Strong Customer Authentication for the PSD2: security issues and possible mitigations to share with end users

Marco Pernpruner, Giada Sciarretta, Silvio Ranise
Security & Trust Research Unit
Fondazione Bruno Kessler, Trento, Italy

FINSEC Project Webinar
September 28, 2020

| Agenda

- Overview of security vulnerabilities affecting the financial scenario

- Impacts of the PSD2 on financial protocols

- Best practices to reduce the risks online

| Agenda

- **Overview of security vulnerabilities affecting the financial scenario**
- Impacts of the PSD2 on financial protocols
- Best practices to reduce the risks online

Security Vulnerabilities

Cerberus banking Trojan source code released for free to cyberattackers

An auction designed to net the developer of the Android malware $100,000 failed.

New 'Alien' malware can steal passwords from 226 Android apps

Most targets are banking apps, but Alien can also show phishing pages for social, instant messaging, and cryptocurrency apps.

Android malware can steal Google Authenticator codes

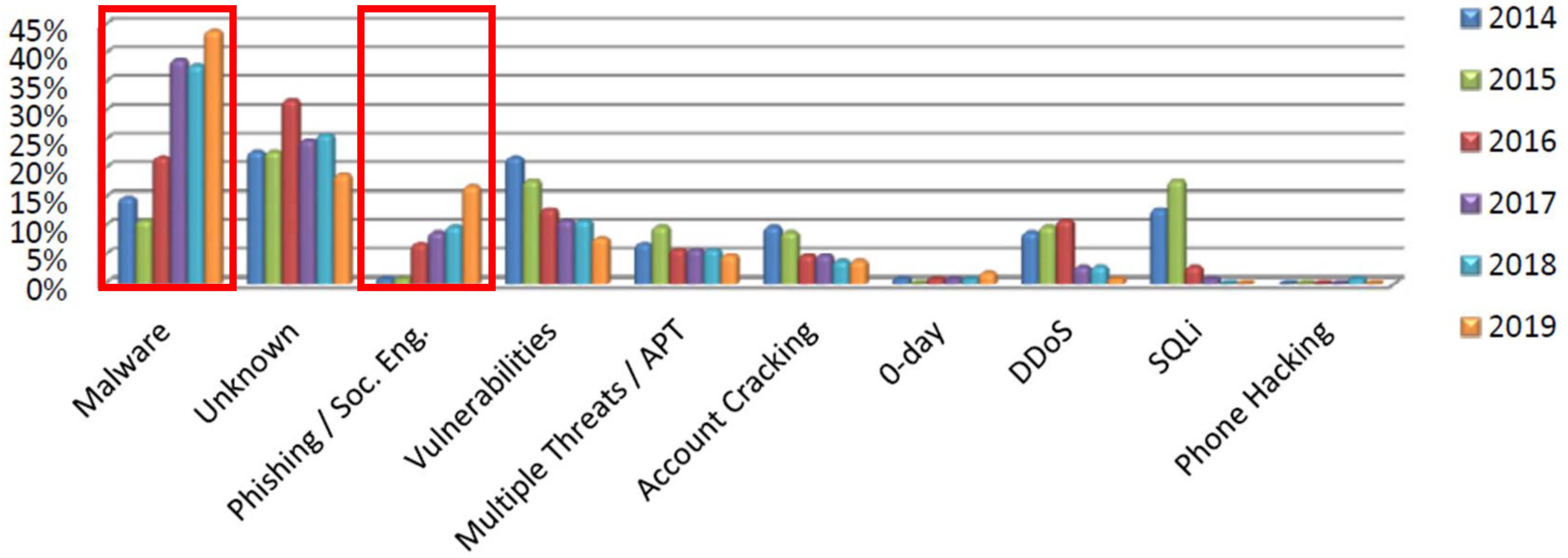
Android Malware Gains 2FA Tokens, Screen

bypassing 2FA on banking

Malicious TrickMo app seen deployed in Germany for now, but broader use is

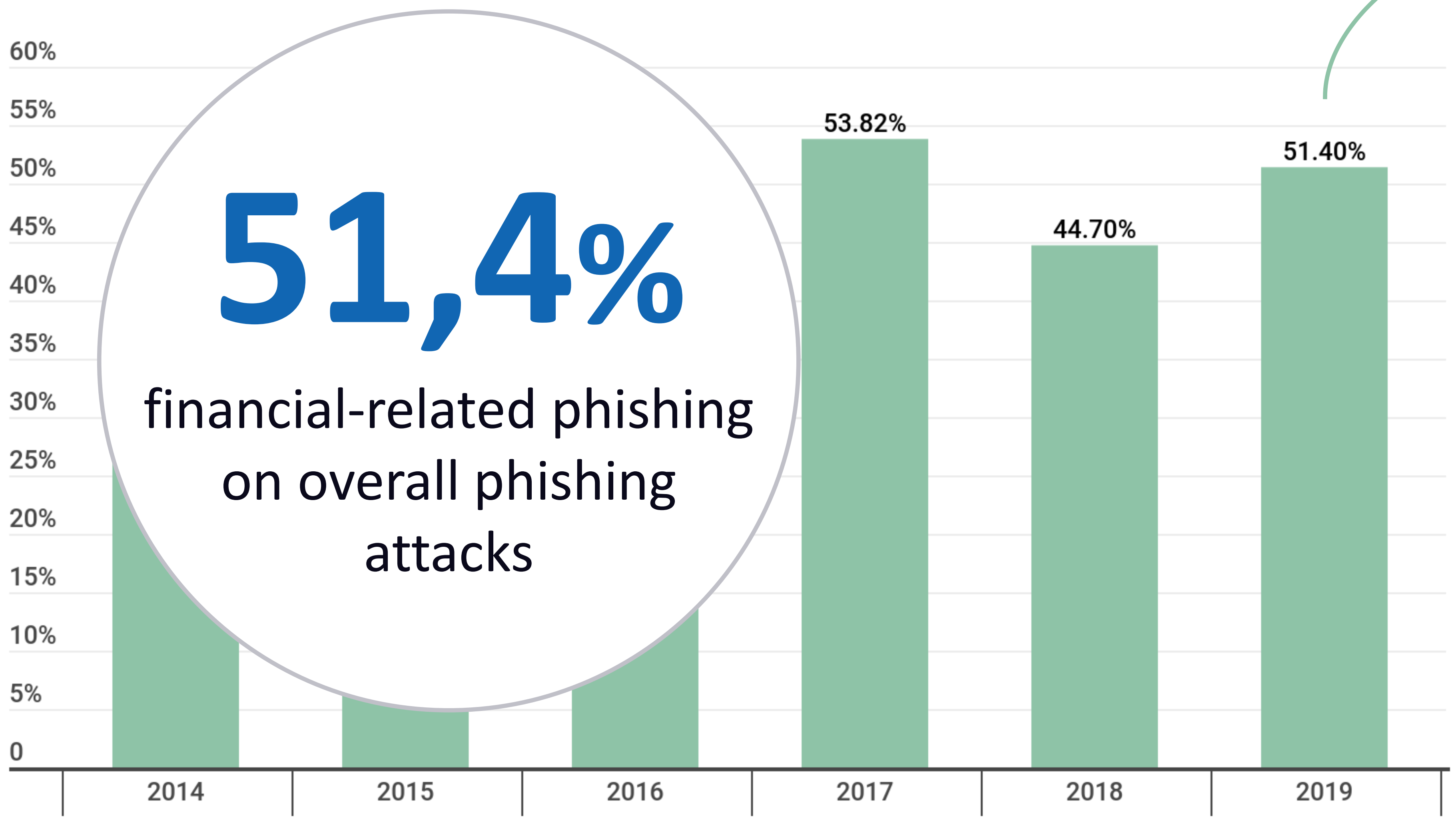
two-factor codes

Security Vulnerabilities
Techniques

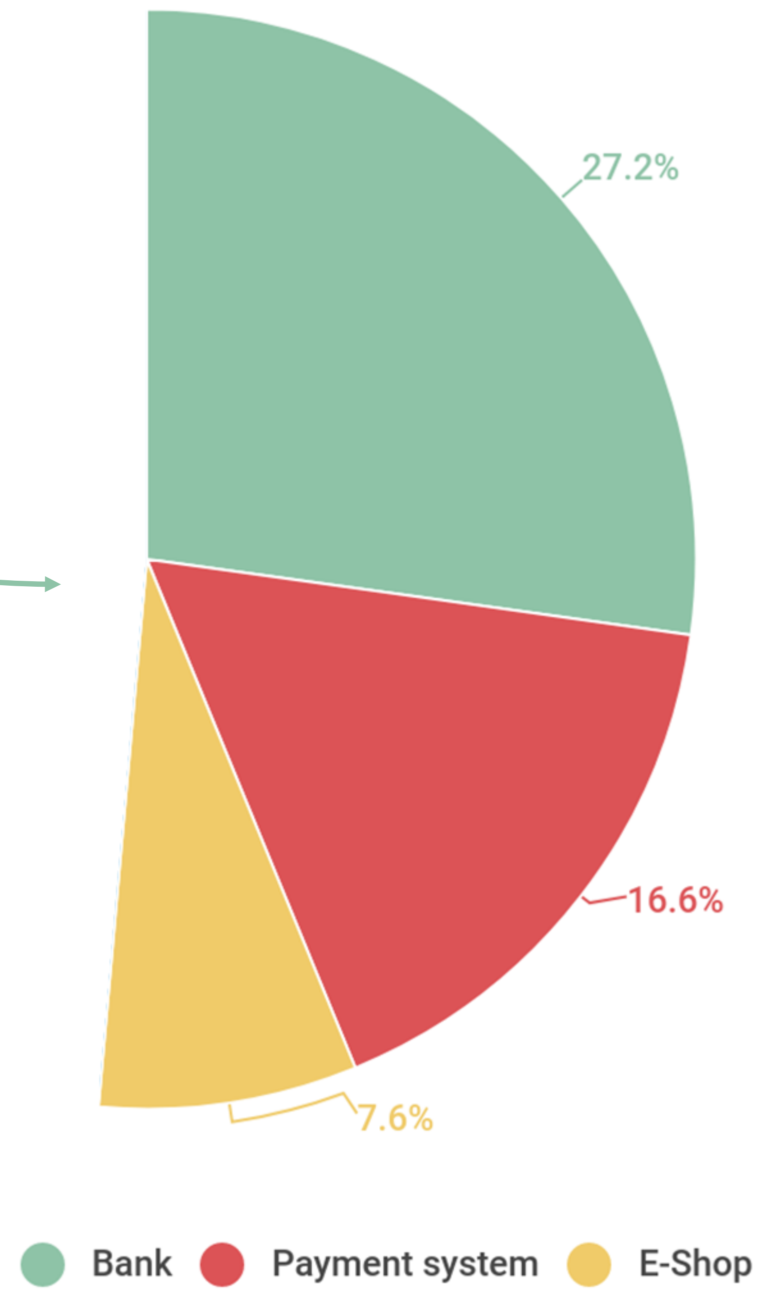


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Security Vulnerabilities
Financial Phishing



The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky, 2014-2019



The distribution of different types of financial phishing detected by Kaspersky in 2019

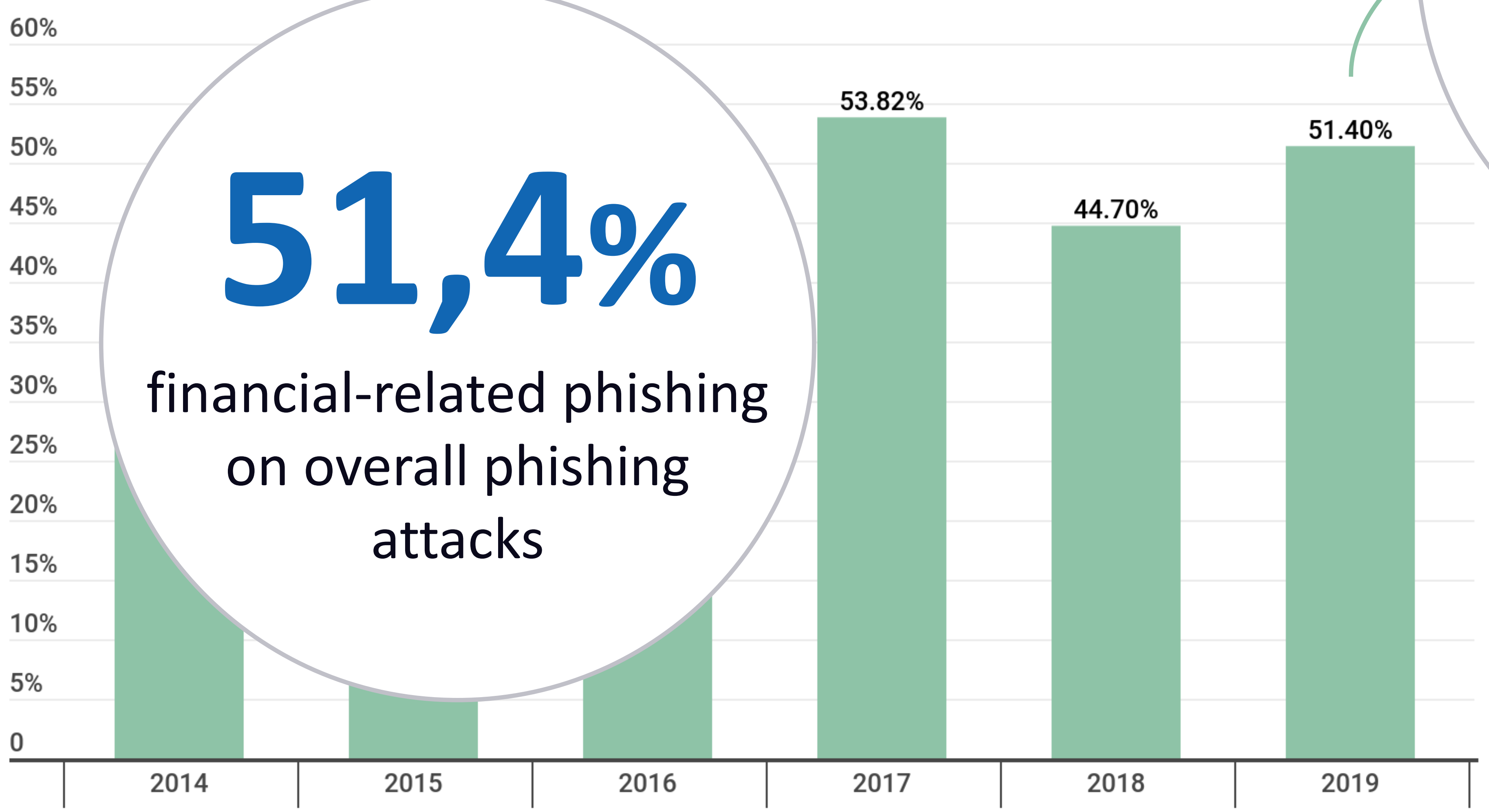
FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC

Source: Kaspersky – https://securelist.com/financial-cyberthreats-in-2019/96692/

Security Vulnerabilities
Financial Phishing



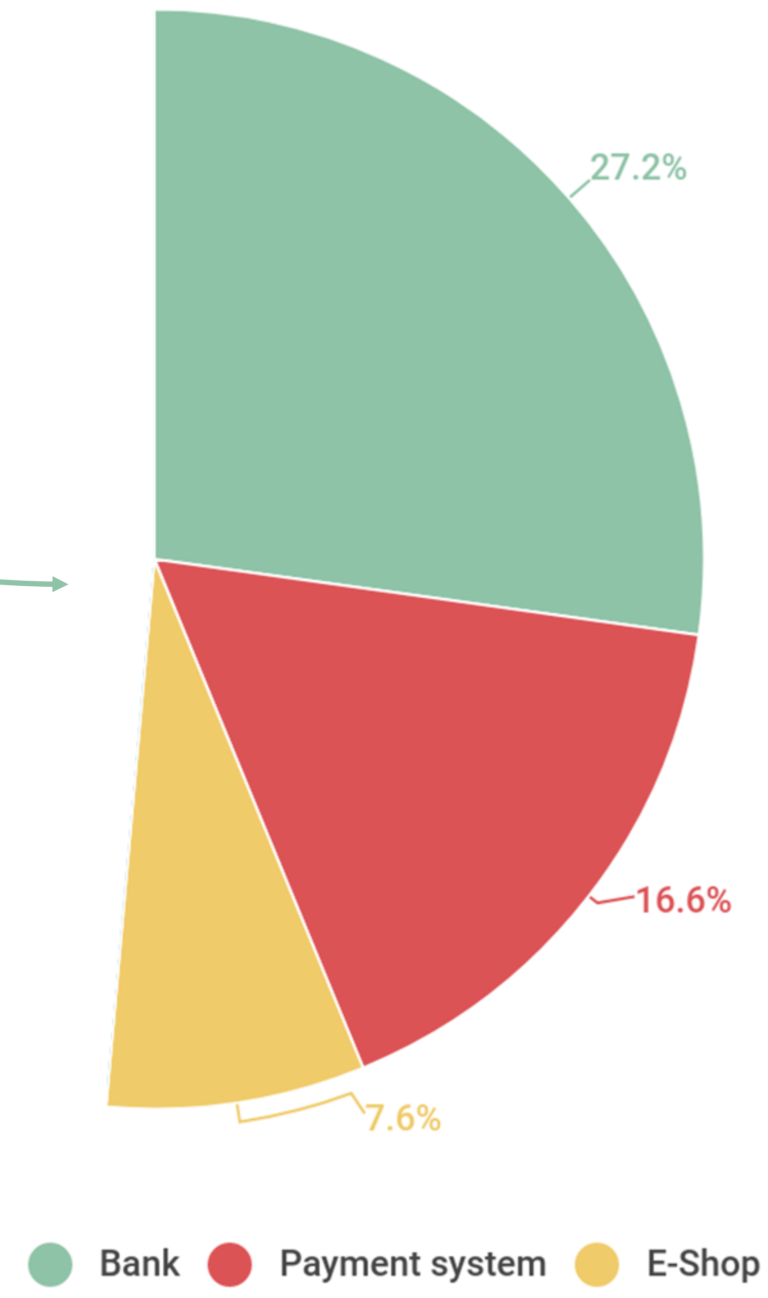
51,4%

financial-related phishing on overall phishing attacks

The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky, 2014-2019

+5,5%

spread of bank-related phishing from 2018 to 2019

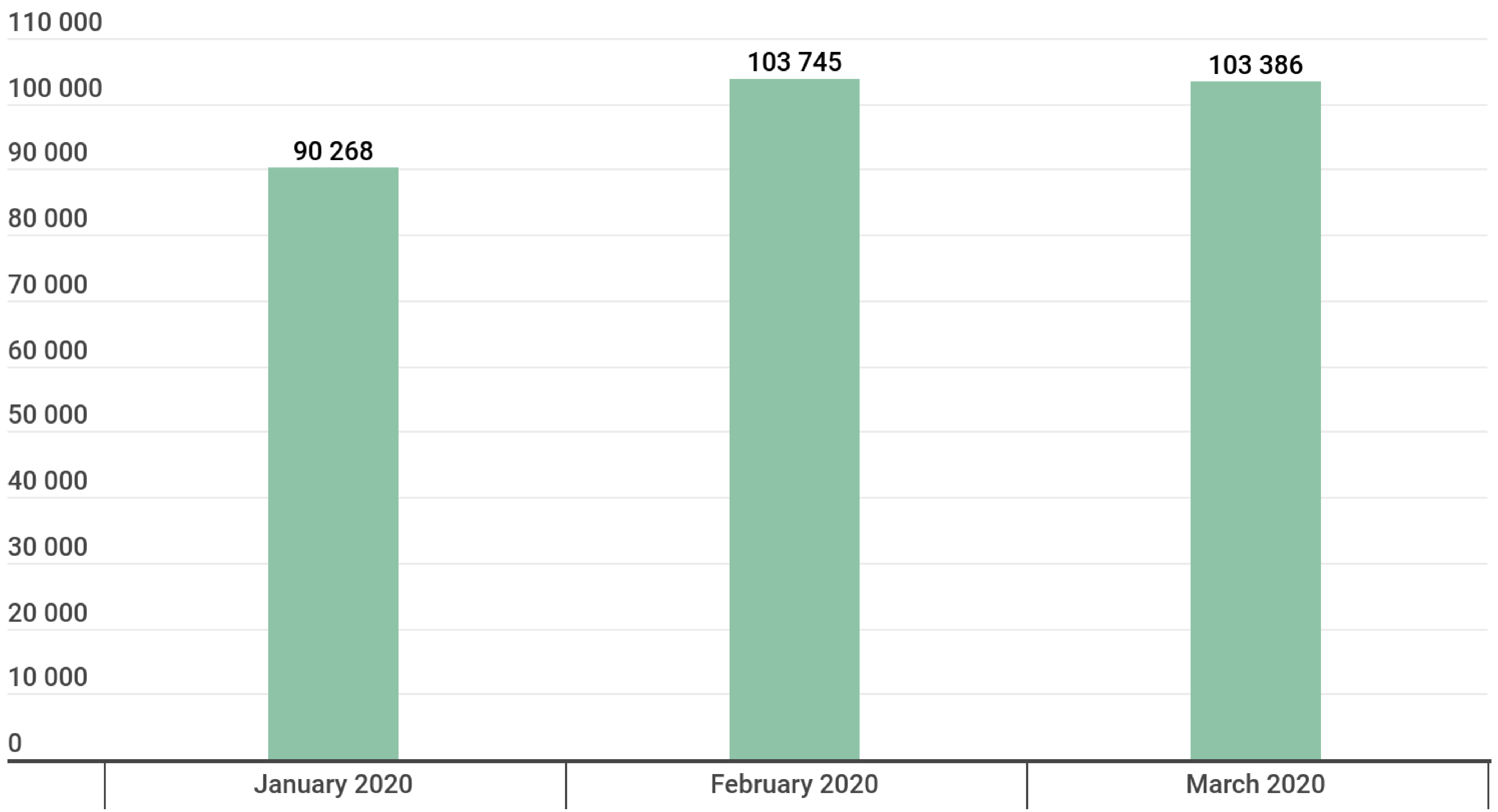


The distribution of different types of financial phishing detected by Kaspersky in 2019

Source: Kaspersky – https://securelist.com/financial-cyberthreats-in-2019/96692/

Source: Kaspersky – https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/

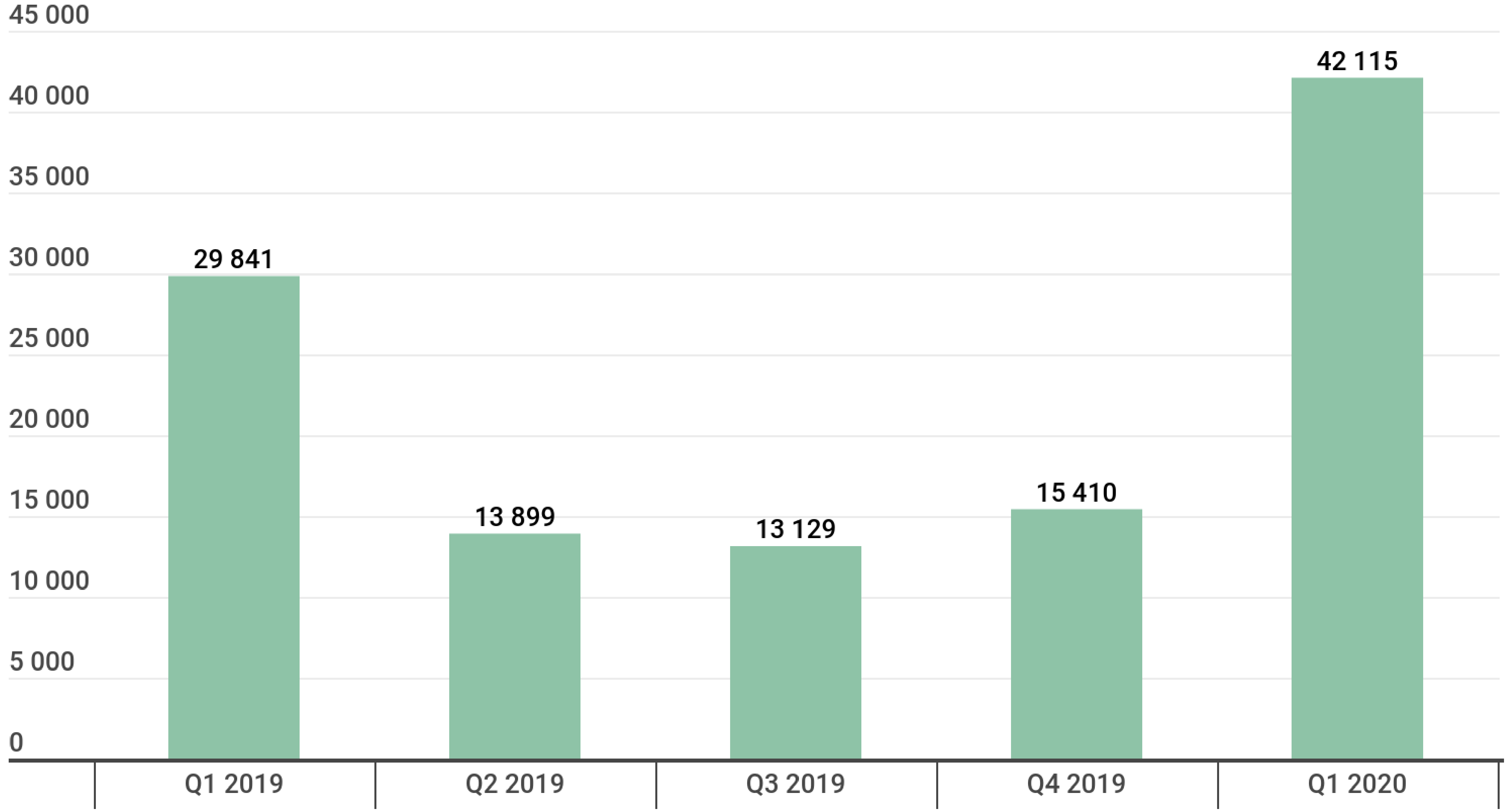
Security Vulnerabilities
Financial Malware



