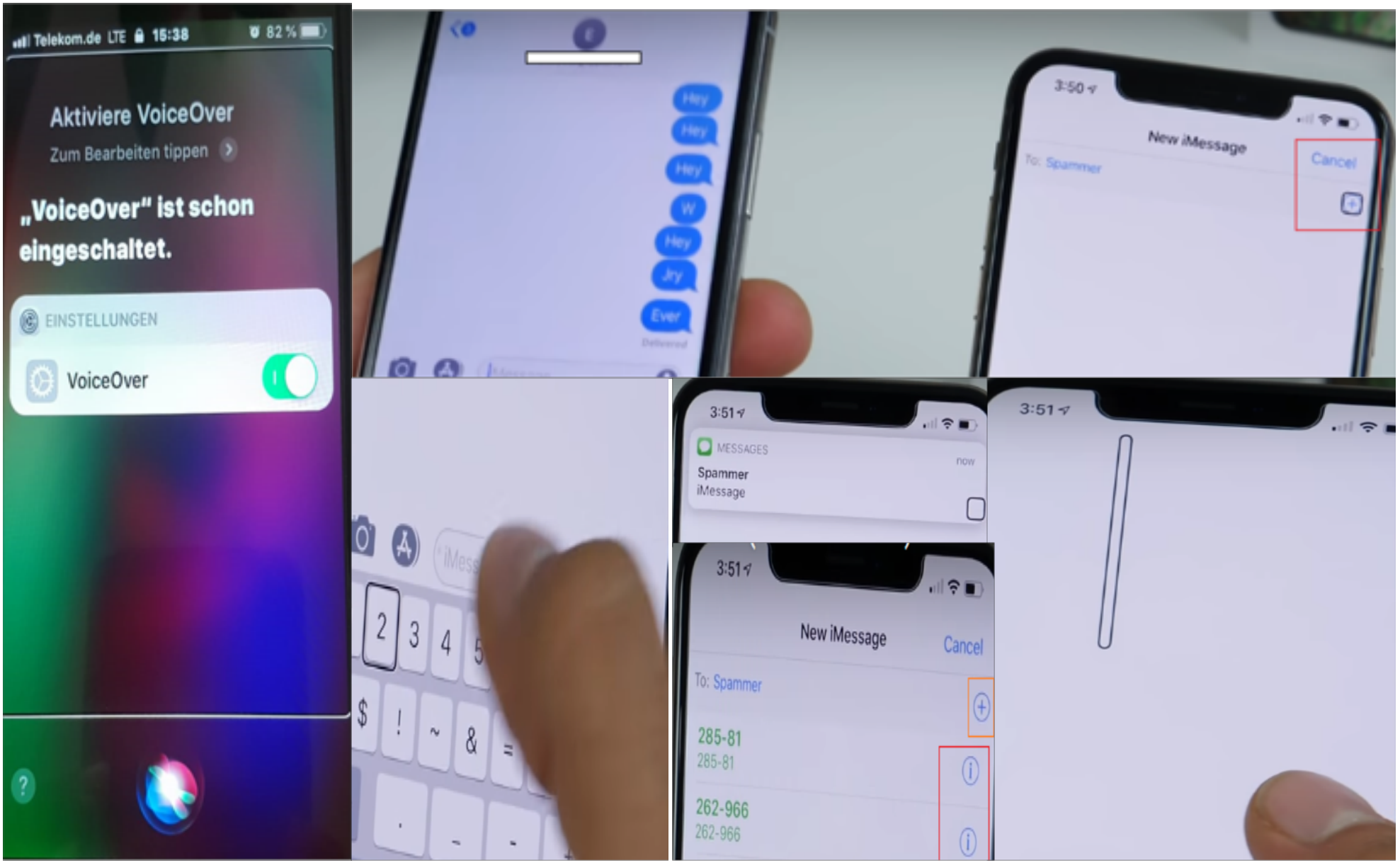




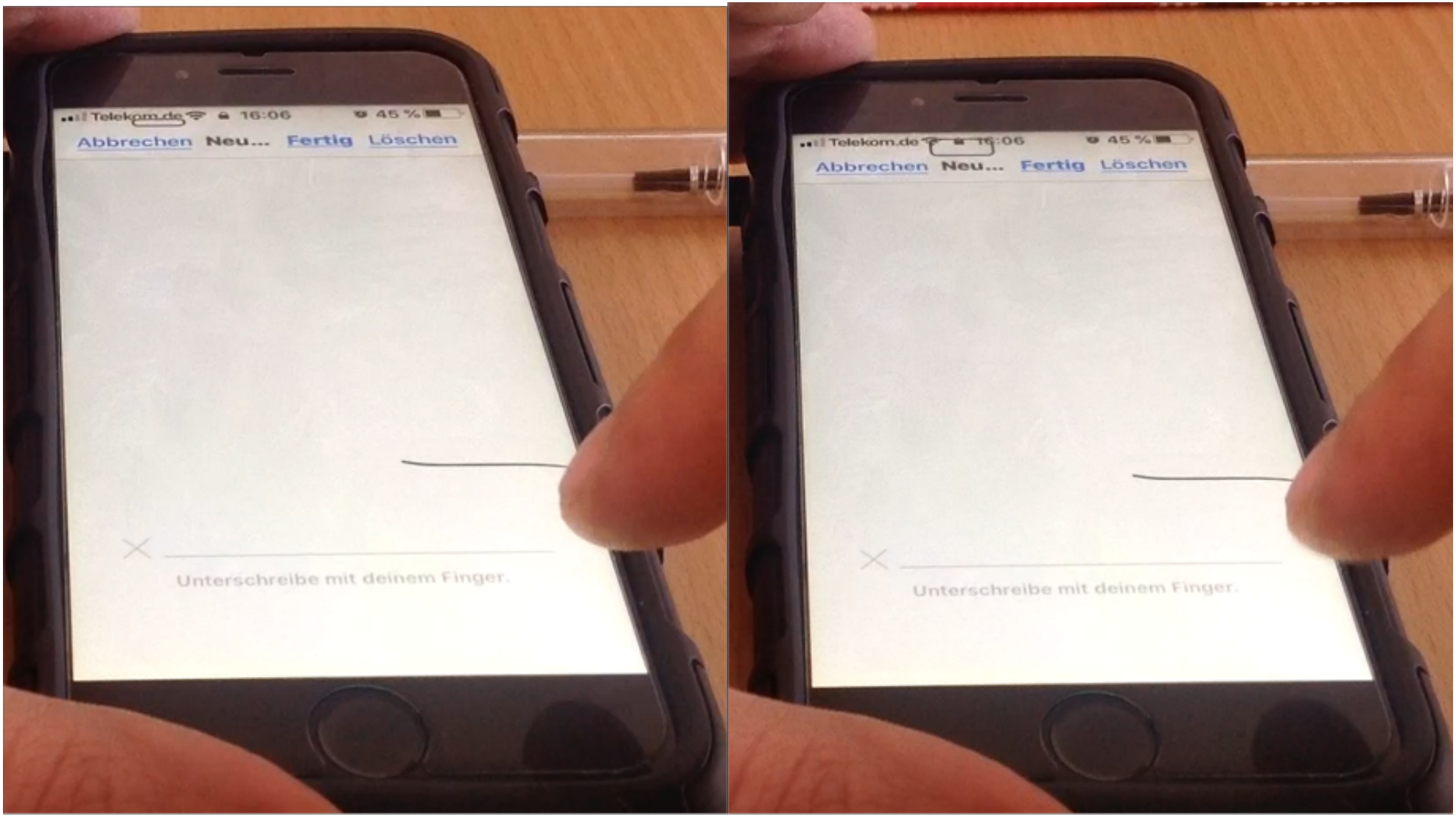
iOS v11.1 - v11.2

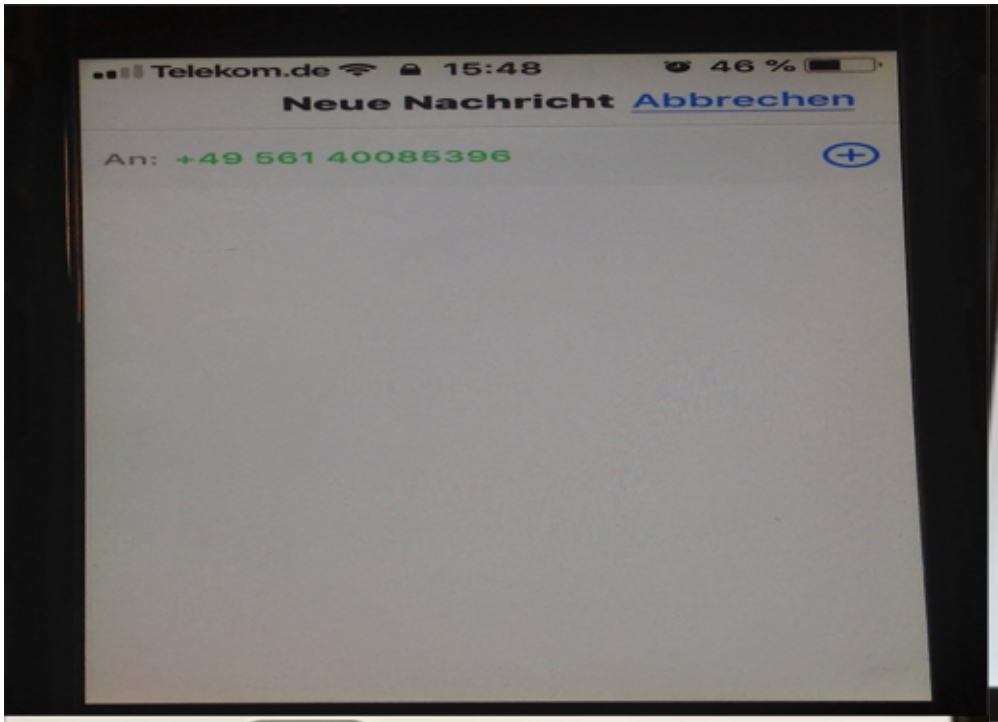