Number of unique users attacked by financial malware

Sources: Kaspersky – https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/

Security Vulnerabilities
Financial Malware



Number of installation packages of mobile banking trojans detected by Kaspersky, Q1 2019 – Q1 2020

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC

Sources: Kaspersky – https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/
Clusit – Rapporto 2020 sulla Sicurezza ICT in Italia

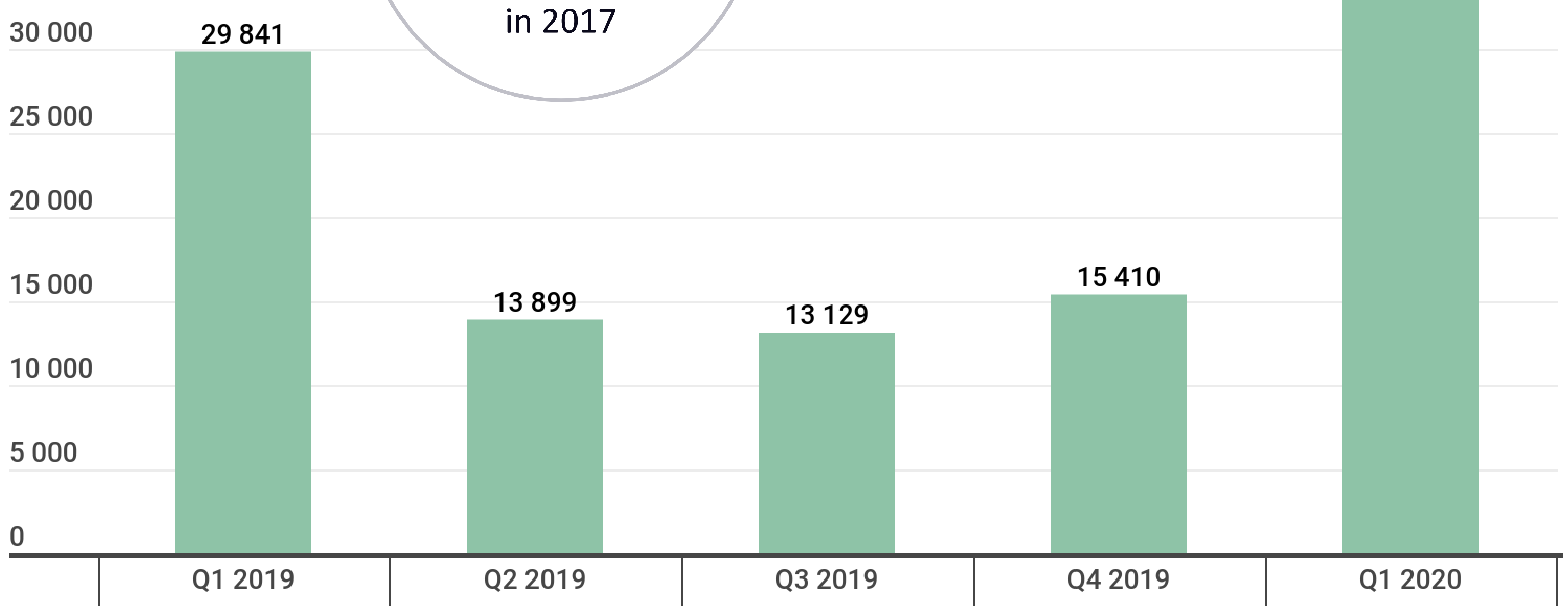
Security Vulnerabilities
Financial Malware

41% infections in the financial scenario by the top 3 malware in 2019

62% infections in the financial scenario by the top 3 malware in 2018

70% infections in the financial scenario by the top 3 malware in 2017

~90% infections in the financial scenario by the top 3 malware in 2016



Number of installation packages of mobile banking trojans detected by Kaspersky, Q1 2019 – Q1 2020

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Security Vulnerabilities

TrickBot

banking credentials

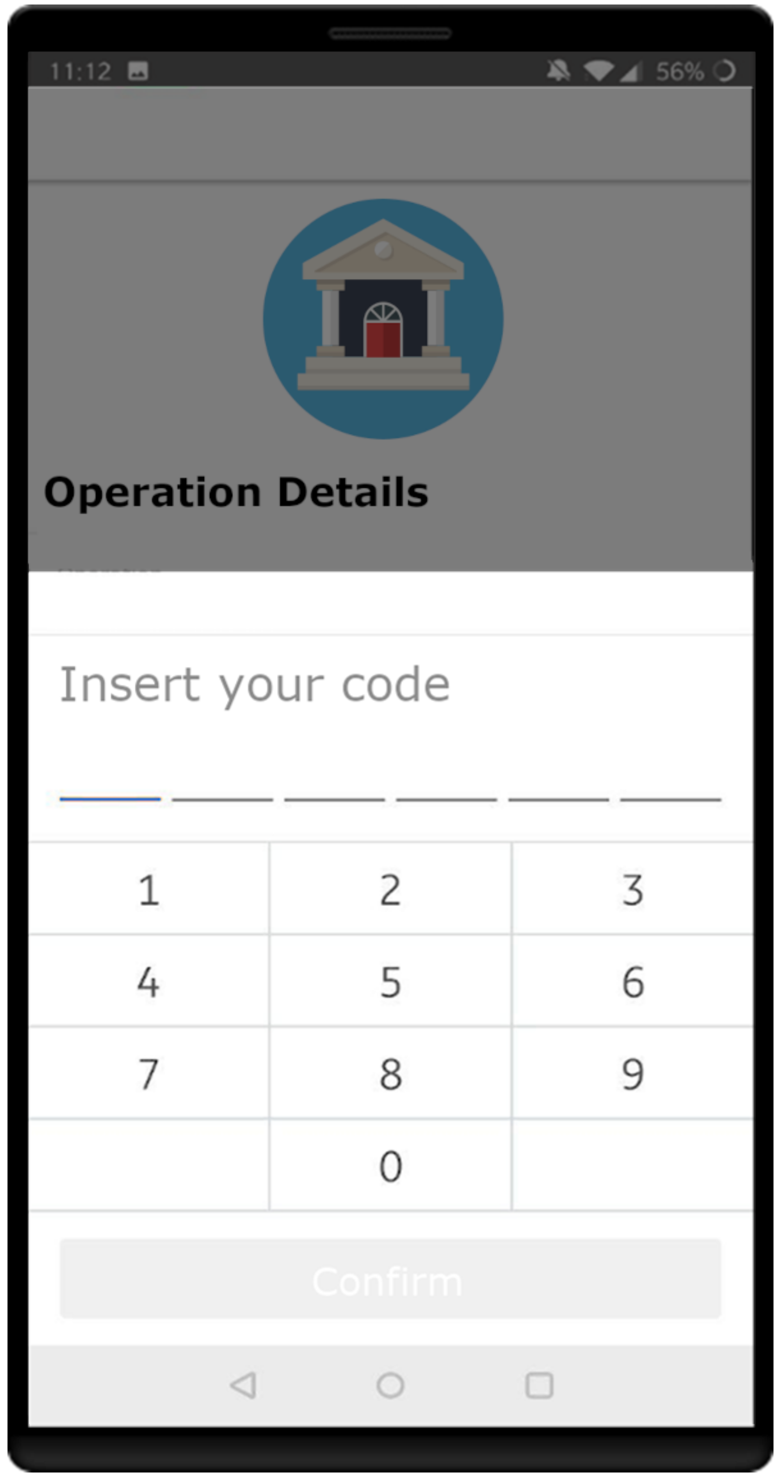
TrickBot now pushes Android app for bypassing 2FA on banking accounts

Malicious TrickMo app seen deployed in Germany for now, but broader use is expected.

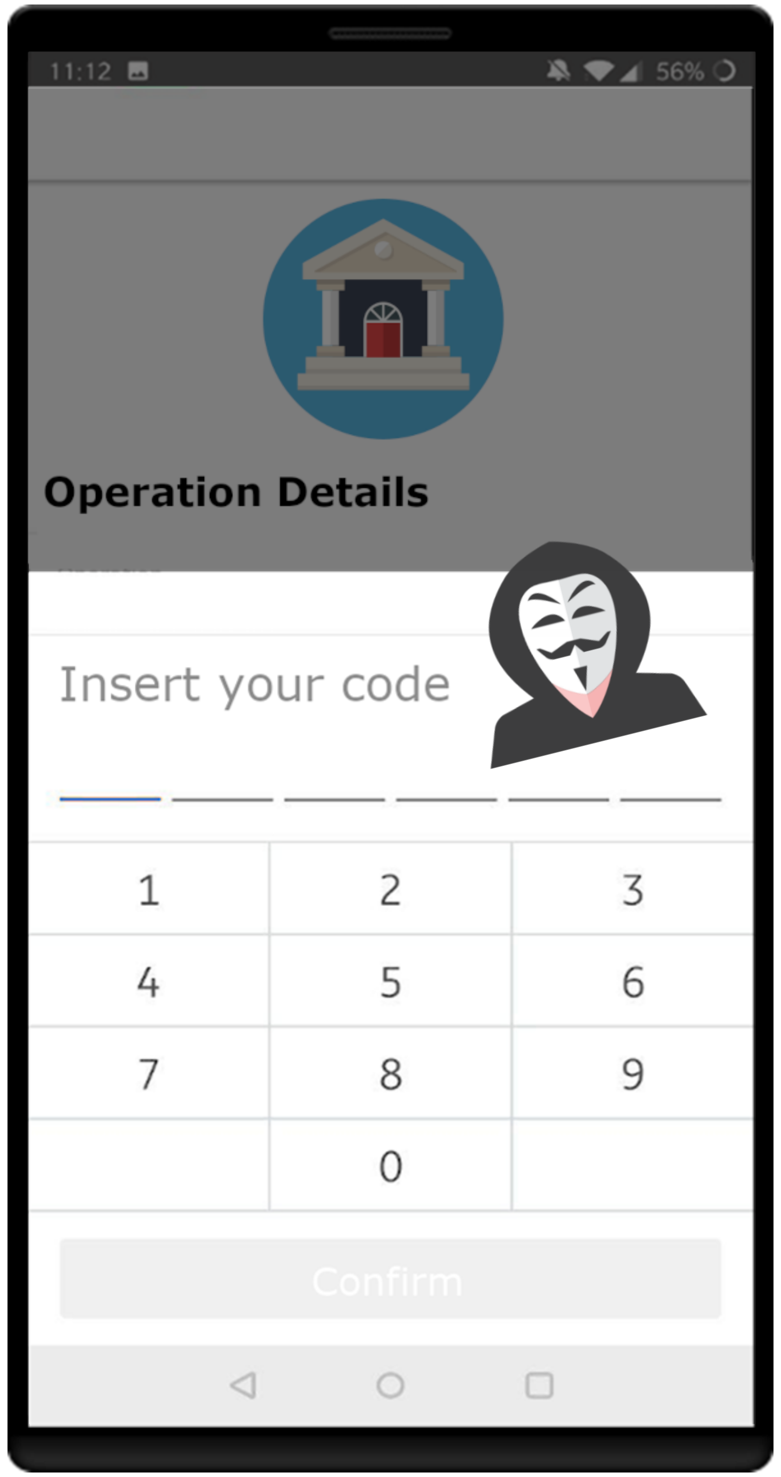
Security Vulnerabilities
TrickBot

- banking credentials
- FileZilla credentials
- KeePass database
- locale SSL certificates
- OpenVPN credentials
- Putty credentials
- OpenSSH keys
- TeamViewer credentials
- Bitcoin wallets
- Outlook credentials
- WinSCP credentials
- VNC credentials
- Git credentials
- Windows RDP credentials

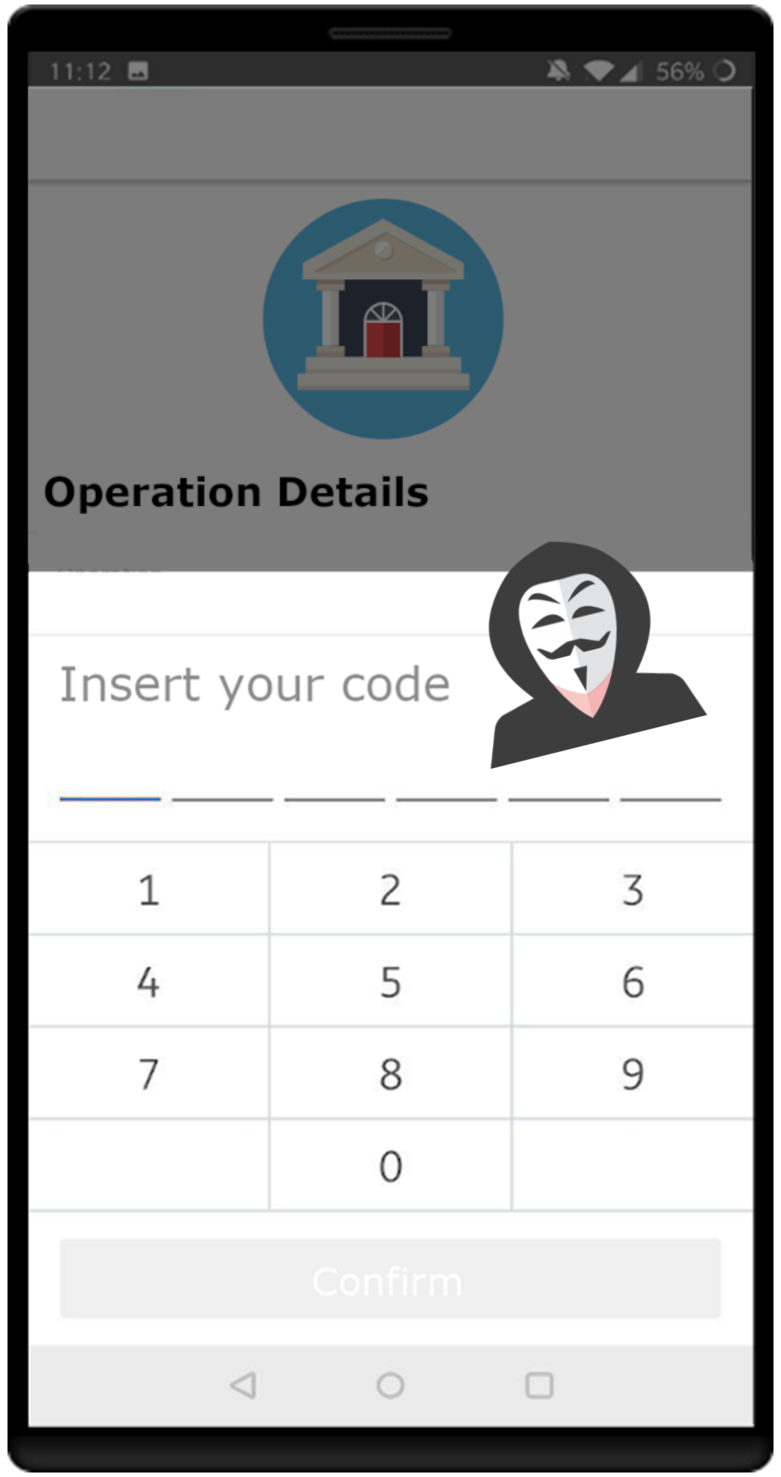
Security Vulnerabilities
TrickBot

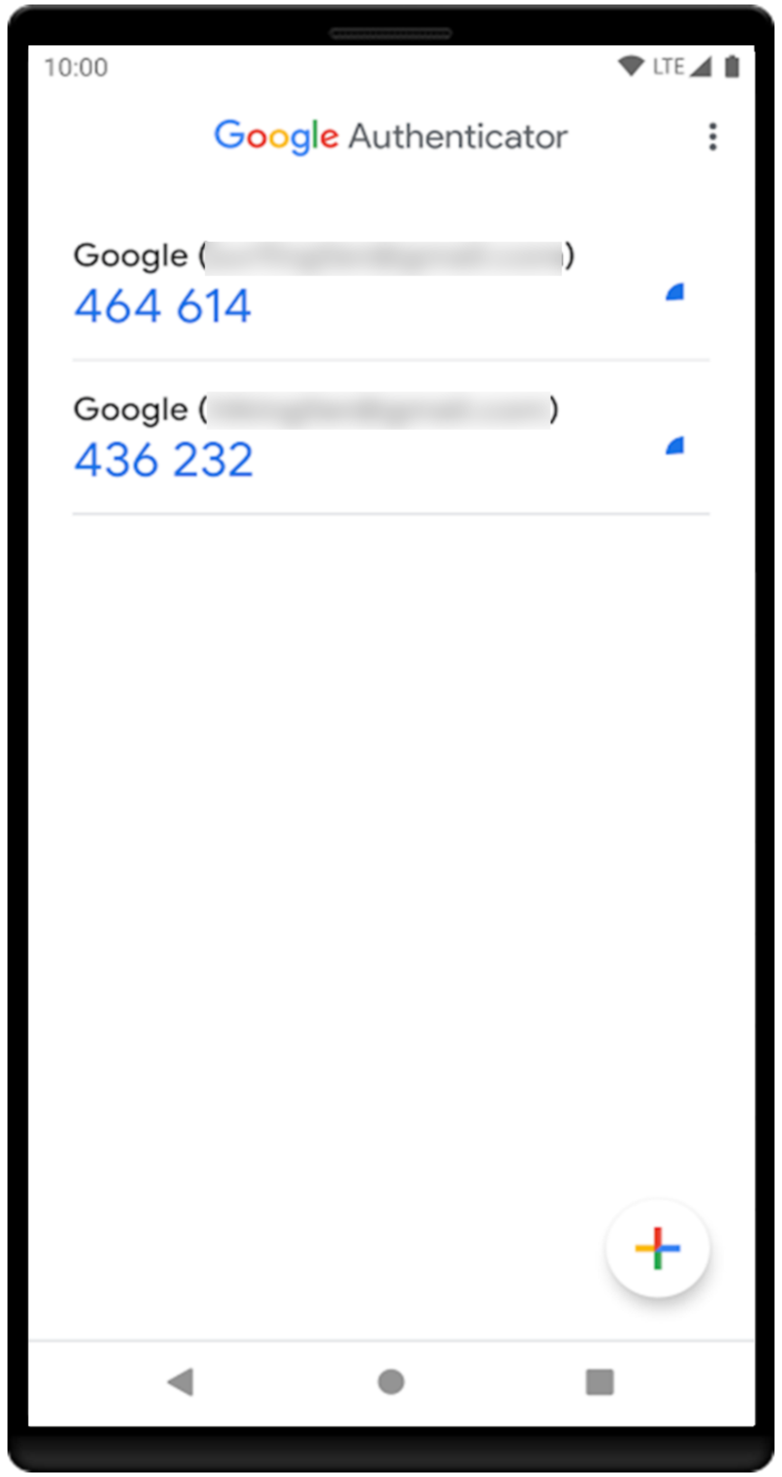


Security Vulnerabilities
TrickBot



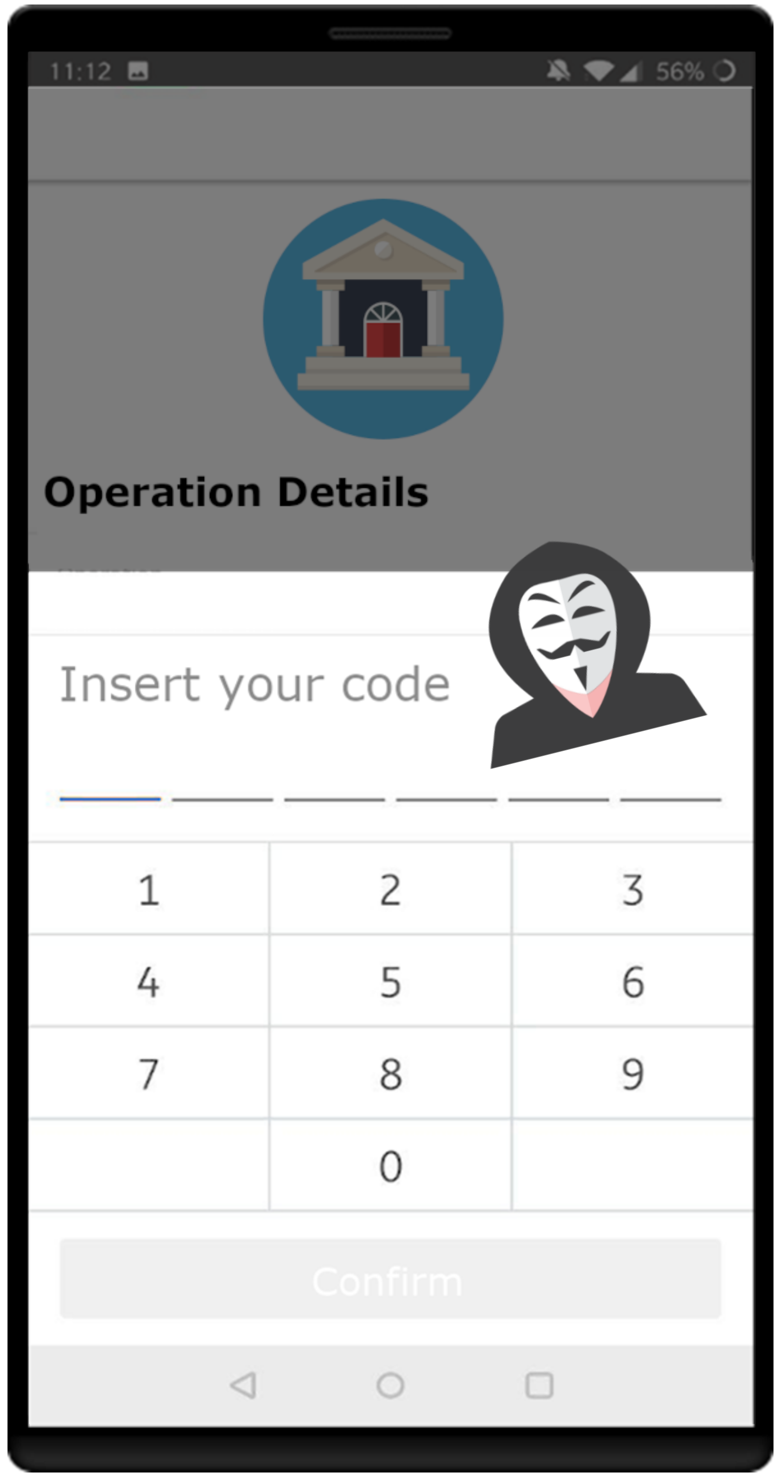
Security Vulnerabilities
TrickBot

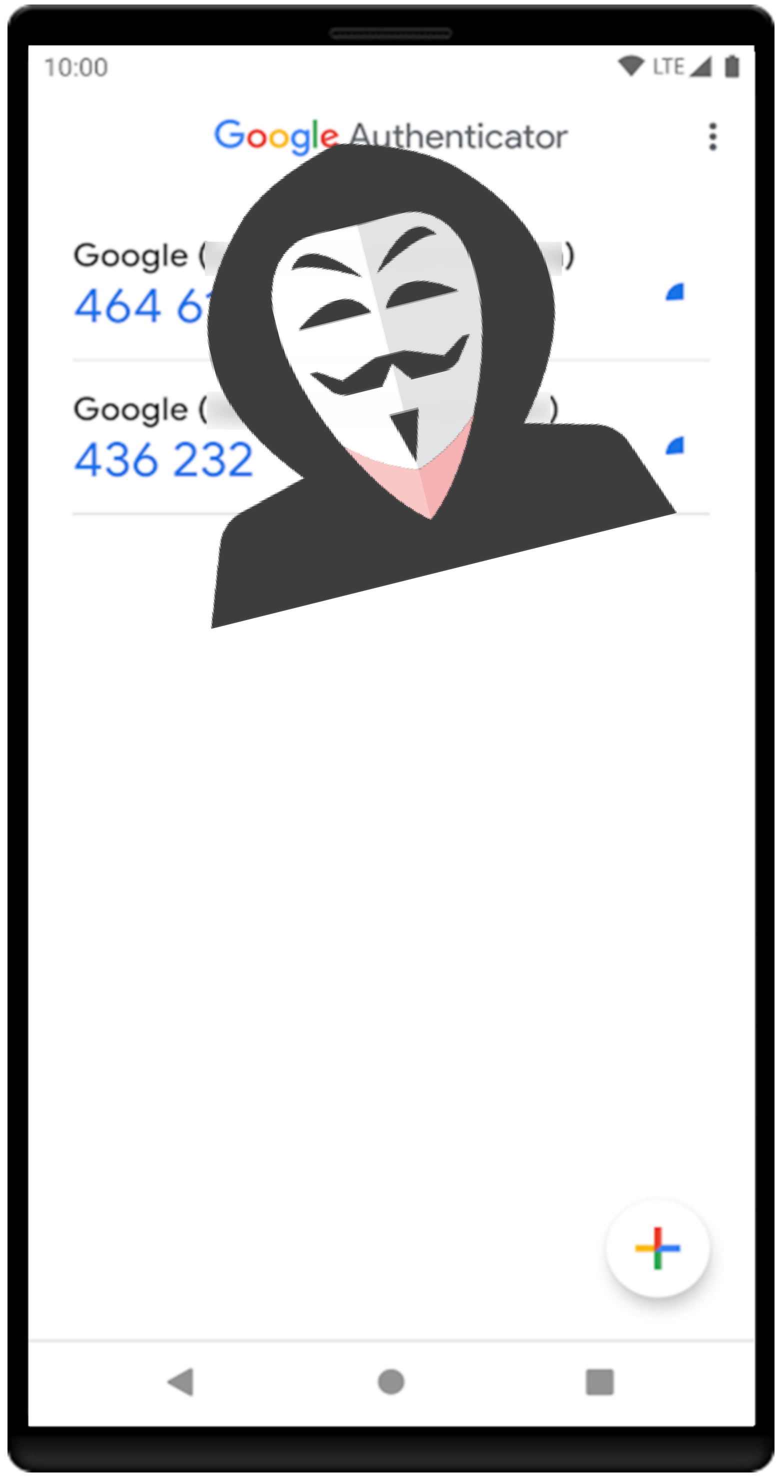




FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Security Vulnerabilities
TrickBot





FONDAZIONE BRUNO KESSLER
ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Agenda

- Overview of security vulnerabilities affecting the financial scenario
- **Impacts of the PSD2 on financial protocols**
- Best practices to reduce the risks online

Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment services in the internal market.

Main focus:

- fostering the birth of new innovative solutions built around financial institutions (*open banking*)
- improving the security of *e-banking* protocols

Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment services in the internal market.

Main focus:

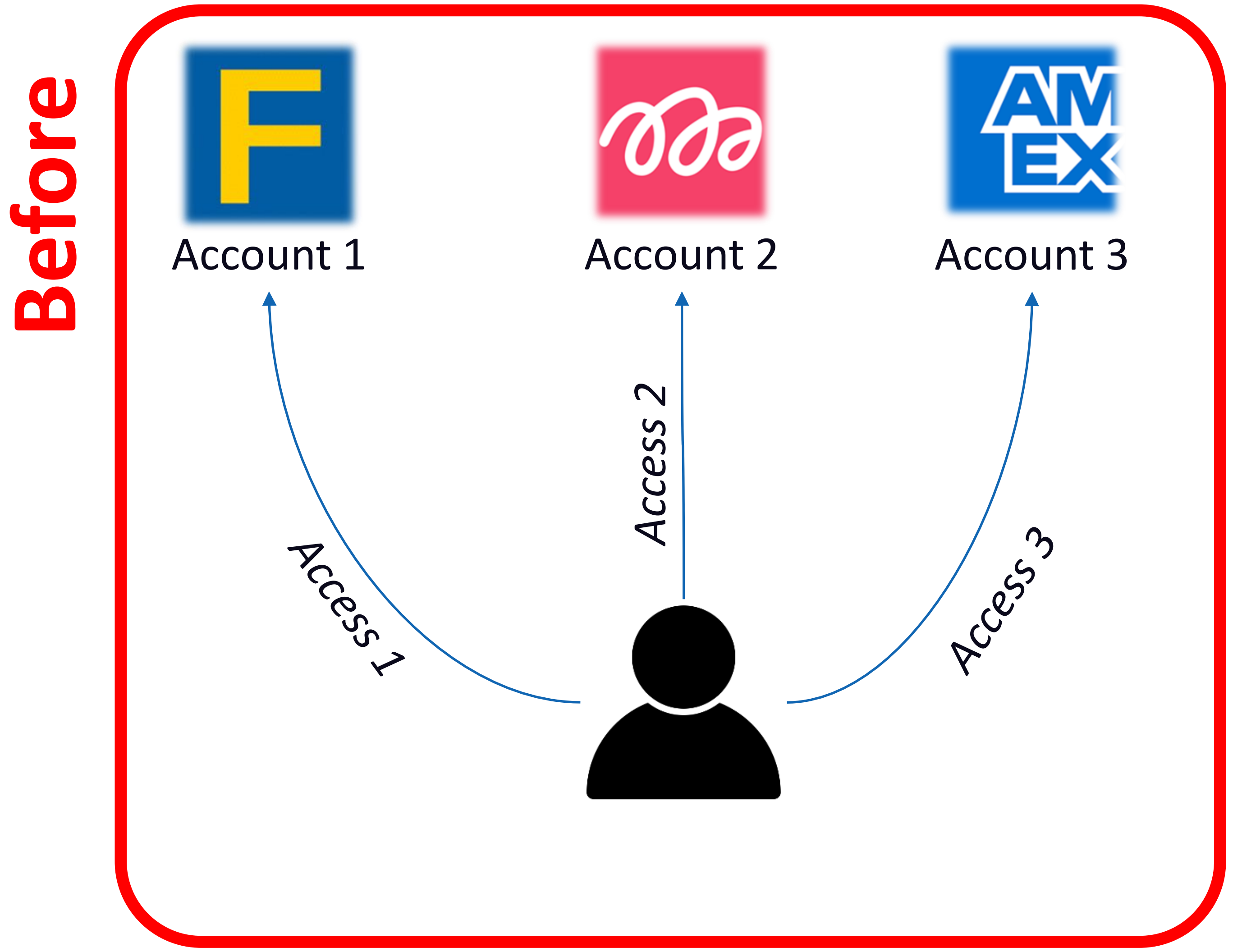
- fostering the birth of new innovative solutions built around financial institutions (*open banking*)
- improving the security of *e-banking* protocols

Payment Services Directive (PSD2)
Open banking

Third-party applications can access and aggregate users' banking information.

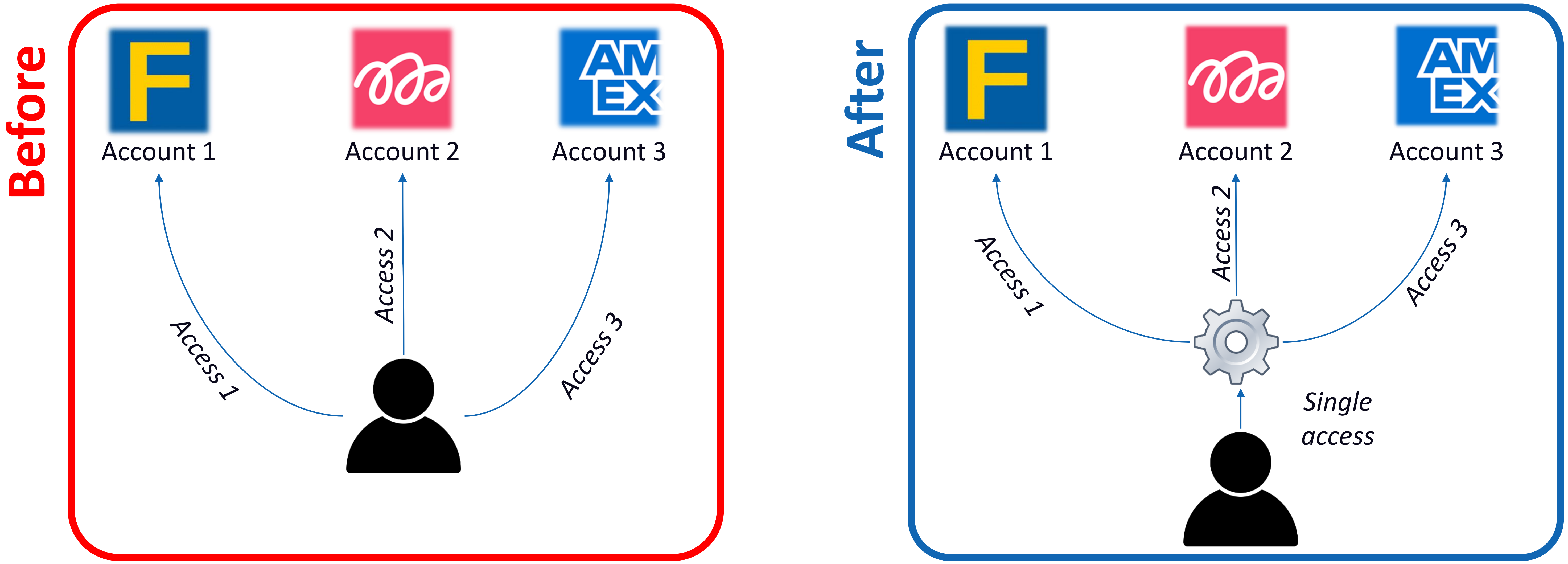
Payment Services Directive (PSD2)
Open banking

Third-party applications can access and aggregate users' banking information.



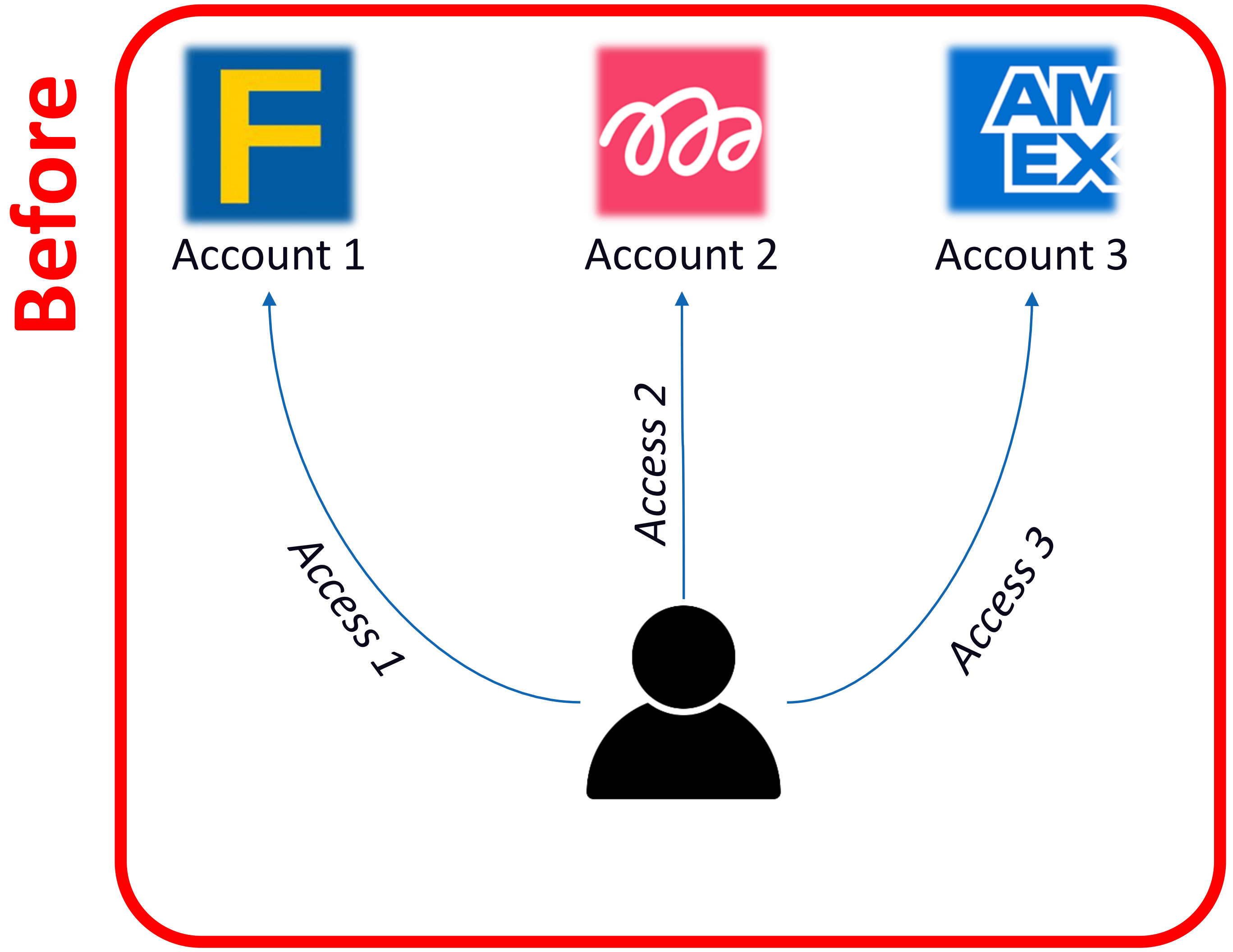
Payment Services Directive (PSD2)
Open banking

Third-party applications can access and aggregate users' banking information.



Payment Services Directive (PSD2)
Open banking

Third-party applications can access and aggreg mation.



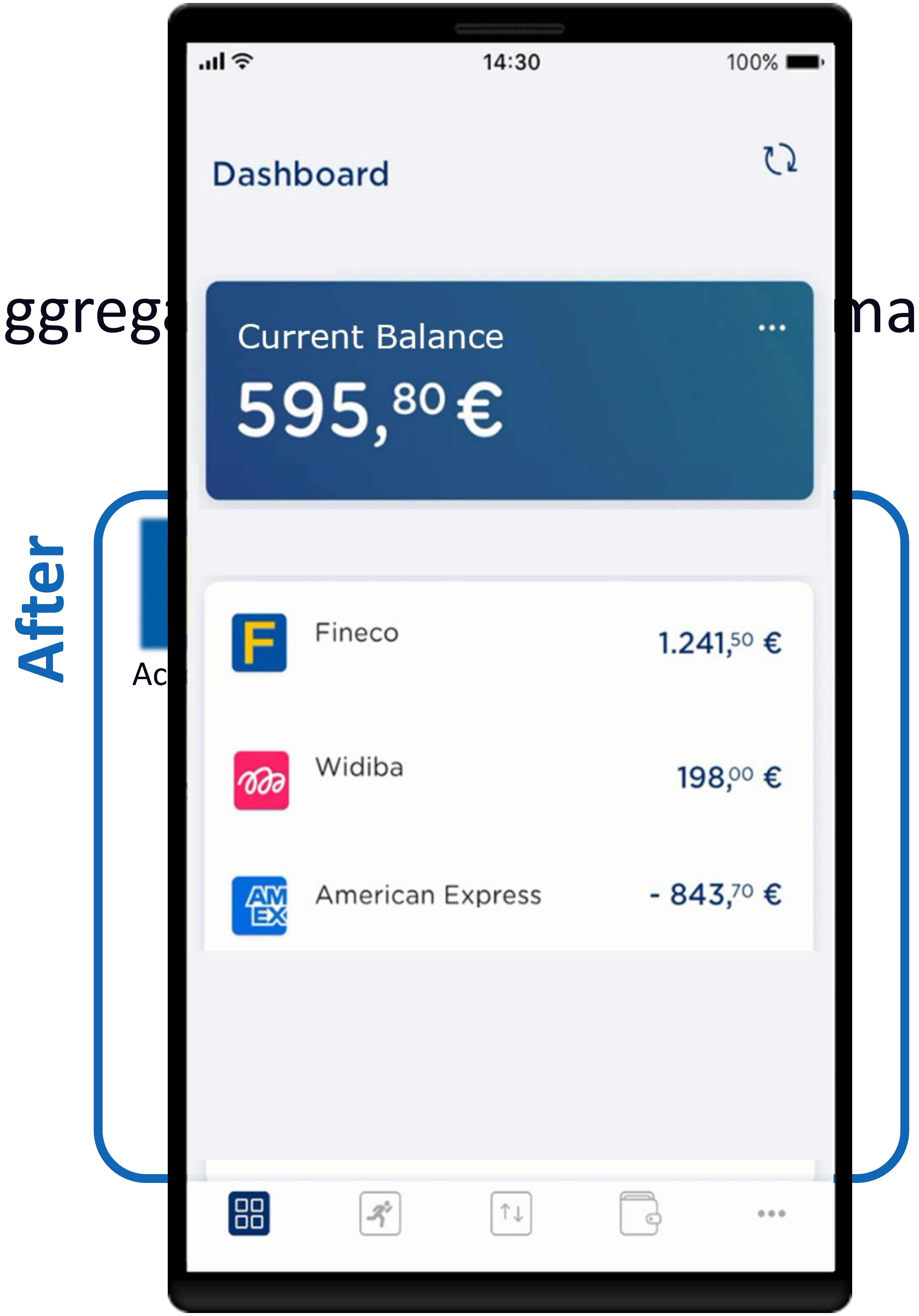


Image Source: edited from Yolt – https://www.yolt.com/

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC

Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment services in the internal market.

Main focus:

- fostering the birth of new innovative solutions built around financial institutions (*open banking*)

- improving the security of *e-banking* protocols

Payment Services Directive (PSD2)
Security of e-Banking Protocols

Strong Customer Authentication (SCA)

Dynamic Linking

Payment Services Directive (PSD2)
Strong Customer Authentication (SCA)

Authentication relying on more than a single *authentication factor:*

Images source: https://appspicket.com/the-next-generation-in-2fa-technology/

Payment S

Strong Cus

Authenticati

Actions	SCA required?
Balance inquiry	Depends on the case
Consultation of payment history of past 90 days	Depends on the case
Payments to trusted beneficiaries	Depends on the case
Recurrent payments with same amount and same payee	Depends on the case
Payments not exceeding € 30	Depends on the case
Payments exceeding € 30	Always

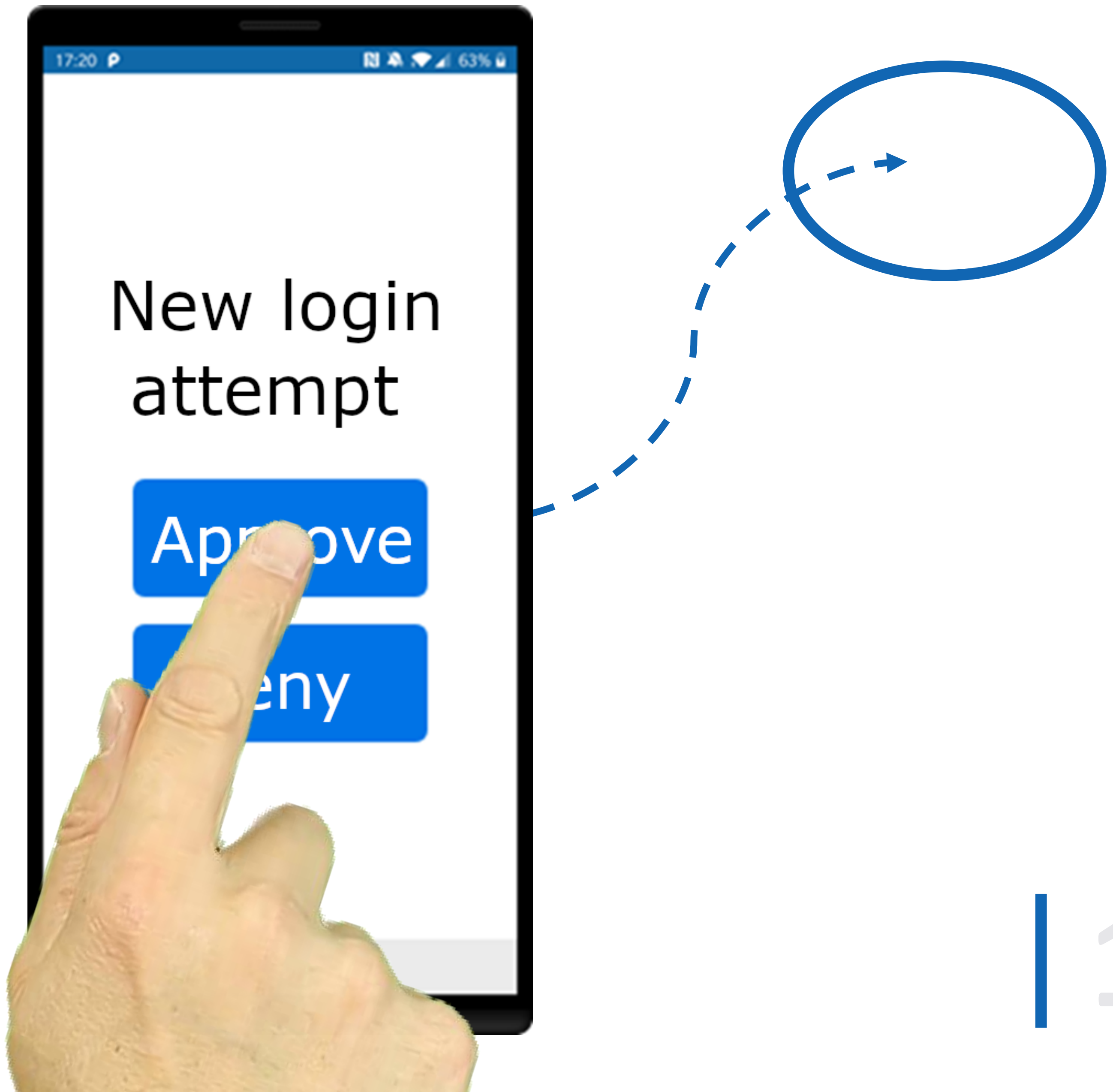
Images source: https://appspicket.com/the-next-generation-in-2fa-technology/

Authentication Code

Authentication factors must generate an *authentication code.*

Authentication code visible to the user

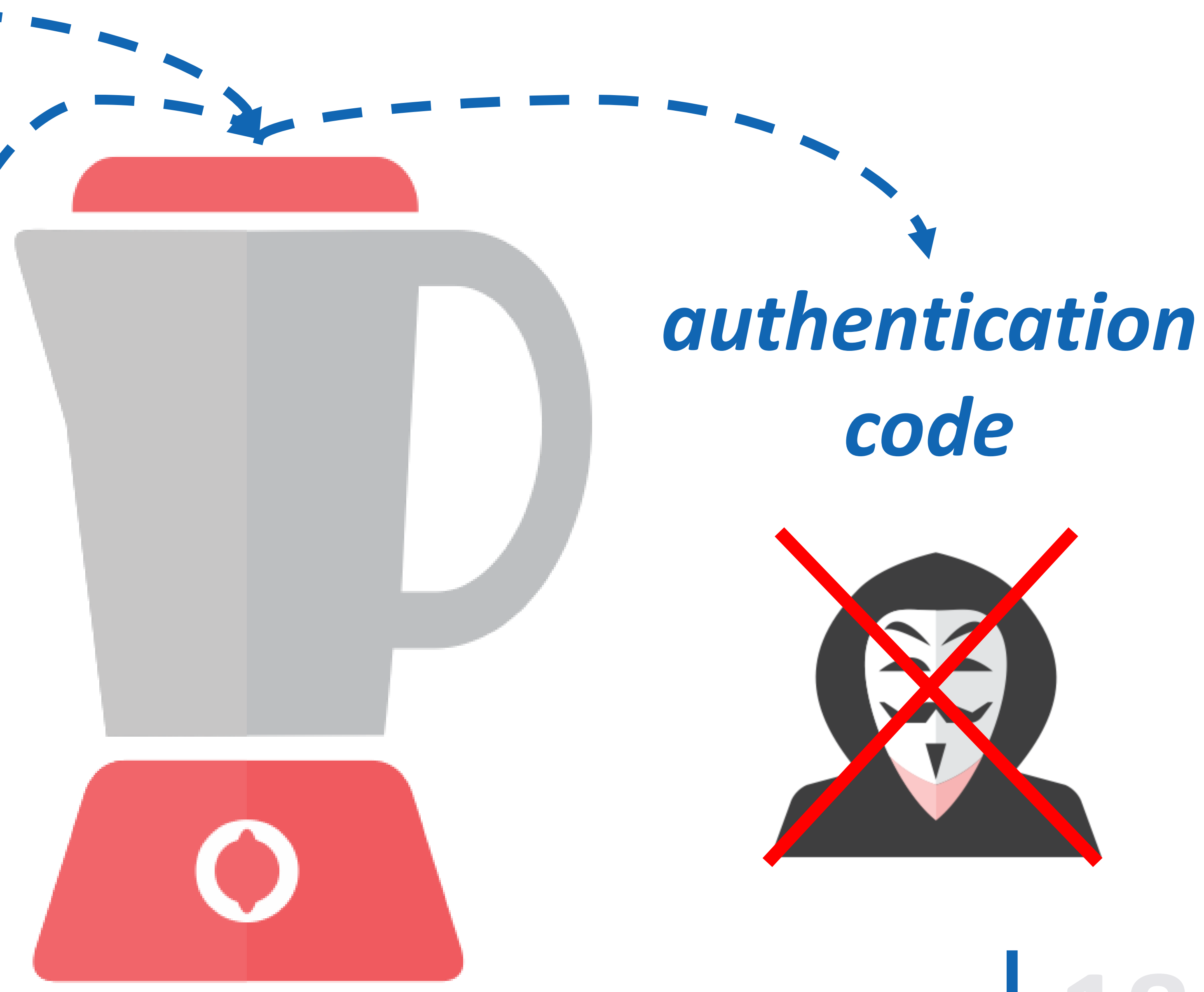
Authentication code hidden to the user



Payment Services Directive (PSD2)
Dynamic Linking

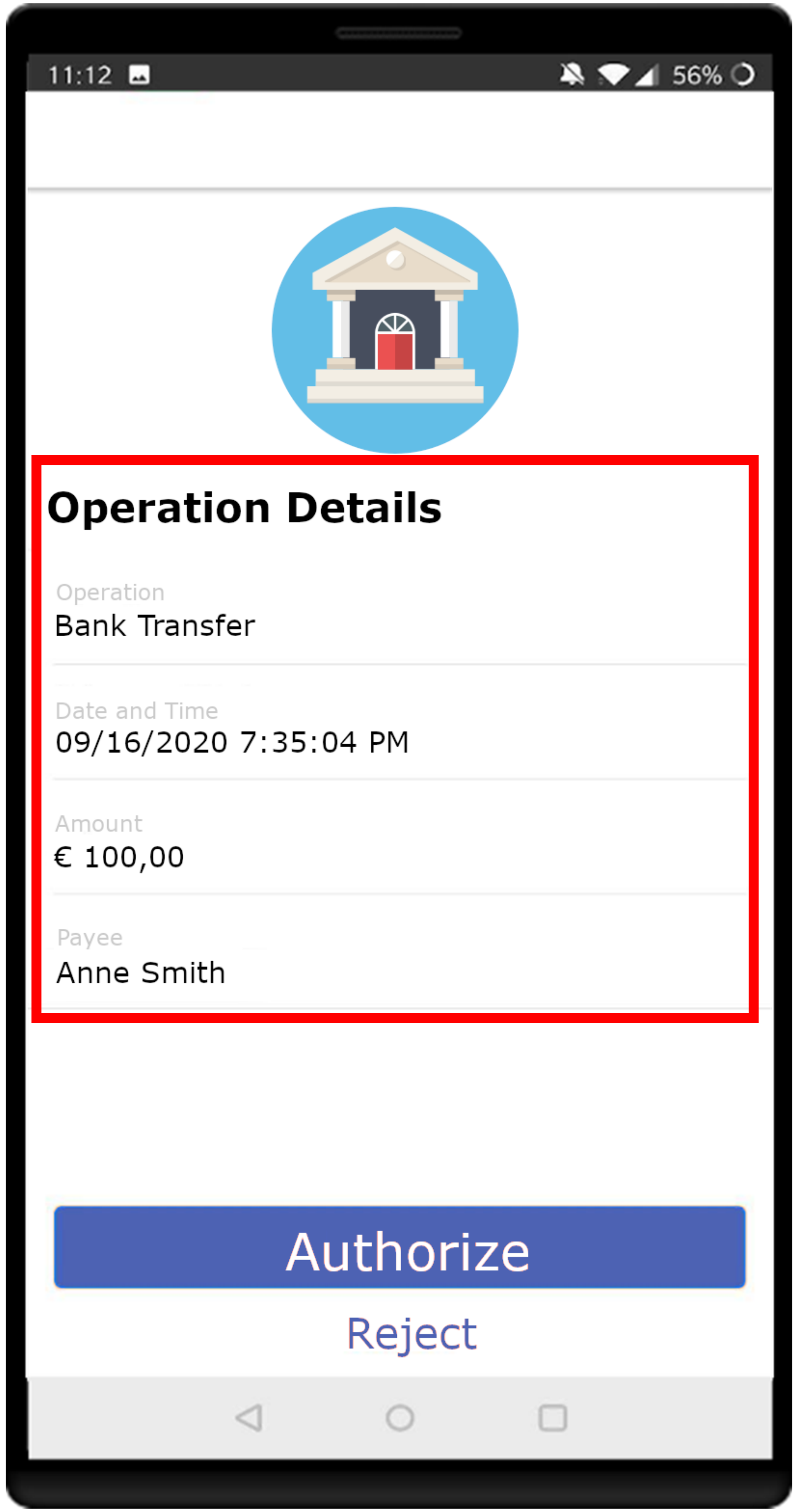
During a transaction, the *authentication code* must be strongly connected with the ongoing operation.