iOS v12.0 & 12.0.1

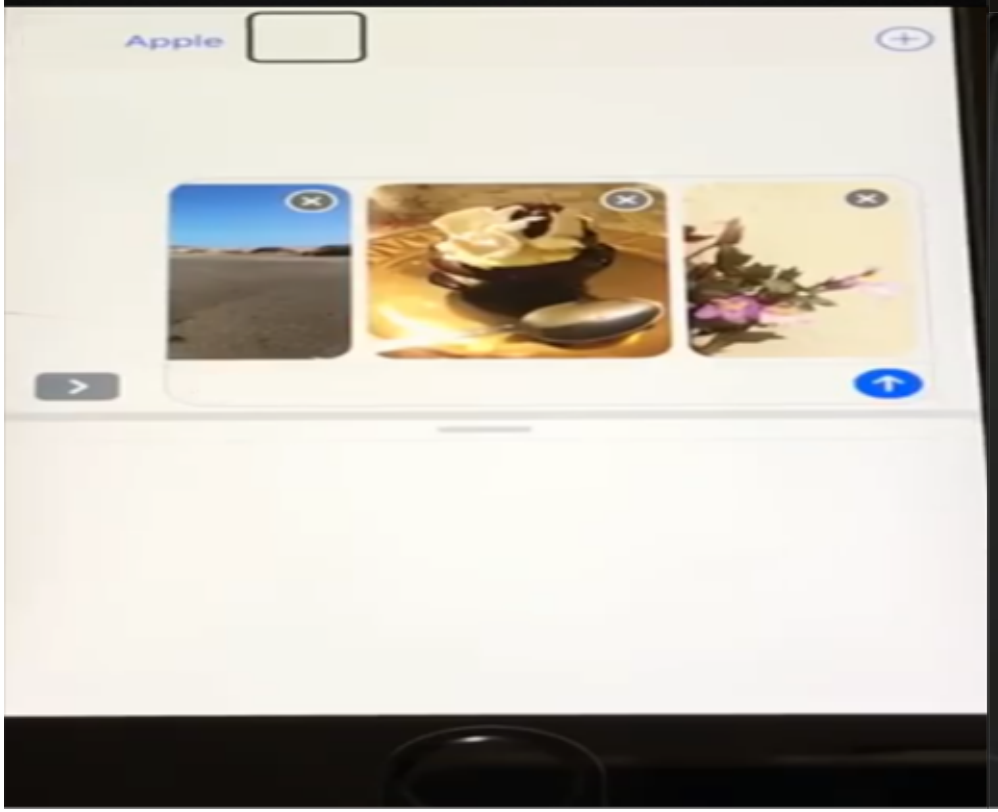


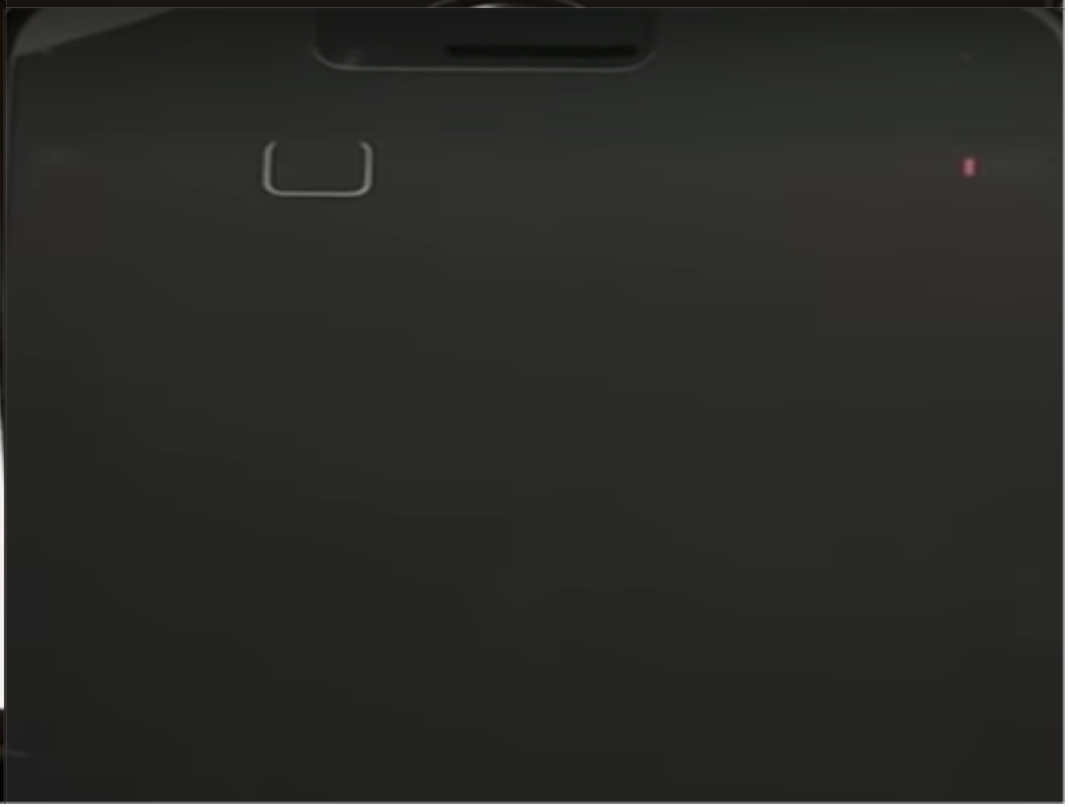
iOS v12.0.1 - Combining Siri, Answer SMS, Photo & VO




Telekom.de
15:48
46 %
Neue Nachricht
Abbrechen
An: +49 561 40085396


iMessage


Apple



Next Stop – Framwork or Sheets

- Creation of manual sheets
- Creation of separate advisories

~Thanks

by JD.com