Transfer no.	AA/1234
Payer Name	John Smith
Payee Name	Anne Smith
Payee IBAN Code	IT12T1234512345123456789012
Amount	100,00 EUR

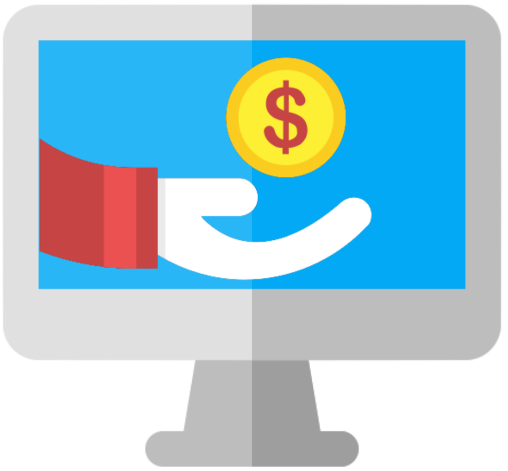


Payment Services Directive (PSD2)
Dynamic Linking

Moreover, the user is always displayed the operations' details before the authorization.



Payment Services Directive (PSD2)
Use Case



1st Bank
Before and After PSD2

2nd Bank
Before and After PSD2

Use Case – Before PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.

Use Case – Before PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.

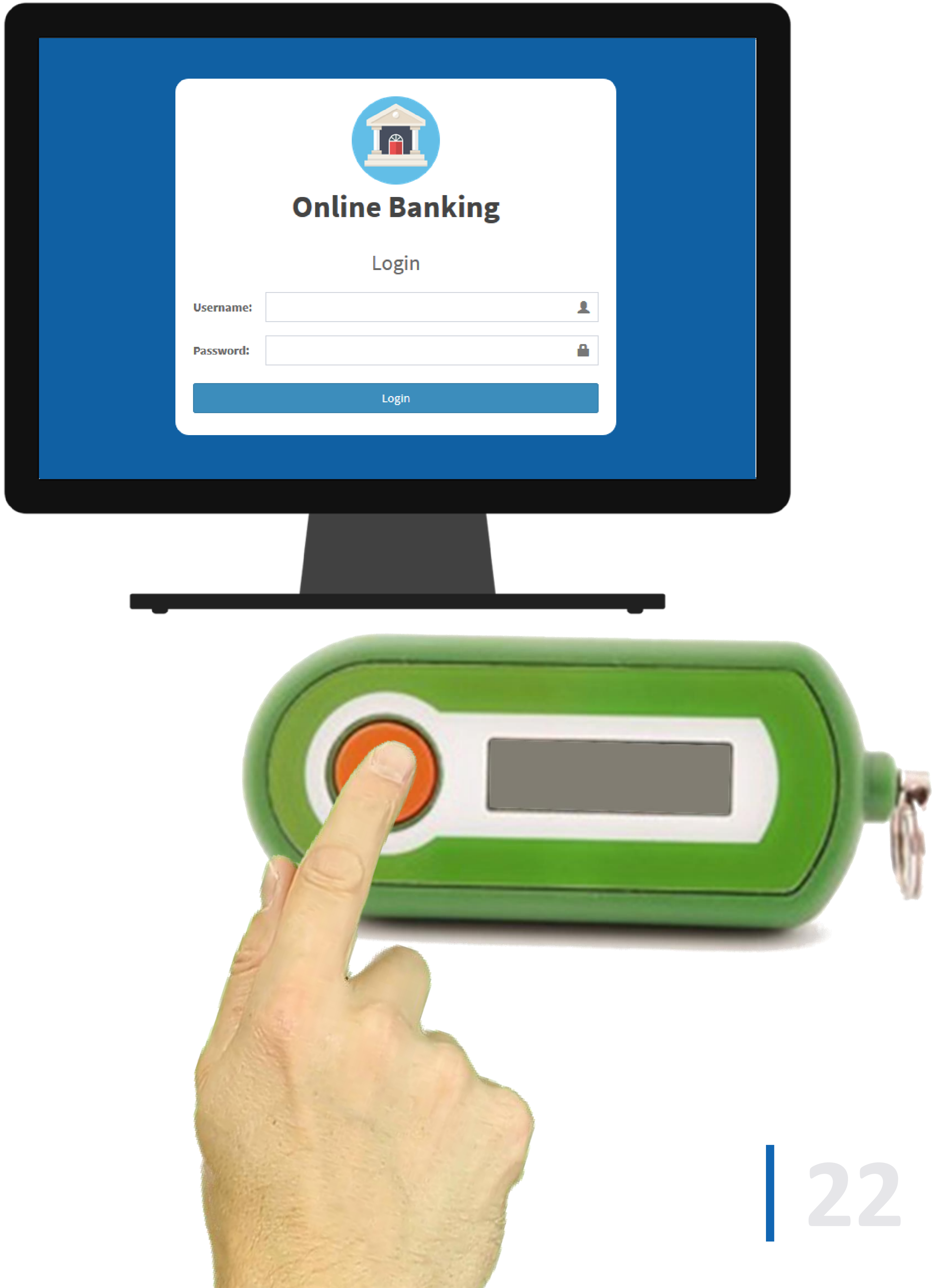
2. The user generates a code through the matrix and inserts it in the online page to authorize the operation.

Use Case – Before PSD2
2nd Bank

1. The user authenticates on the online banking and performs an operation.

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FIN SEC

Use Case – Before PSD2
2nd Bank



1. The user authenticates on the online banking and performs an operation.

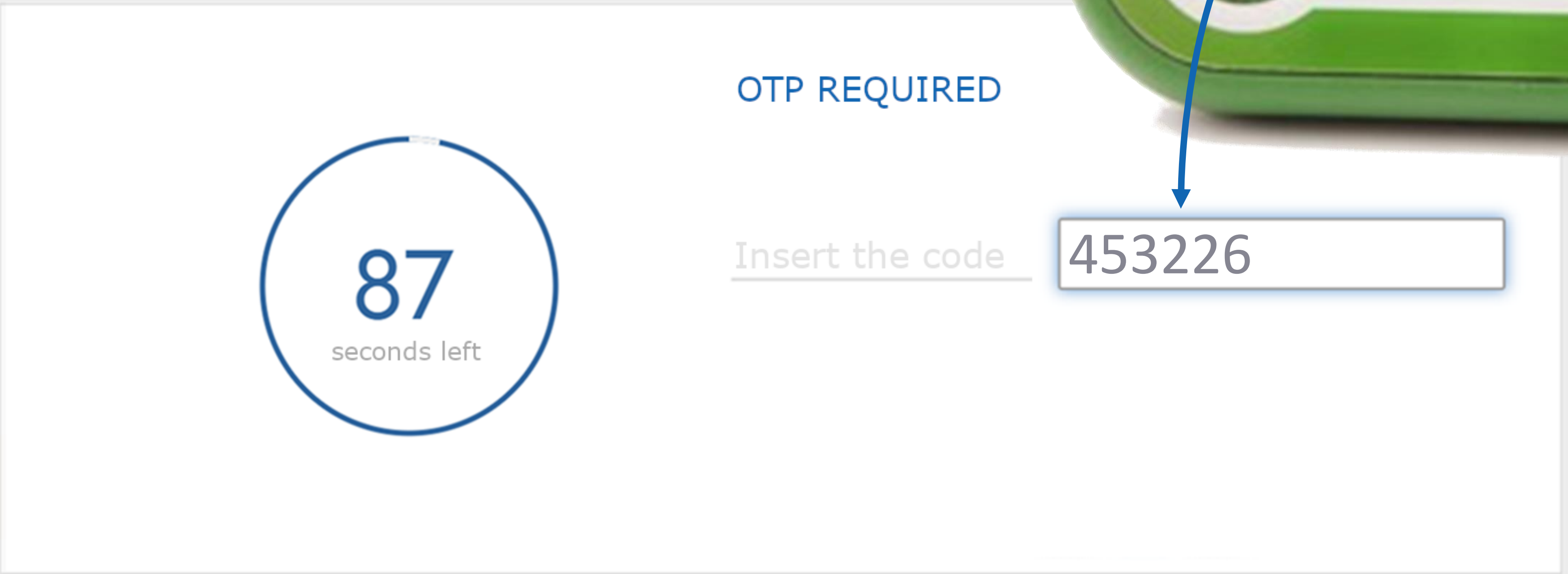
2. The user generates a code through the device and inserts it in the online page to authorize the operation.

FONDAZIONE BRUNO KESSLER
ICT
CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST
SECURITY & TRUST
FINSEC

Use Case – Before PSD2
2nd Bank

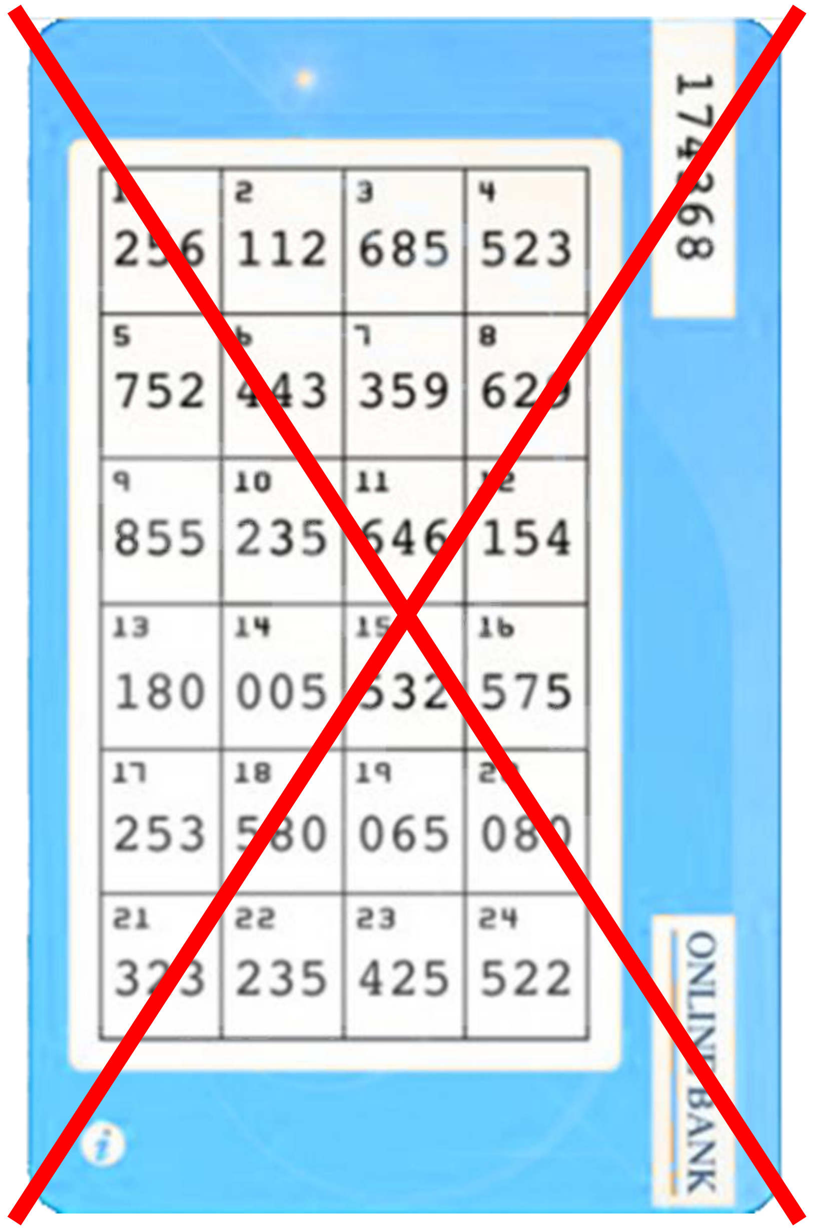
1. The user authenticates on the online banking and performs an operation.

2. The user generates a code through the device and inserts it in the online page to authorize the operation.



Payment Services Directive (PSD2)
Not Compliant Solutions

1. The authentication code is not connected with the ongoing operation.



2. Users cannot be aware of which operation they are about to authorize.

Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Silvio Ranise
«*MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols*», ETAA@ESORICS 2019

Use Case Analysis – Before PSD2
1st and 2nd Bank

MuFASA

4 single attackers

Comb	SL	OP	AV	UI	SP	AL	Likelihood	PV	AD	LC	AP	AI	Impact	Risk
ES	5	4	7	4	5	5	MEDIUM	8	6	9	4	7	HIGH	HIGH
MB	3	4	7	4	4	4	MEDIUM	8	6	9	4	7	HIGH	HIGH
SS	9	5	3	2	7	5	MEDIUM	1	7	9	4	5	MEDIUM	MEDIUM
SE	4	9	7	4	6	6	MEDIUM	6	5	9	4	6	MEDIUM	MEDIUM

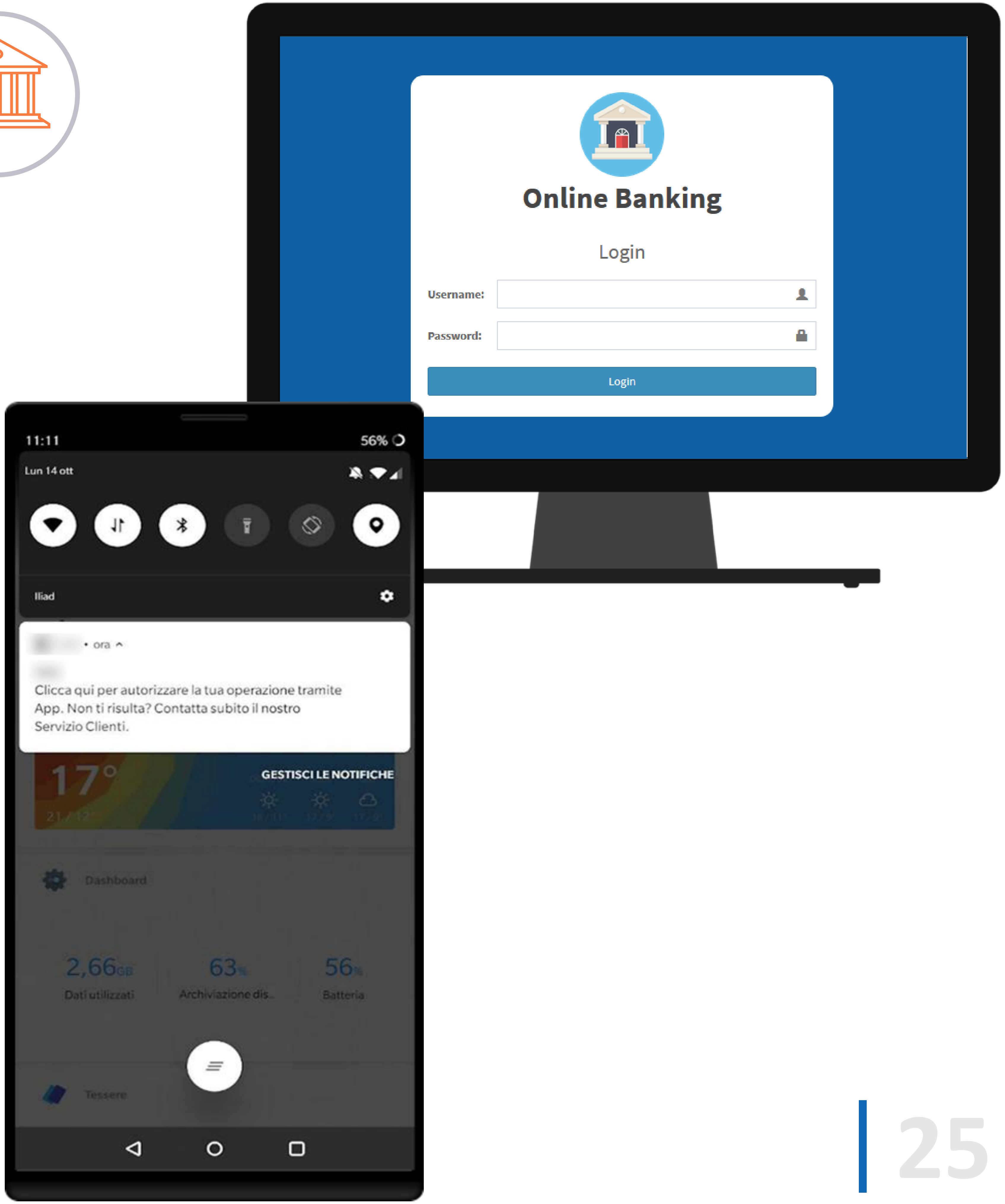
Use Case – After PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Use Case – After PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation.

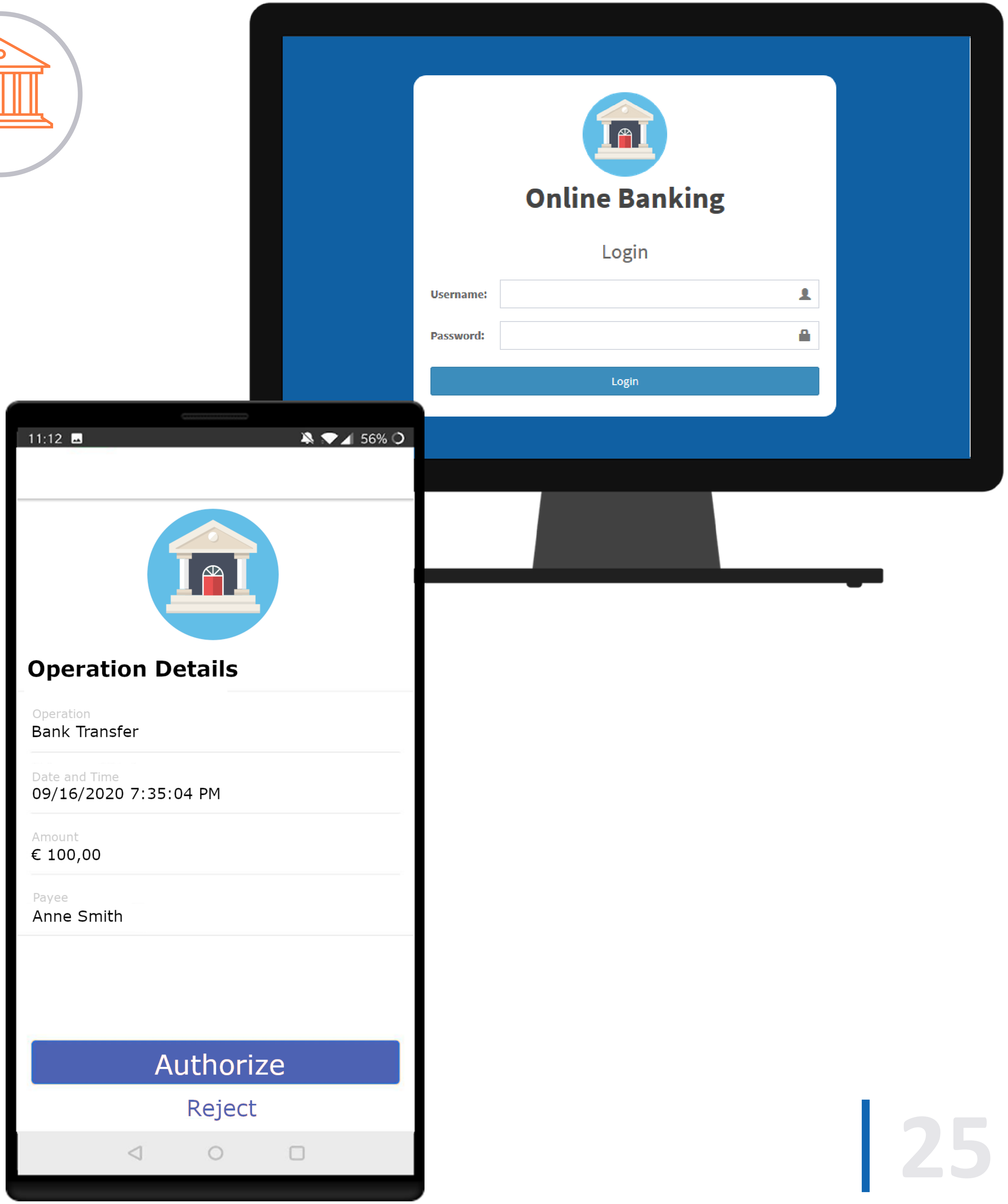


Use Case – After PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation.

Use Case – After PSD2
1st Bank

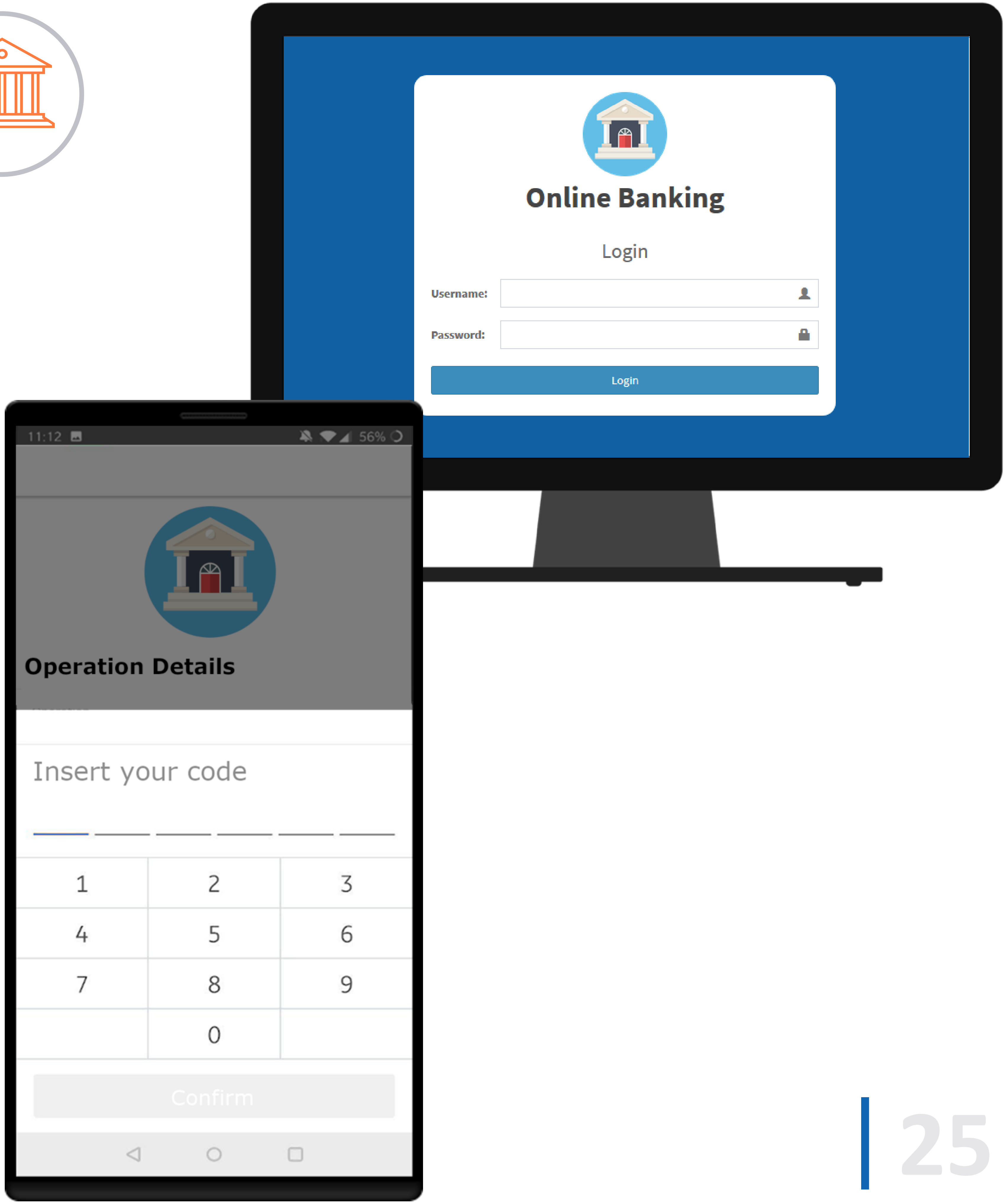
1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation.



FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Use Case – After PSD2
1st Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation.
3. By inserting a specific PIN, the user can authorize the operation.



FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC

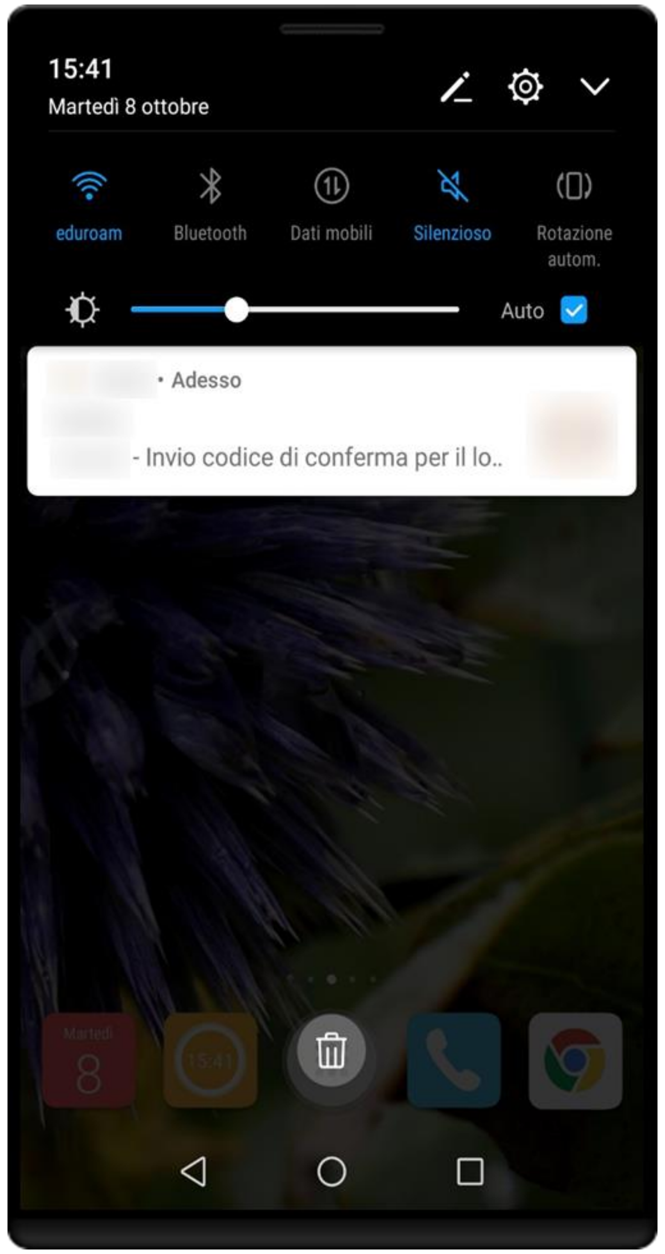
Use Case – After PSD2
2^{nd} Bank

1. The user authenticates on the online banking and performs an operation.

FBK ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
FINSEC

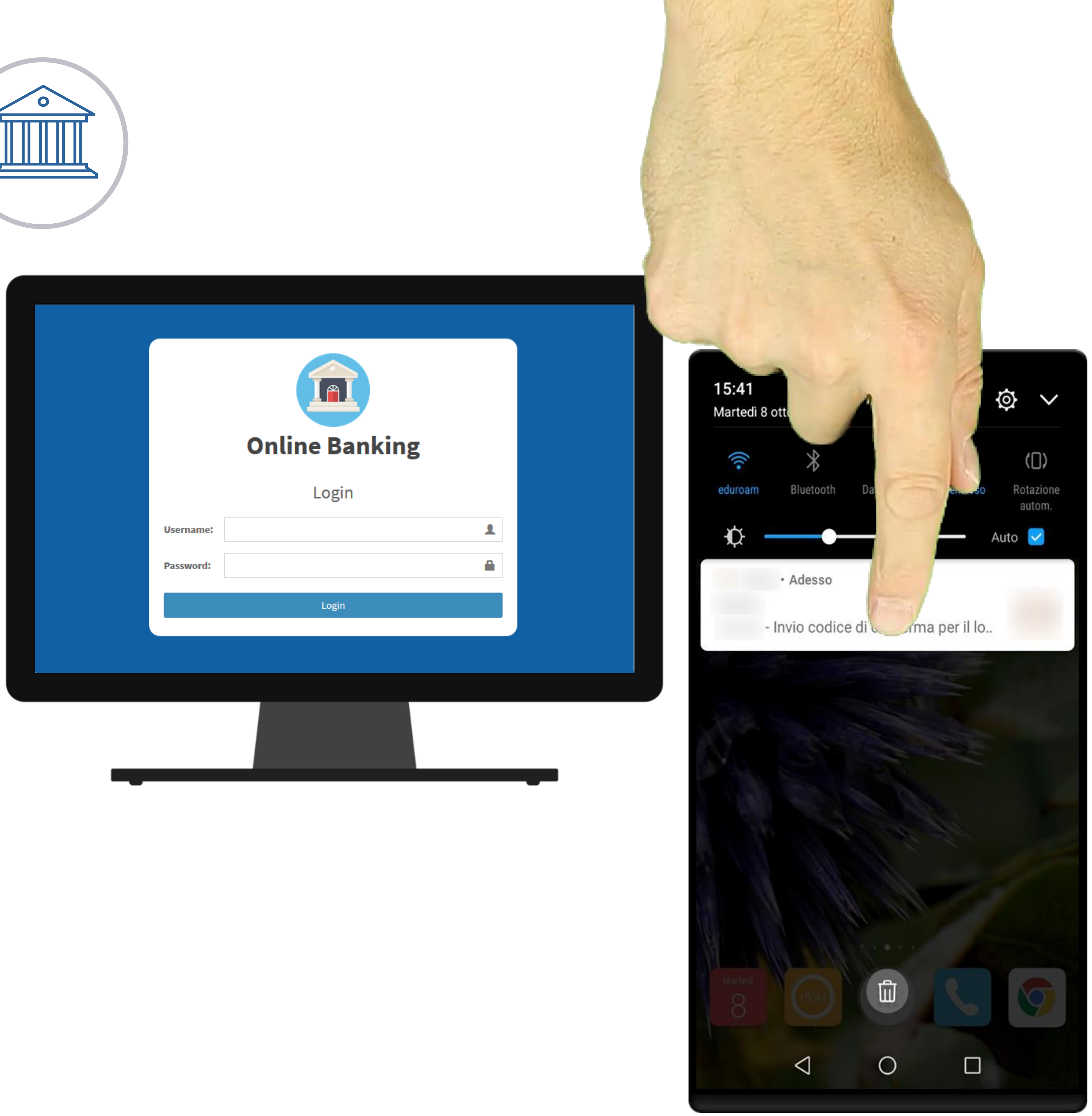
Use Case – After PSD2
2nd Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation and containing an OTP code.



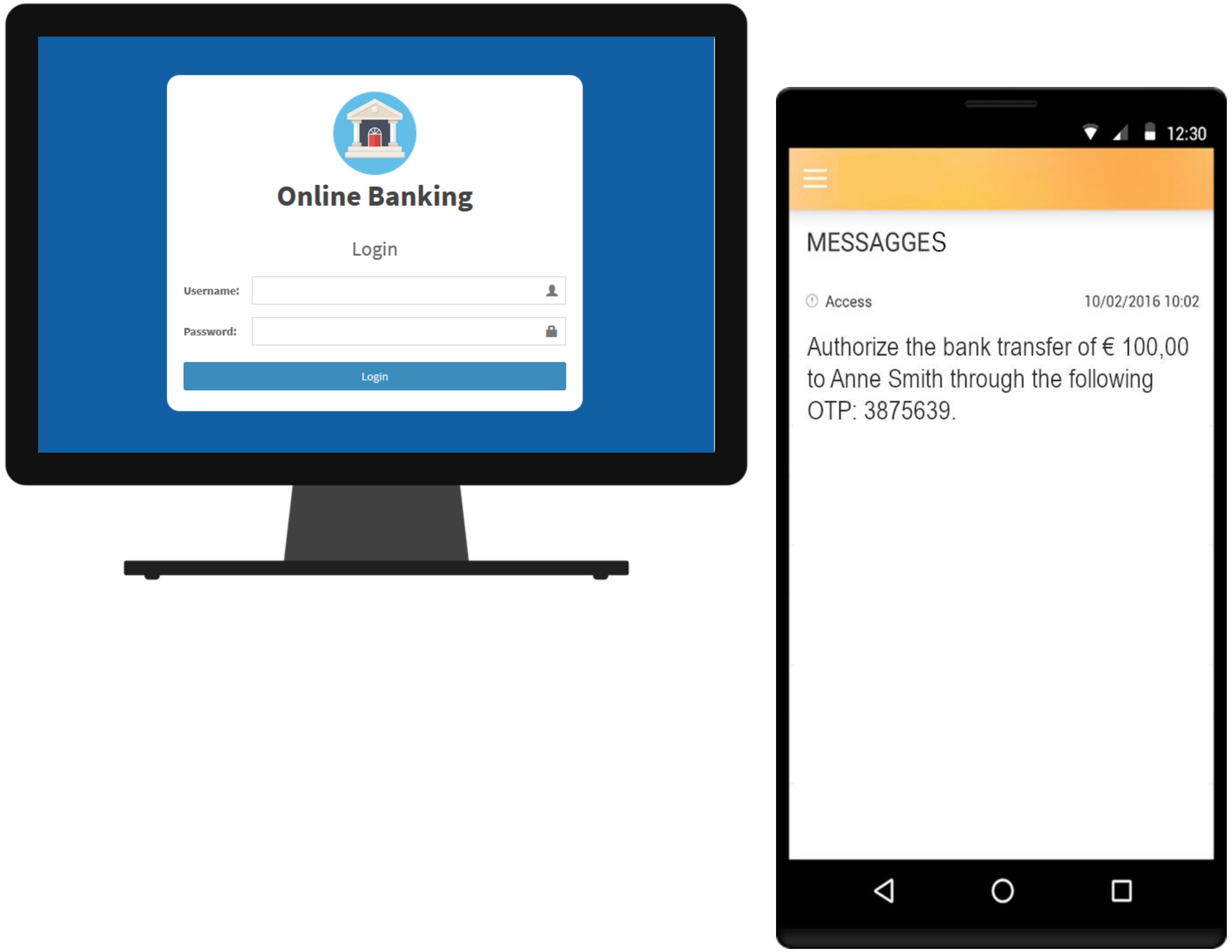
Use Case – After PSD2
2nd Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation and containing an OTP code.



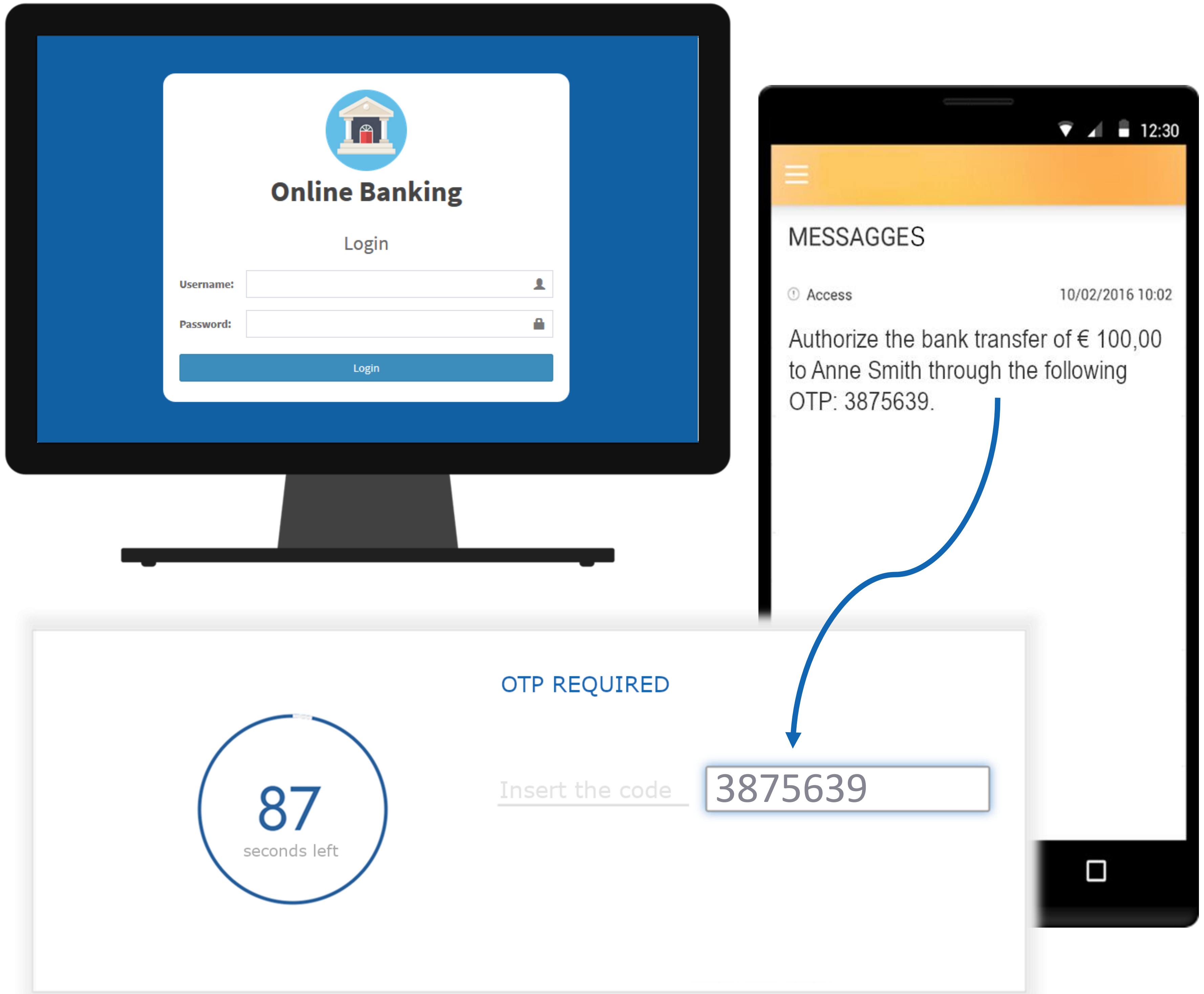
Use Case – After PSD2
2nd Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation and containing an OTP code.



Use Case – After PSD2
2nd Bank

1. The user authenticates on the online banking and performs an operation.
2. The user receives a *push notification* detailing the ongoing operation and containing an OTP code.
3. The user inserts the OTP code in the online page to authorize the operation.



FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Silvio Ranise
«*MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols*», ETAA@ESORICS 2019

Use Case Analysis – After PSD2
1st and 2nd Bank

MuFASA

0 single attackers

Advantages:

Security:

Dynamic Linking

- the user is aware of the ongoing operation
- the authentication code is connected with the ongoing operation and session, therefore it cannot be used anywhere nor for any other operation
- *only for 1st bank*: the authentication code is sent directly through the network, without requiring the user to manually enter it → attackers that intercept the code while the user is typing are mitigated

Usability: common devices are leveraged (smartphone)

Use Case

Compliance with the PSD2

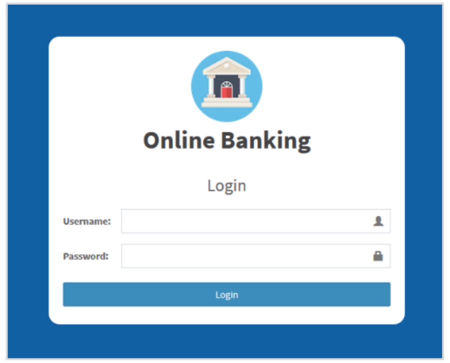
Requirement	Before PSD2		After PSD2	
	Bank 1	Bank 2	Bank 1	Bank 2
Strong Customer Authentication	✔ Factors: credentials (K) matrix card (P)	✔ Factors: credentials (K) OTP generator (P)	✔ Factors: credentials, PIN (K) smartphone (P)	✔ Factors: credentials (K) smartphone (P)
Dynamic Linking (link between authentication code and operation)	✘ Matrix contains fixed codes	✘ OTP generator generates time-based OTPs	✔ Authentication code is bound to the operation	✔ Authentication code is bound to the operation
Dynamic Linking (information on the operation displayed to the user)	✘ Matrix cannot display any information	✘ OTP generator cannot display any other information	✔ Details are displayed in the notification	✔ Details are displayed in the notification
	4 single attackers		*0 single attackers*	

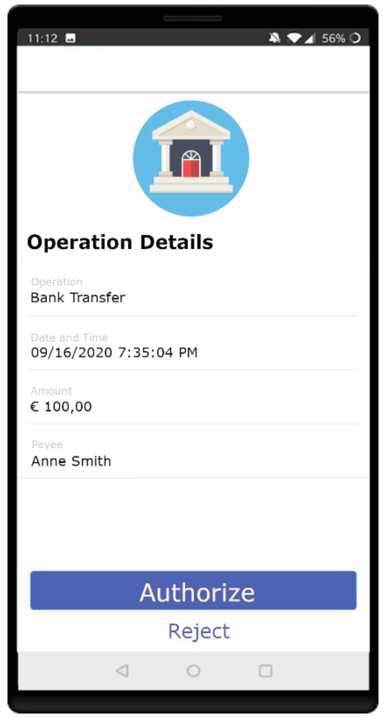
FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

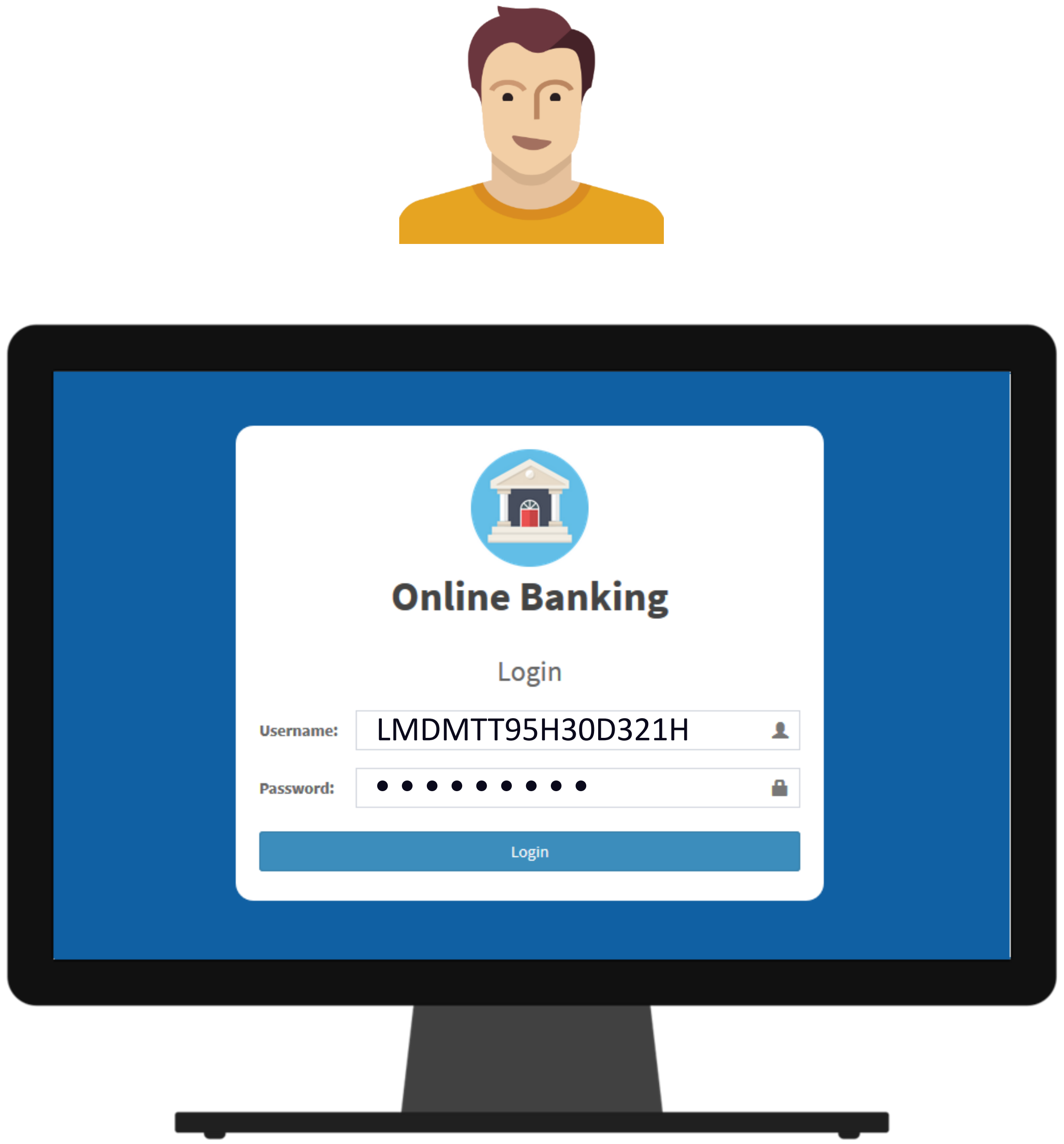
FINSEC

Advanced Vulnerabilities
Man in the Browser (Login)

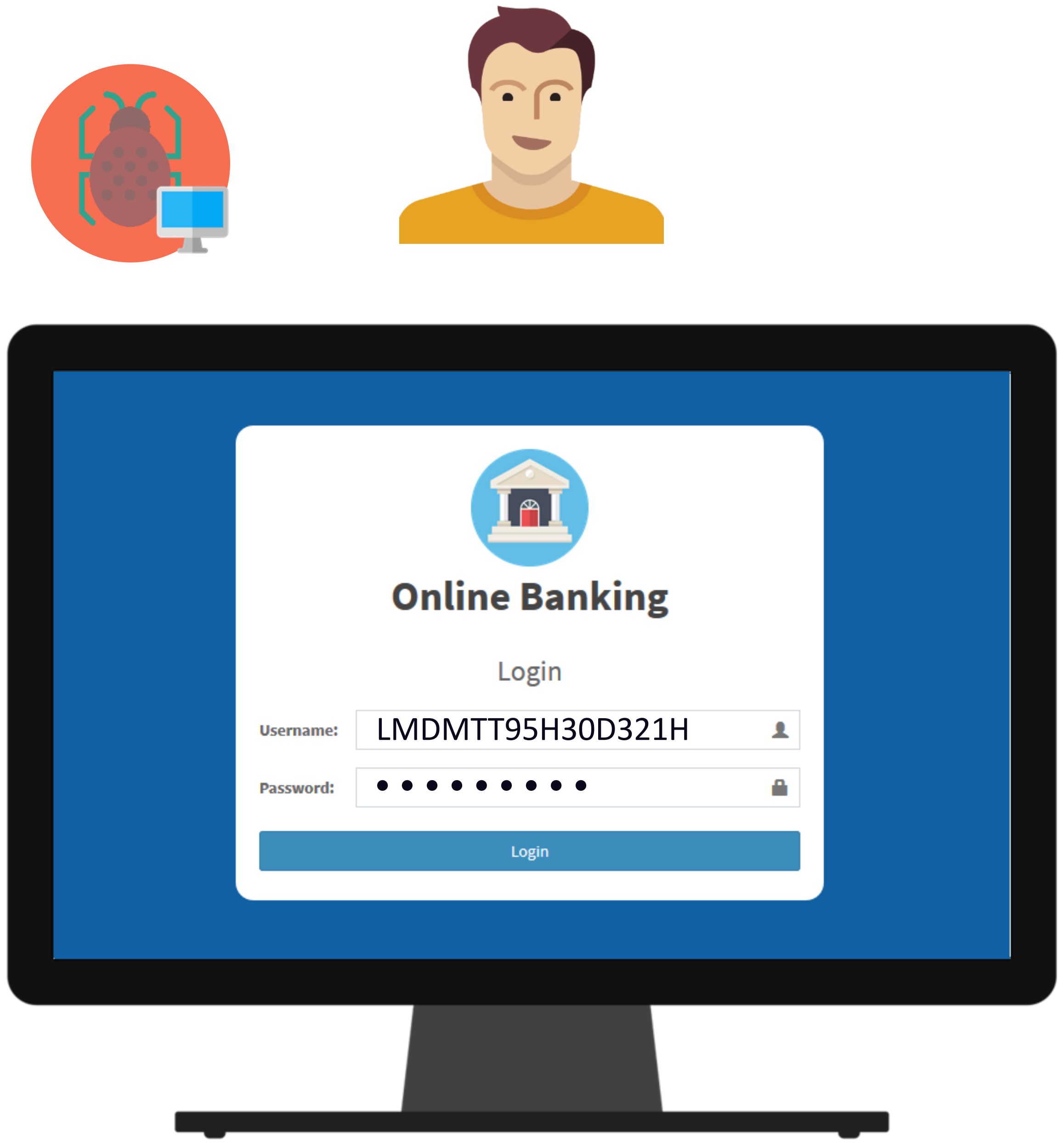




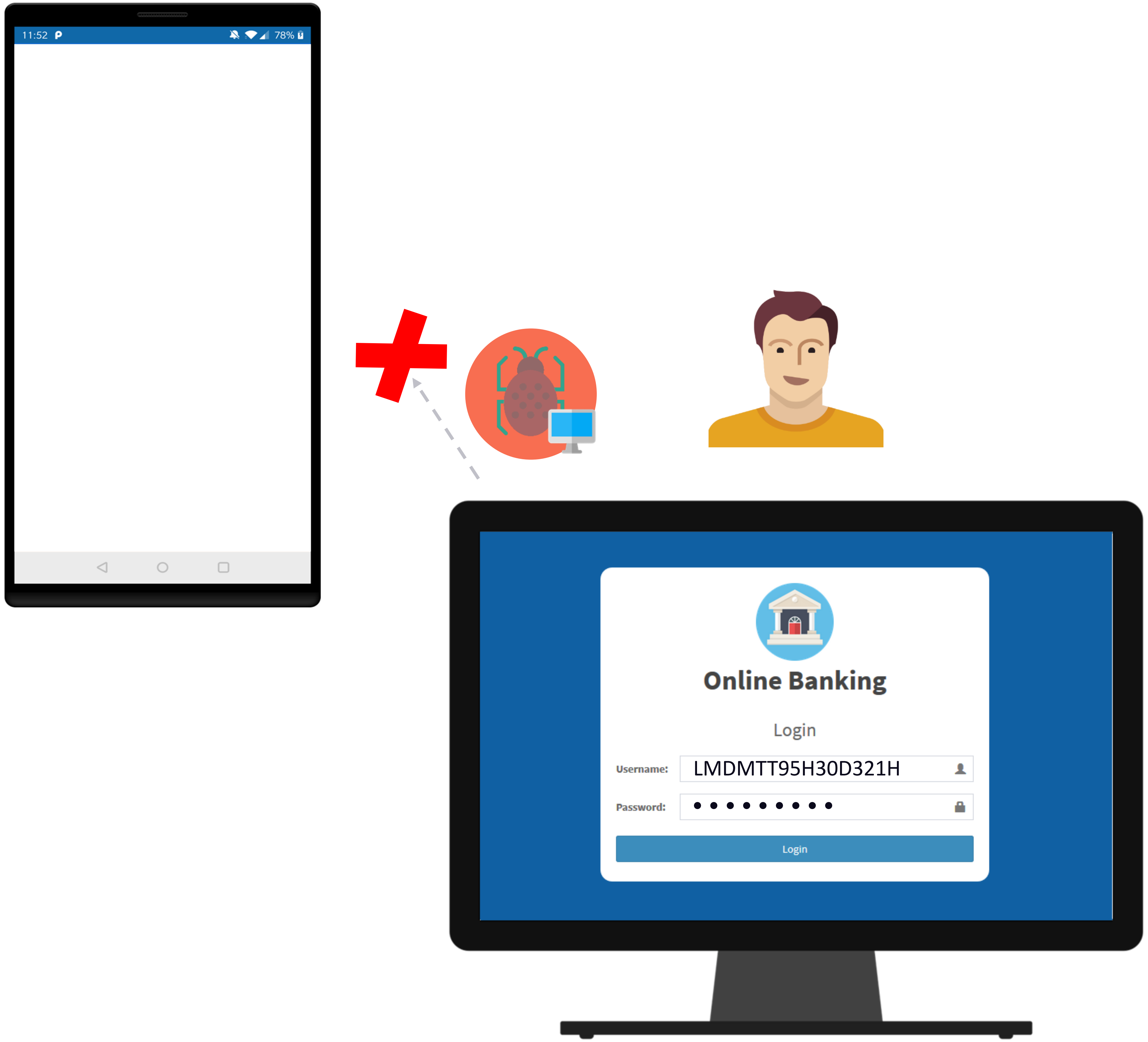
Advanced Vulnerabilities
Man in the Browser (Login)



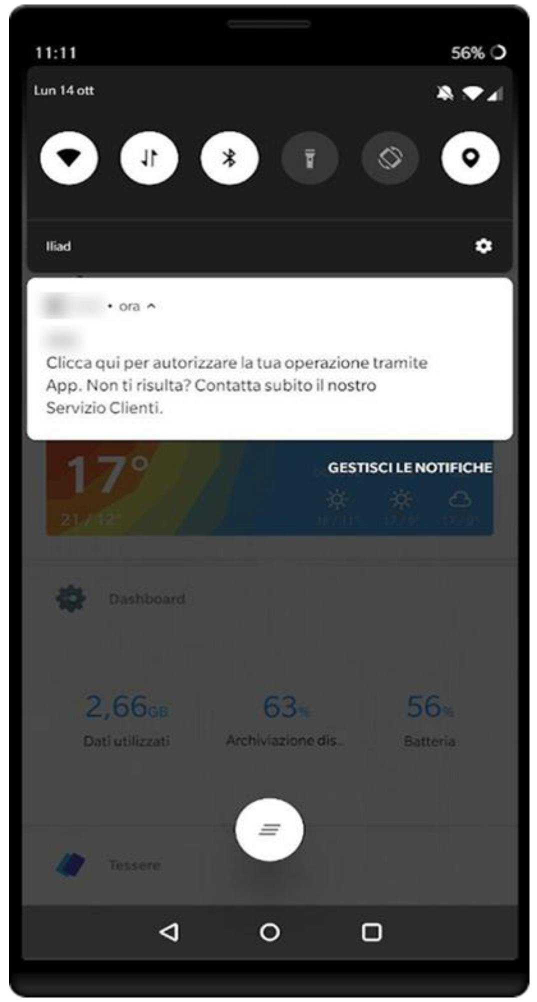
Advanced Vulnerabilities
Man in the Browser (Login)



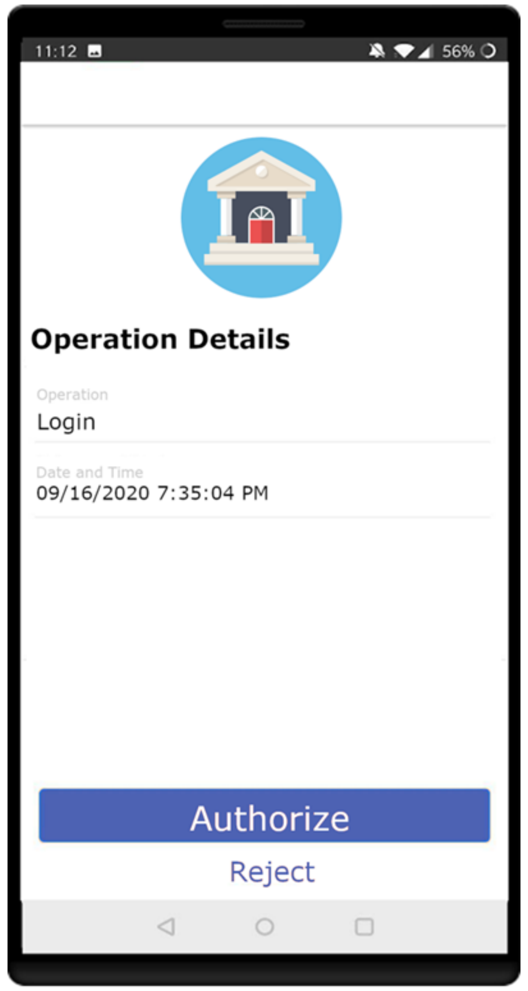
Advanced Vulnerabilities
Man in the Browser (Login)

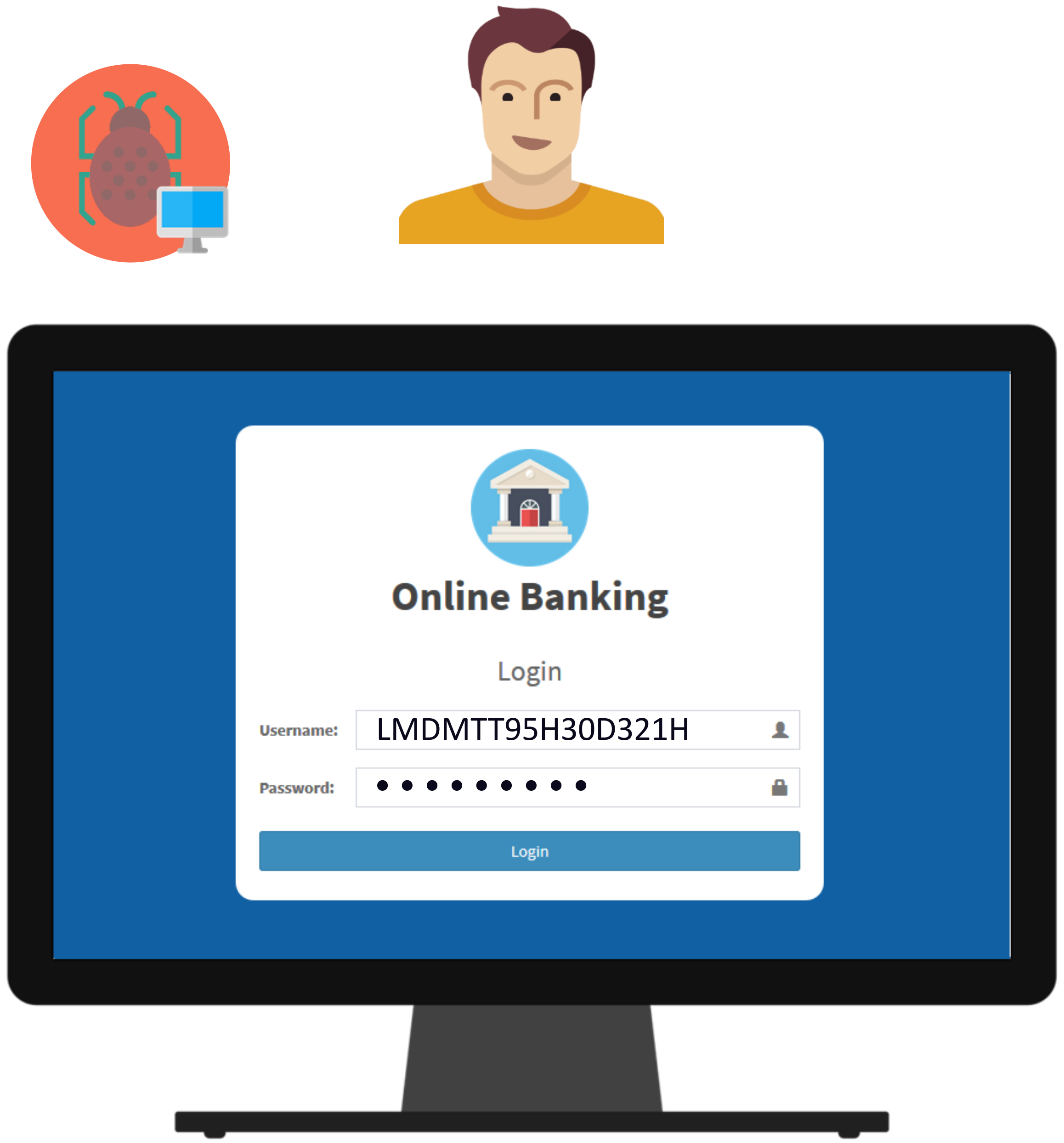


Advanced Vulnerabilities
Man in the Browser (Login)

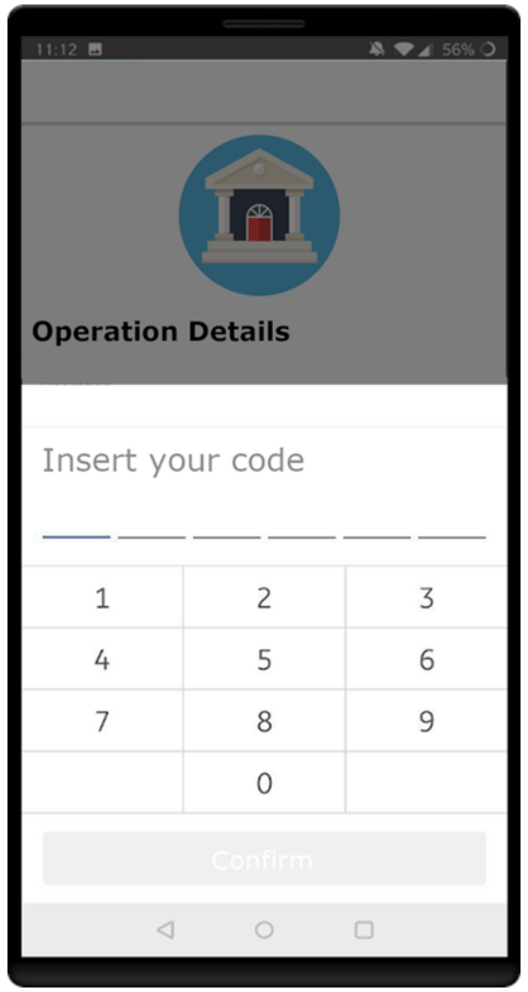


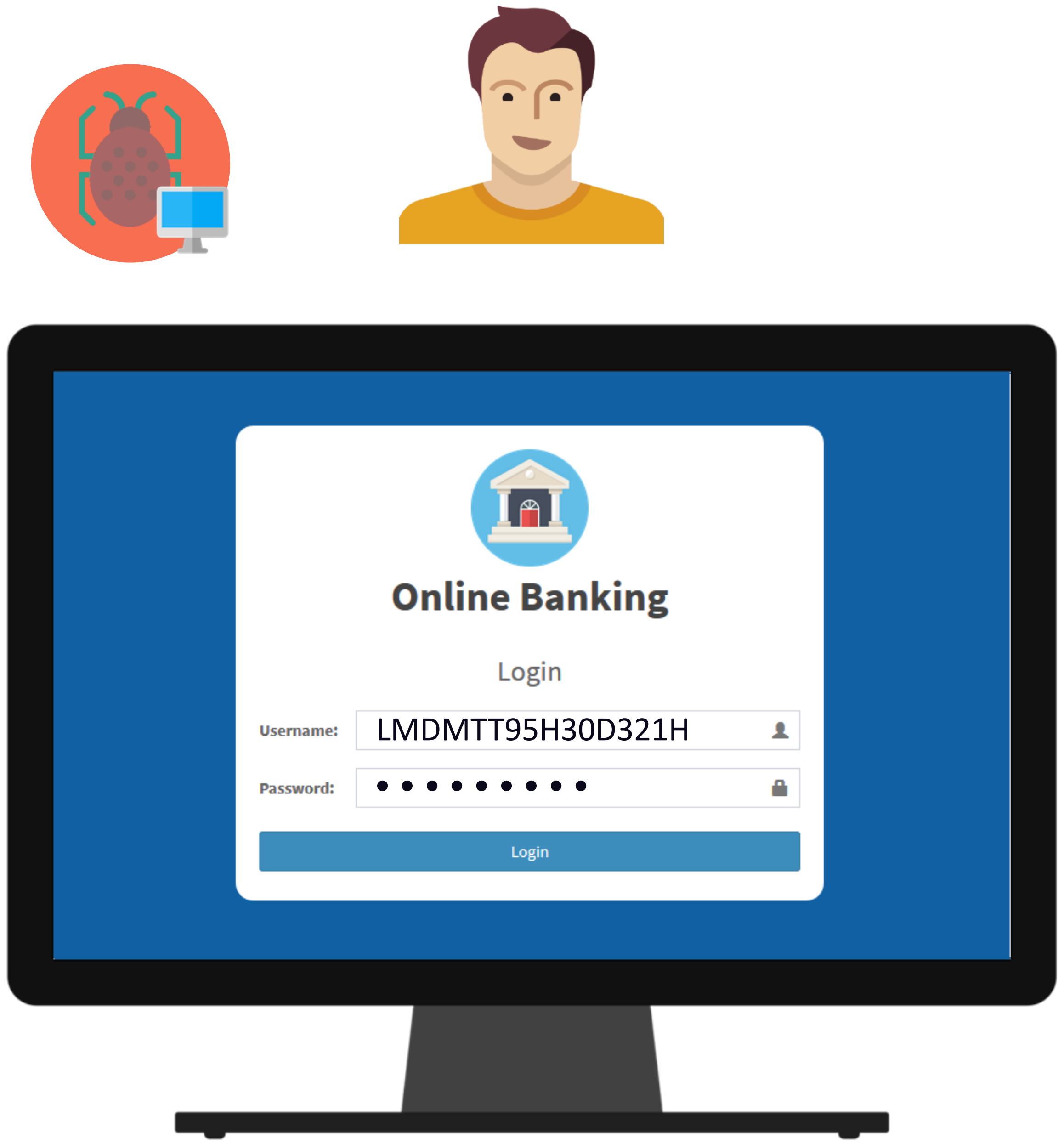
Advanced Vulnerabilities
Man in the Browser (Login)



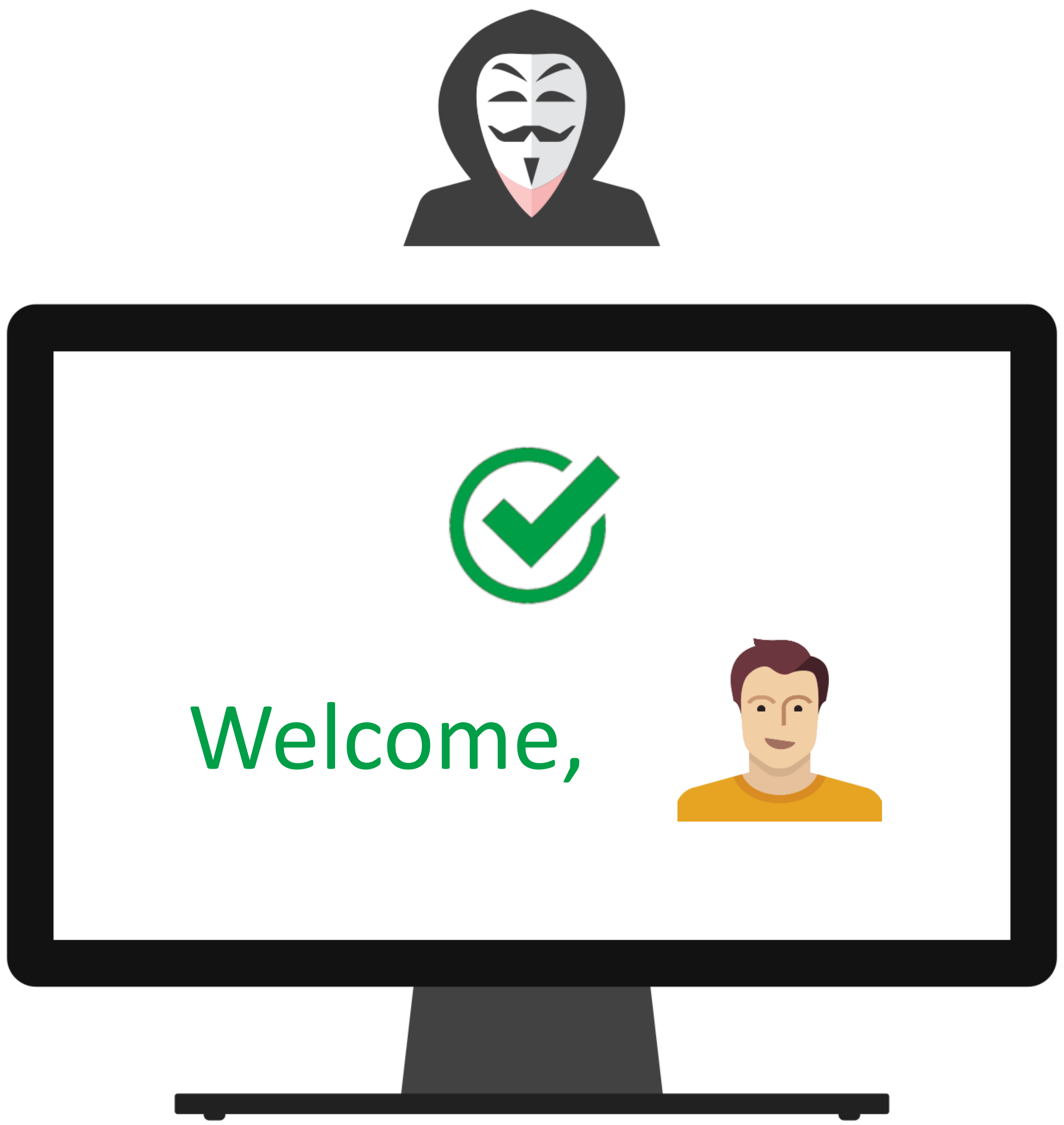


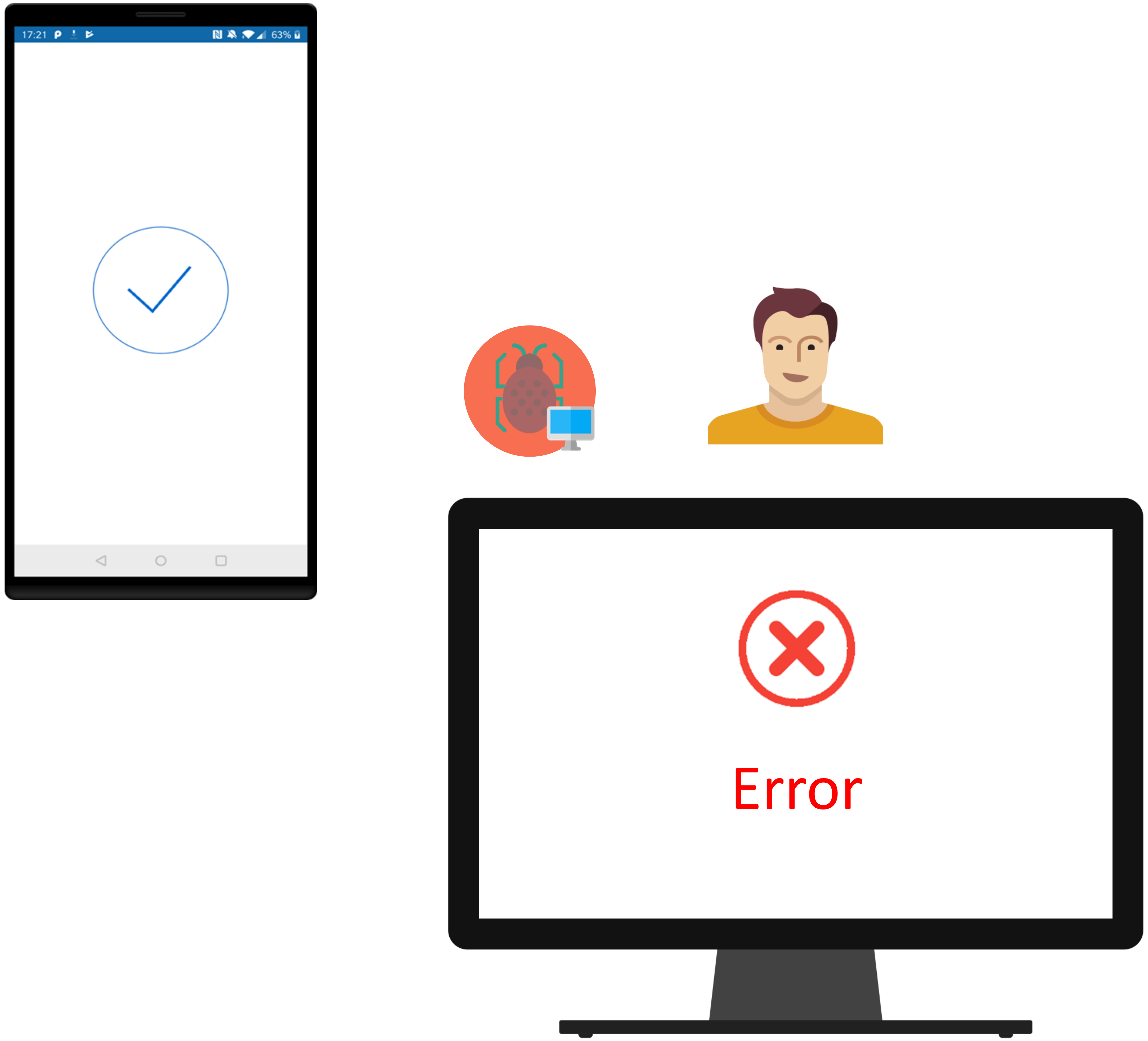
Advanced Vulnerabilities
Man in the Browser (Login)



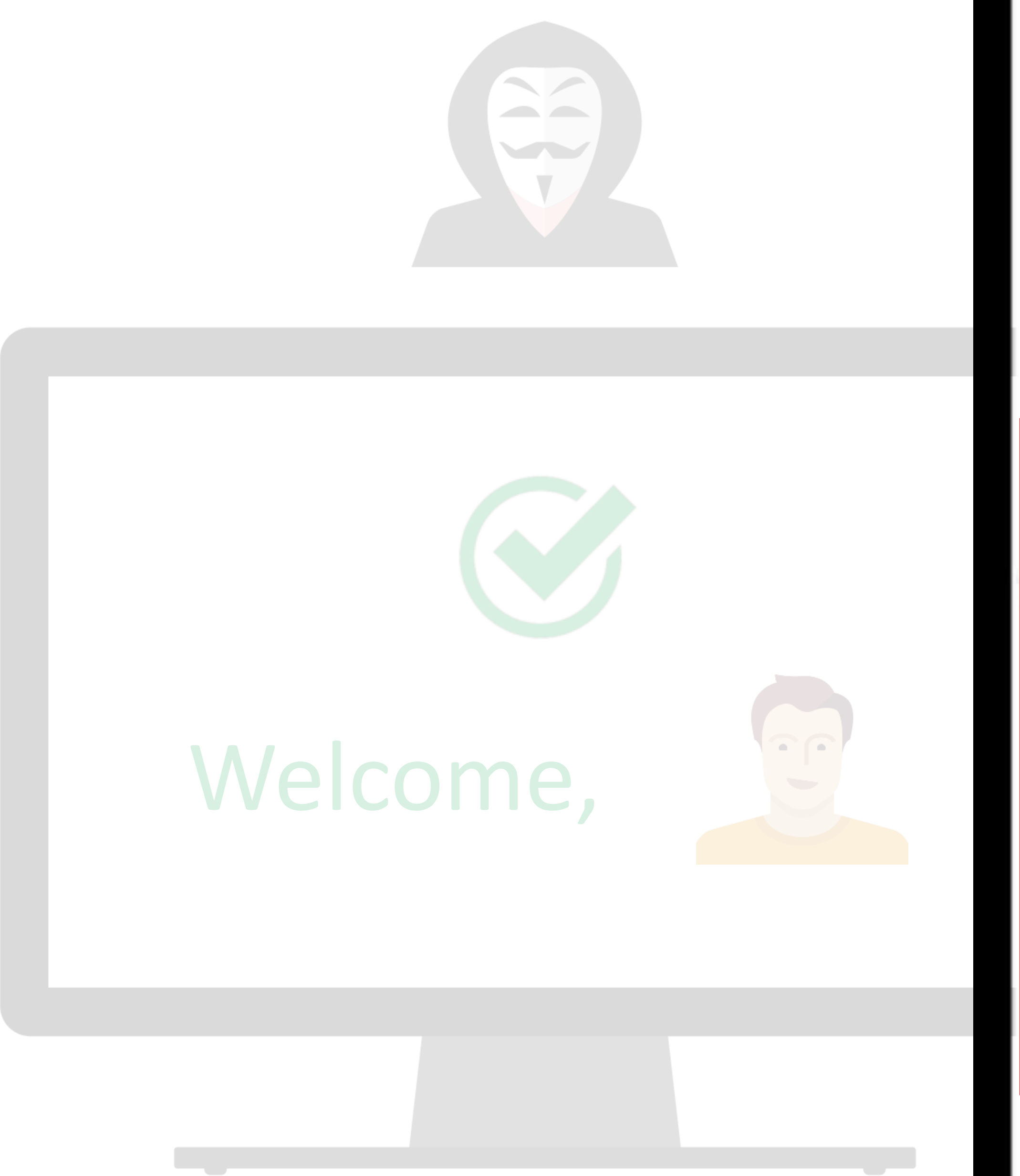


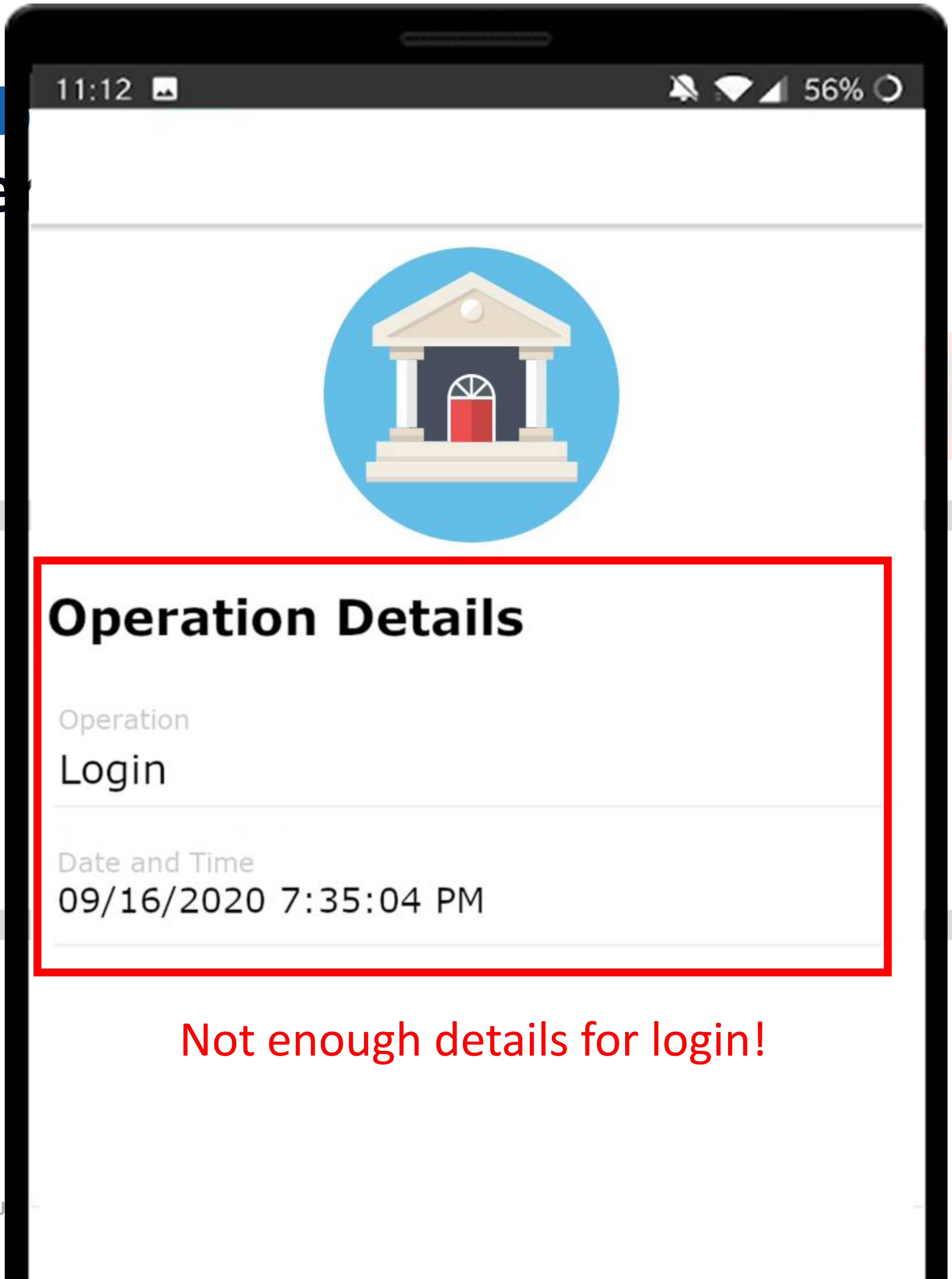
Advanced Vulnerabilities
Man in the Browser (Login)

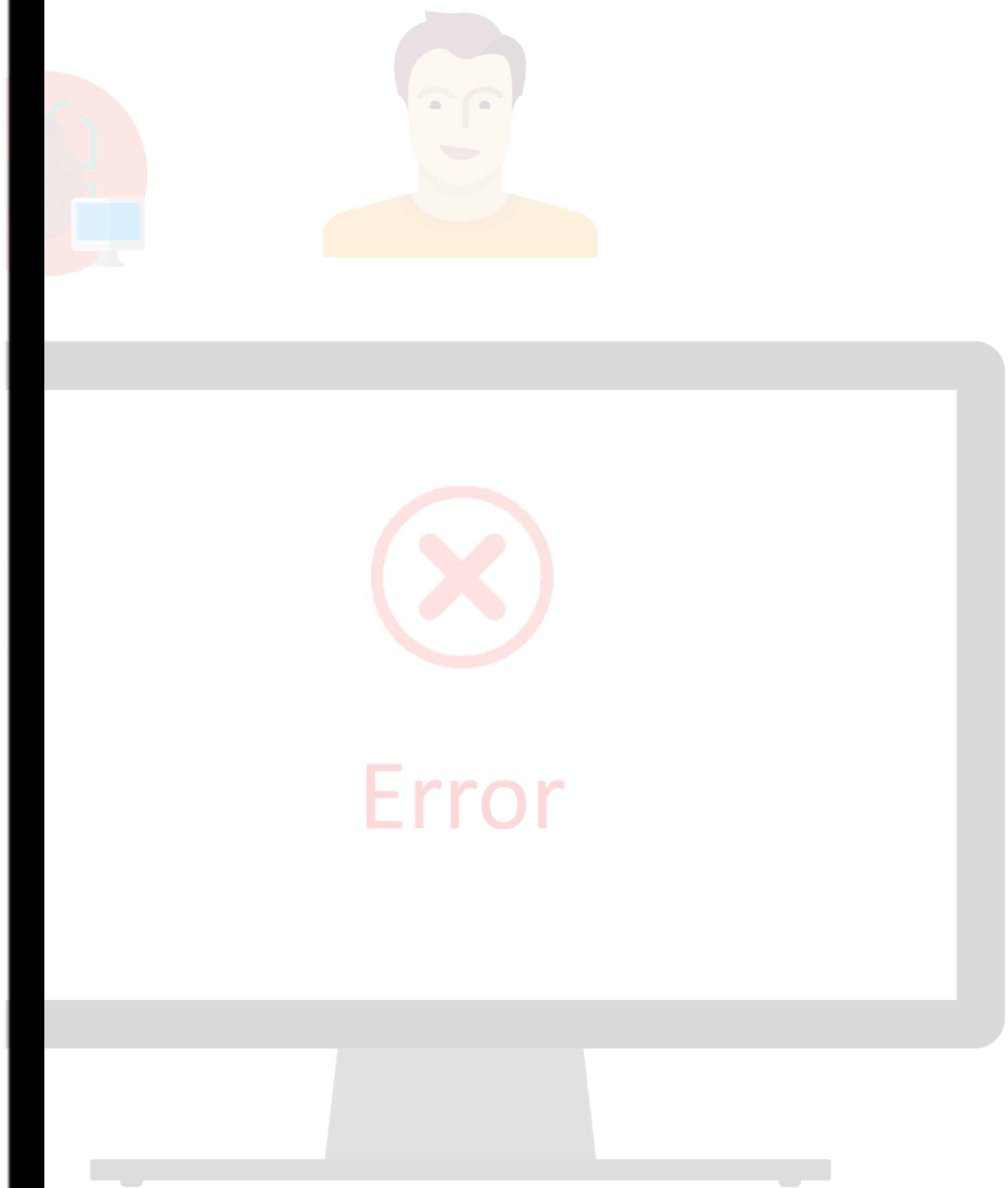




Advanced Vulneral
Man in the Browse

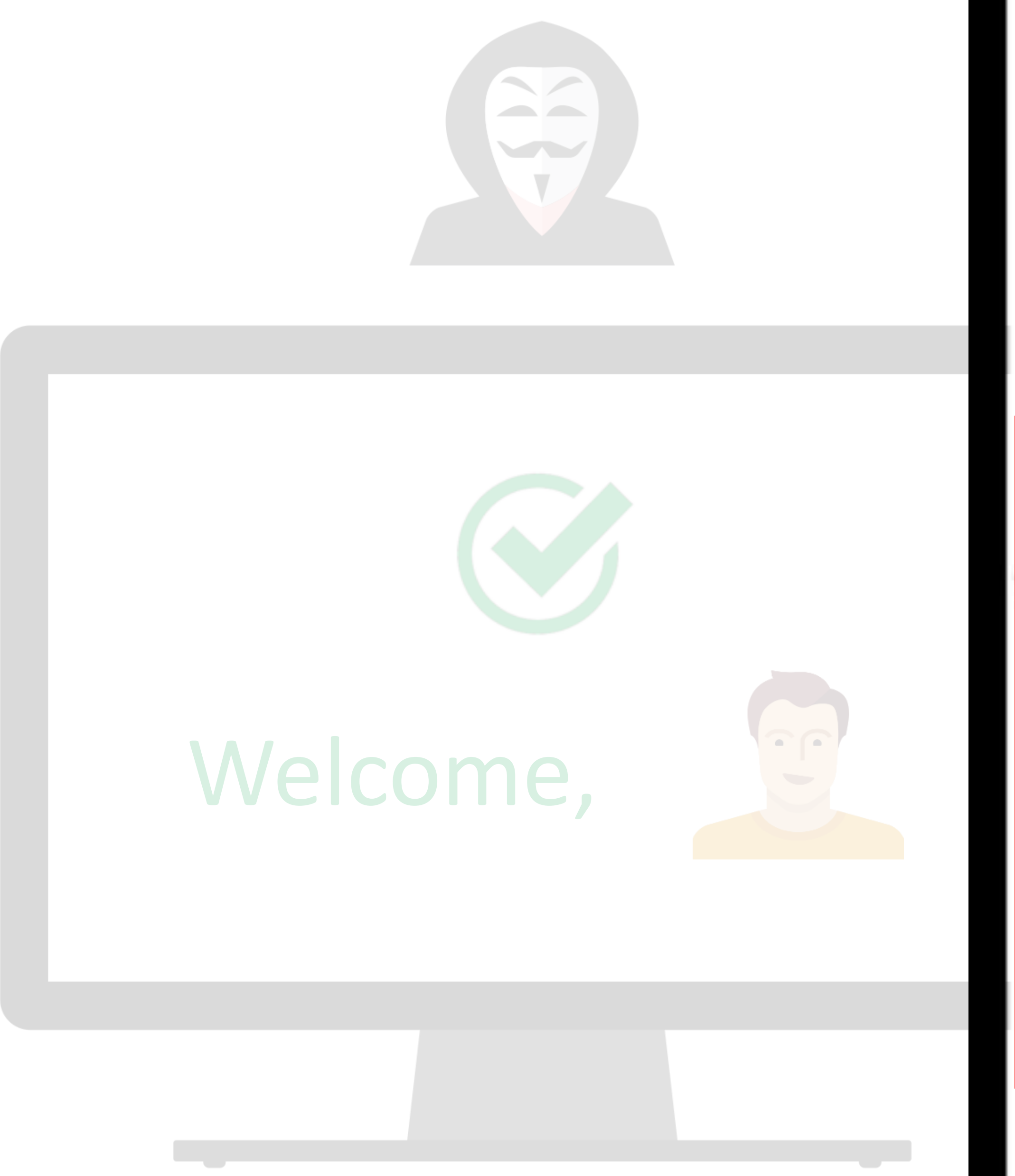


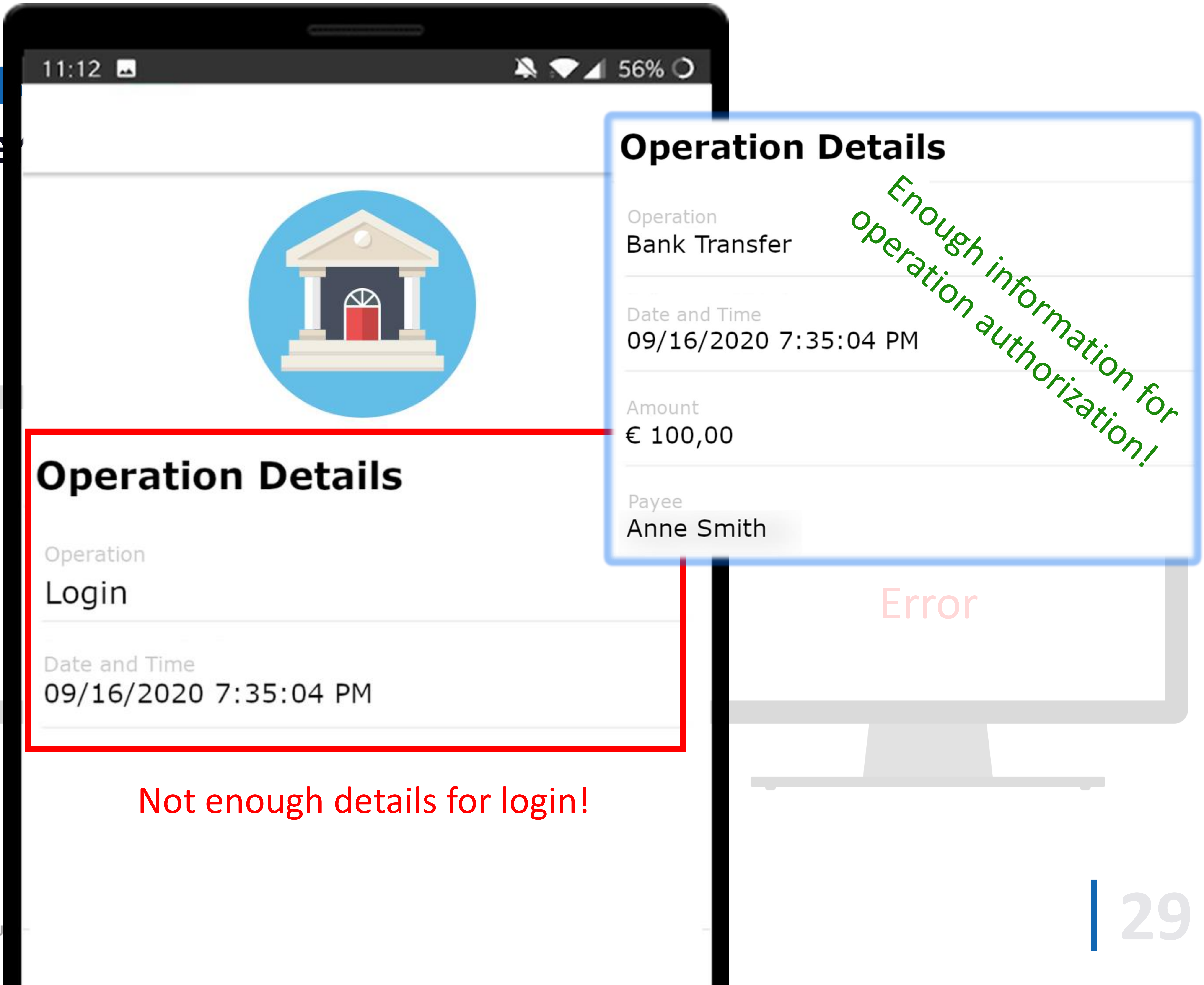




Not enough details for login!

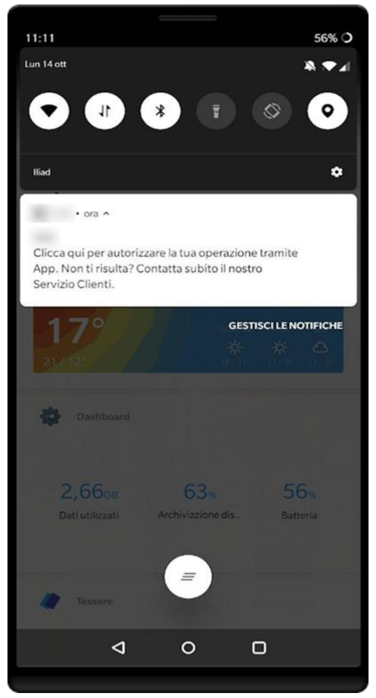
Advanced Vulneral
Man in the Browse





Advanced Vulnerabilities
Total-mobile

The use of mobile (web) applications to perform operations lead to some further considerations to be done.



Credentials are typed on the mobile device (app or browser).

The push notification is sent to *the same* mobile device.

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC

Agenda

- Overview of security vulnerabilities affecting the financial scenario
- Impacts of the PSD2 on financial protocols
- **Best practices to reduce the risks online**

Best Practices

Our actions have such an important role in cyber security.

80%

of *hacking-related data breaches* is caused by compromised credentials

>85%

of *social-related data breaches* is caused by *phishing*

Source: 2019 Data Breach Investigations Report, Verizon.

Image source: https://travelskills.com/2017/09/21/5-ways-to-prevent-shoulder-surfing/

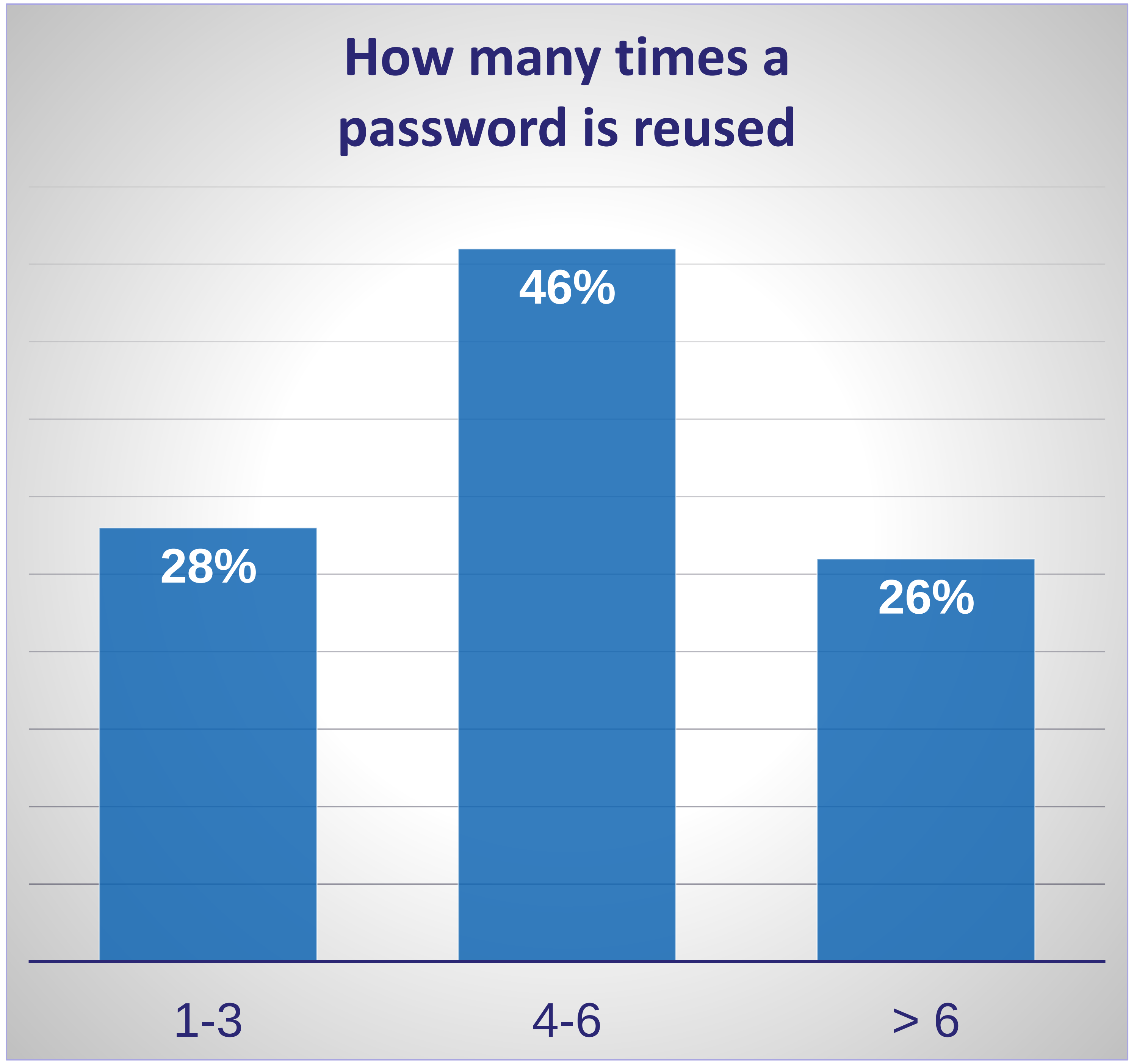
Best Practices
Passwords

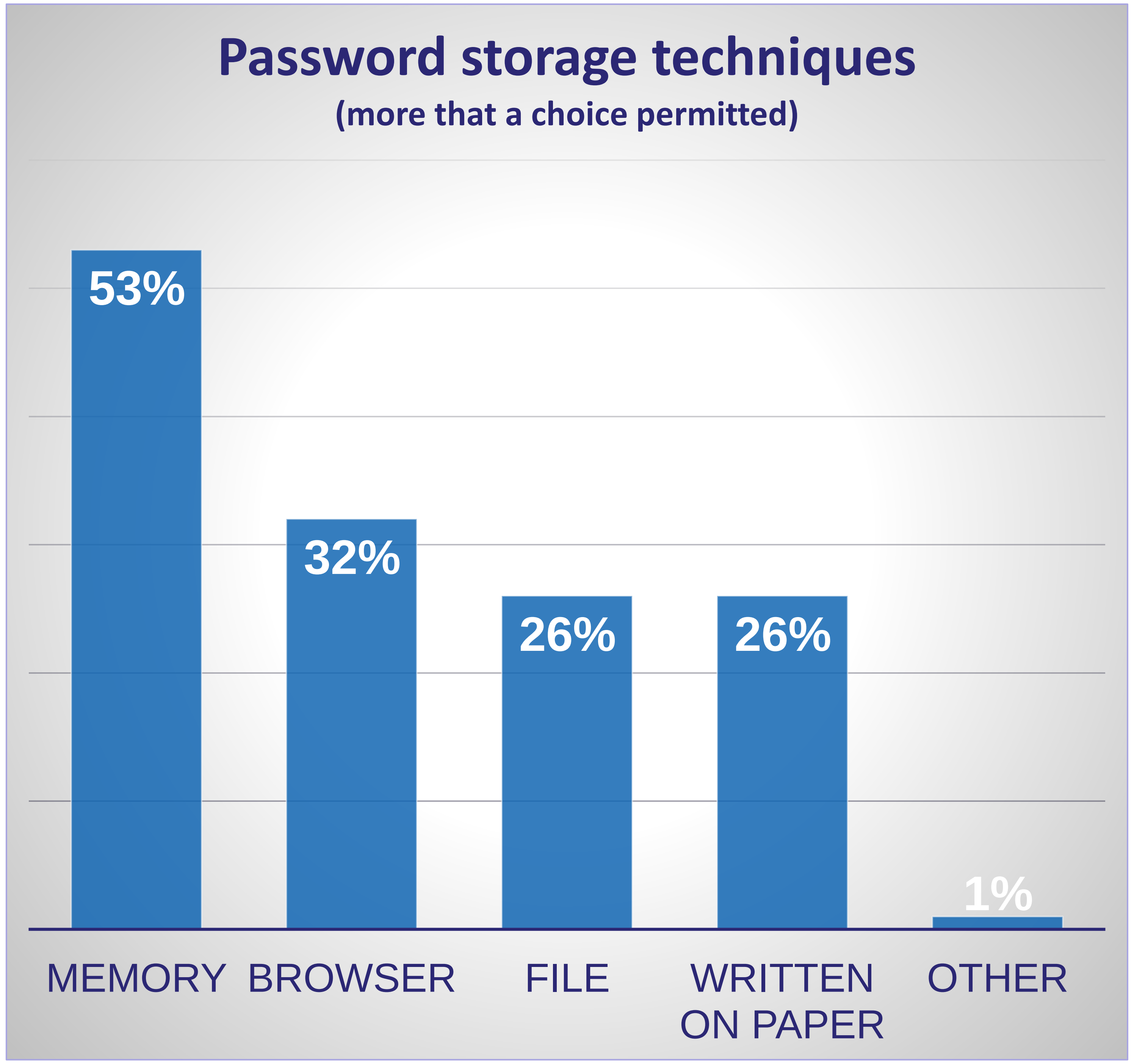
Properly choose and securely store passwords, change them frequently and avoid using the same ones for every account.

Keep attention when performing operations in public spaces, especially when inserting passwords, PINs or OTPs.

Source: The 2019 State of Password and Authentication Security Behaviors Report, Ponemon Institute

Best Practices
Passwords

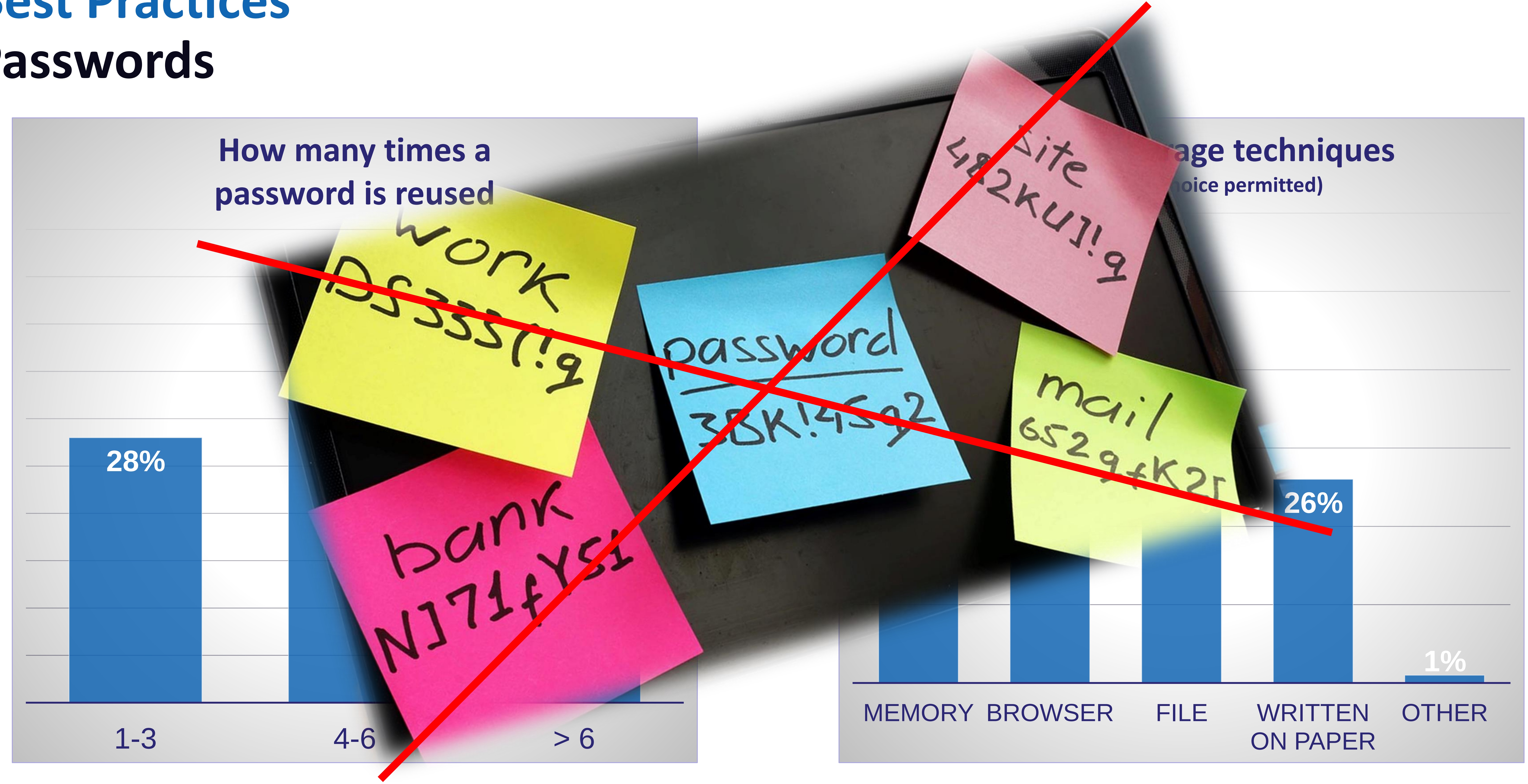




FONDAZIONE BRUNO KESSLER
ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Source: The 2019 State of Password and Authentication Security Behaviors Report, Ponemon Institute

Best Practices
Passwords



FONDAZIONE BRUNO KESSLER
ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Best Practices
Devices

Download app only from official stores.

Avoid rooting or jailbraking your devices.

Update applications, operating system and antimalware.

Best Practices
Connections

Ensure that the connection is secure while performing sensitive operations (banking transactions, authentications, etc.)

Avoid, if possible, performing sensitive operations when connected to public WiFi networks.

Best Practices
Phishing

Fake invoices for phony grants target PayPal customers

Phishing emails promise Belgians a €250 Covid-19 premium

Tuesday, 18 August 2020

Swiss state-owned companies targeted by phishing scams

phish in the sea

During the pandemic a digital crimewave has flooded the internet

The rush to remote working has outpaced cyber-security

Outlook "mail issues" phishing – don't fall for this scam!

Phishers Are Posing as Contract Partners to Access Company Data

Fraudsters take aim at active directory passwords

Organizations facing nearly 1,200 phishing attacks each month

Best Practices
Phishing

Congratulations	**Congratulations - You Have (1) New Sams Club Reward Ready To Claim!:** - Sams Club Has A Bi...	**19 apr**
|USPS|'s Survey	**Congratulations , a surprise is waiting for you**	**18 apr**
Congratulations	**Congratulations - You Have (1) New Walgreens Reward Ready To Claim!:** - Walgreens Has A Bi...	**16 apr**
CBD Today	**Is this CBD gummies really the new miracle cure?** - CAN THESE GUMMY BEARS REALLY STOP ...	**15 apr**
PRIVATESPORTSHOP	**Il primo sito di vendite evento dedicato allo sport: sconti fino all'80% tutto l'anno!** - Consegna a...	**12 apr**
Date Cute Russian	**Lonely Russian Girls Looking for Boyfriends**	**11 apr**
	(nessun oggetto) - Marco https://clck.ru/Mt3uQ	**11 apr**
ActionAid	**Un bambino ha bisogno di te** - Mostra le immagini di questo messaggio Se ritieni questa mail i...	**11 apr**
Streaming fantasy	**Disney + Pixar + Marvel + StarWars + National Geographic + I Simpsons per 6,99 al mese.** - Dis...	**10 apr**
Prima Assicurazioni	**Polizza Auto Annuale da 178,06 euro** - Mostra le immagini di questo messaggio Se ritieni ques...	**10 apr**
Pandemic Survival	**Corona Is Spinning Out of Control...** - Your Gov. Is Lying To You...10.Corona is not "controllable"...	**9 apr**

Best Practices
Phishing

Congratulations	**Congratulations - You Have (1) New Sams Club Reward Ready To Claim!:** - Sams Club Has A B...	
|USPS|'s Survey	**Congratulations , a surprise is waiting for you**	18 apr
Congratulations	**Congratulations - You Have (1) New Walgreens Reward Ready To Claim!:** - Walgreens Has A Bi...	16 apr
CBD Today	**Is this CBD gummies really the new miracle cure?** - CAN THESE GUMMY BEARS REALLY STOP ...	15 apr
PRIVATESPORTSHOP	**Il primo sito di vendite evento dedicato allo sport: sconti fino all'80% tutto l'anno!** - Consegna a...	12 apr
Date Cute Russian	**Lonely Russian Girls Looking for Boyfriends**	11 apr
	(nessun oggetto) - Marco https://clck.ru/Mt3uQ	11 apr
ActionAid	**Un bambino ha bisogno di te** - Mostra le immagini di questo messaggio Se ritieni questa mail i...	11 apr
Streaming fantasy	**Disney + Pixar + Marvel + StarWars + National Geographic + I Simpsons per 6,99 al mese.** - Dis...	10 apr
Prima Assicurazioni	**Polizza Auto Annuale da 178,06 euro** - Mostra le immagini di questo messaggio Se ritieni ques...	10 apr
Pandemic Survival	**Corona Is Spinning Out of Control...** - Your Gov. Is Lying To You...10.Corona is not "controllable"...	9 apr

Winnings, discounts or money benefits

Best Practices
Phishing

Congratulations	**Congratulations - You Have (1) New Sams Club Reward Ready To Claim!:** - Sams Club Has A Bi...	19 apr
|USPS|'s Survey	**Congratulations , a surprise is waiting for you**	18 apr
Congratulations	**Congratulations - You Have (1) New Walgreens Reward Ready To Claim!:** - Walgreens Has A Bi...	
CBD Today	**Is this CBD gummies really the new miracle cure?** - CAN THESE GUMMY BEARS REALLY STOP ...	
PRIVATESPORTSHOP	**Il primo sito di vendite evento dedicato allo sport: sconti fino all'80% tutto l'anno!** - Consegna a...	12 apr
Date Cute Russian	**Lonely Russian Girls Looking for Boyfriends**	11 apr
	(nessun oggetto) - Marco https://clck.ru/Mt3uQ	11 apr
ActionAid	**Un bambino ha bisogno di te** - Mostra le immagini di questo messaggio Se ritieni questa mail i...	11 apr
Streaming fantasy	**Disney + Pixar + Marvel + StarWars + National Geographic + I Simpsons per 6,99 al mese.** - Dis...	10 apr
Prima Assicurazioni	**Polizza Auto Annuale da 178,06 euro** - Mostra le immagini di questo messaggio Se ritieni ques...	10 apr
Pandemic Survival	**Corona Is Spinning Out of Control...** - Your Gov. Is Lying To You...10.Corona is not “controllable”...	9 apr

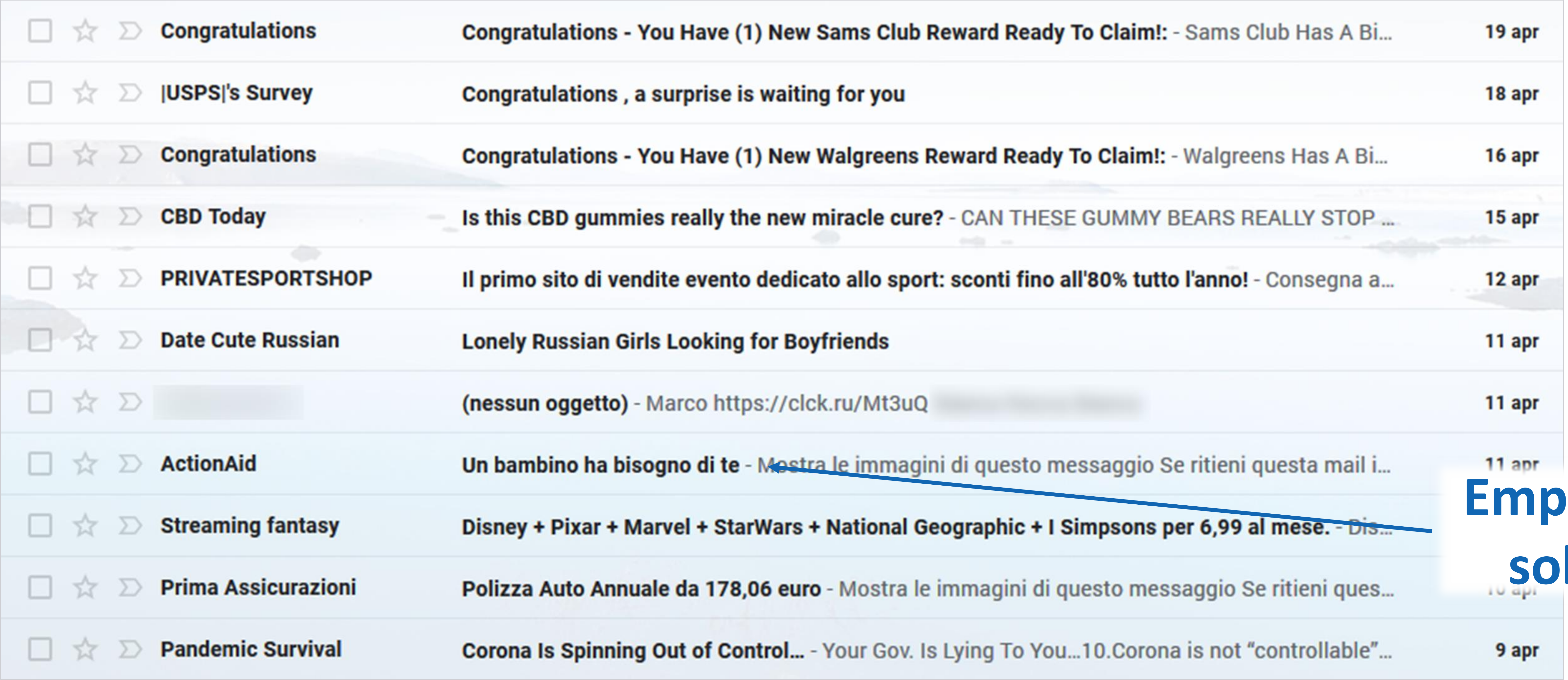
Miracolous cures

Best Practices
Phishing

Congratulations	**Congratulations - You Have (1) New Sams Club Reward Ready To Claim!:** - Sams Club Has A Bi...	19 apr
|USPS|'s Survey	**Congratulations , a surprise is waiting for you**	18 apr
Congratulations	**Congratulations - You Have (1) New Walgreens Reward Ready To Claim!:** - Walgreens Has A Bi...	16 apr
CBD Today	**Is this CBD gummies really the new miracle cure?** - CAN THESE GUMMY BEARS REALLY STOP ...	15 apr
PRIVATESPORTSHOP	**Il primo sito di vendite evento dedicato allo sport: sconti fino all'80% tutto l'anno!** - Consegna a...	12 apr
Date Cute Russian	**Lonely Russian Girls Looking for Boyfriends**	11 apr
	(nessun oggetto) - Marco https://clck.ru/Mt3uQ	11 apr
ActionAid	**Un bambino ha bisogno di te** - Mostra le immagini di questo messaggio Se ritieni questa mail i...	11 apr
Streaming fantasy	**Disney + Pixar + Marvel + StarWars + National Geographic + I Simpsons per 6,99 al mese.** - Dis...	10 apr
Prima Assicurazioni	**Polizza Auto Annuale da 178,06 euro** - Mostra le immagini di questo messaggio Se ritieni ques...	10 apr
Pandemic Survival	**Corona Is Spinning Out of Control...** - Your Gov. Is Lying To You...10.Corona is not "controllable"...	9 apr

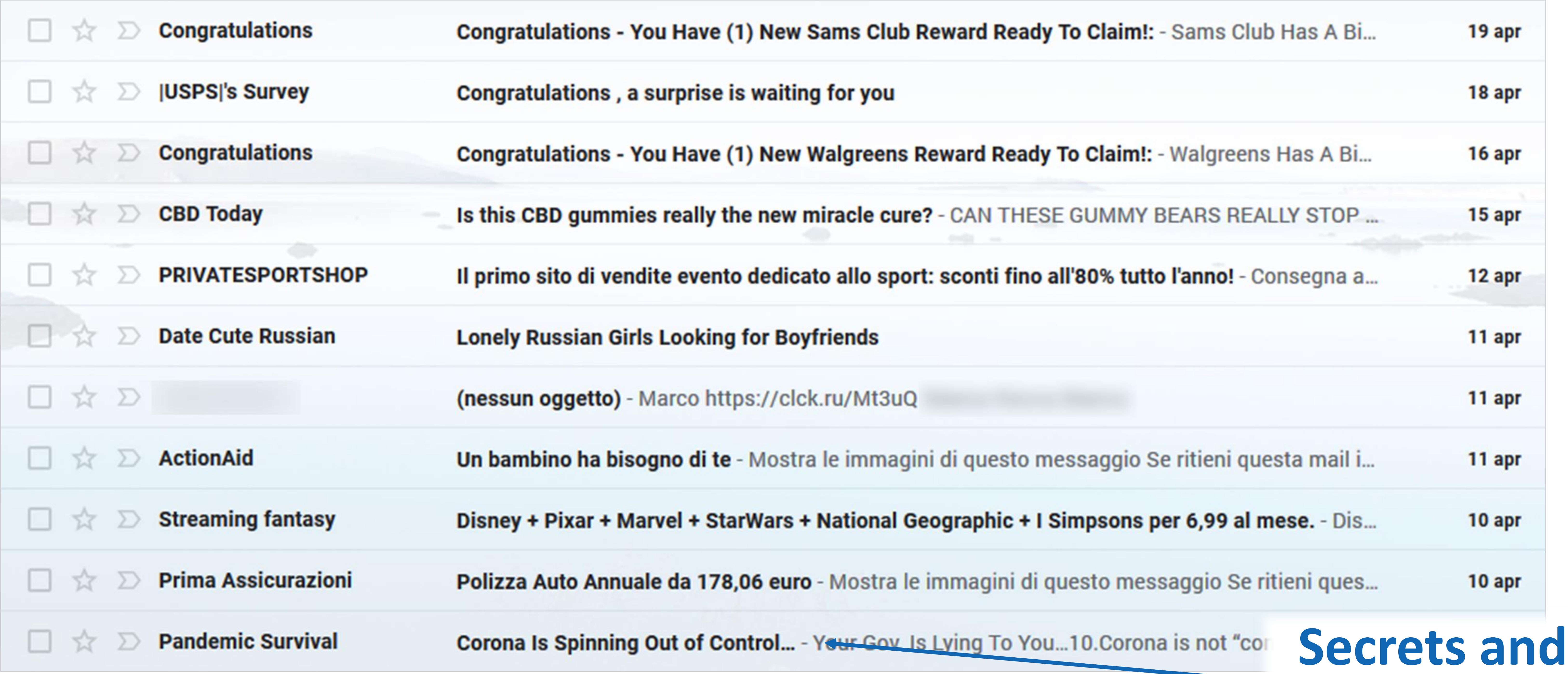
Meetings

Best Practices
Phishing



Empathy and solidarity

Best Practices
Phishing



Secrets and conspiracies

FONDAZIONE BRUNO KESSLER ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST
FINSEC

Best Practices
Phishing

- Beware of links in emails or text messages. Banking and postal institutes never ask you for personal information through these means.

- Never lower your guard in case of suspicious emails, not even if (apparently) coming from a known person.

- Pay attention to the linguistic and grammatical structure of the email: they are often translated through automatic services.

- Beware of emails requesting you to perform operations shortly: attackers often create pressure to prevent victims from paying much attention to details.

Best Practices
Phishing

Esclusiva Vodafone	**Passa a Fibra a 27,90€ al mese. 2 mesi di canone in regalo! Solo online** - Mostra le immagini di...	8 apr
Difesa e sicurezza .	**In vendita in Italia la torcia militare progettata per le forze speciali USA** - In vendita in Italia la t...	8 apr
Infinity	**Infinity supporta la raccolta fondi «Aiutiamo chi ci aiuta»** - Infinity porta avanti l'impegno socia...	7 apr
CBD Today	**Experience the benefits of clinically validated Cannabliss CBD Gummies** - CAN THESE GUMMY...	5 apr

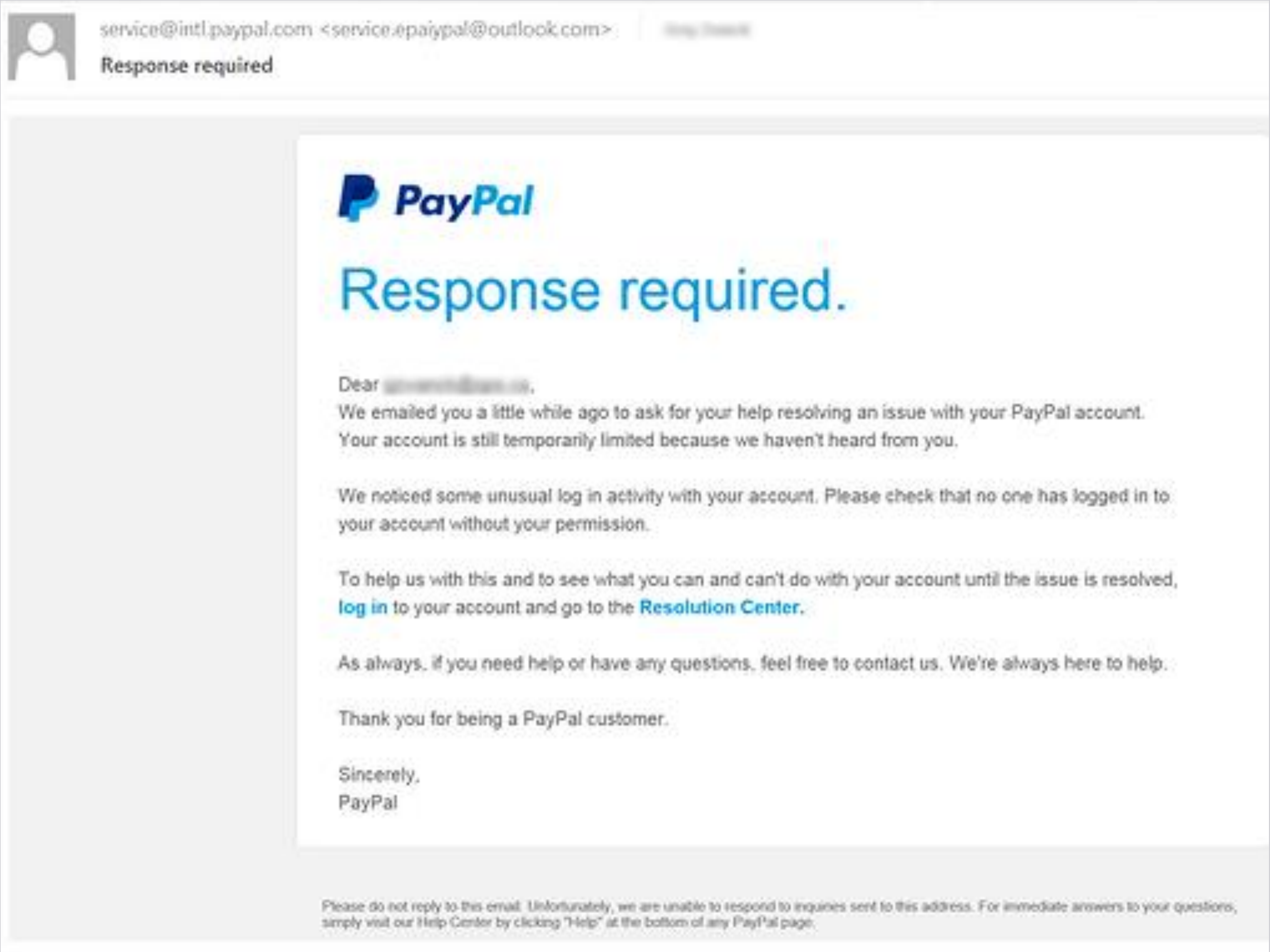
Sender apparently trusted (Italian telco)

Best Practices
Phishing

Sender apparently trusted (Italian telco)

… but only apparently!

Best Practices
Phishing


service@intl.paypal.com <service.epaiypal@outlook.com>

Response required

PayPal

Response required.

Dear ,

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

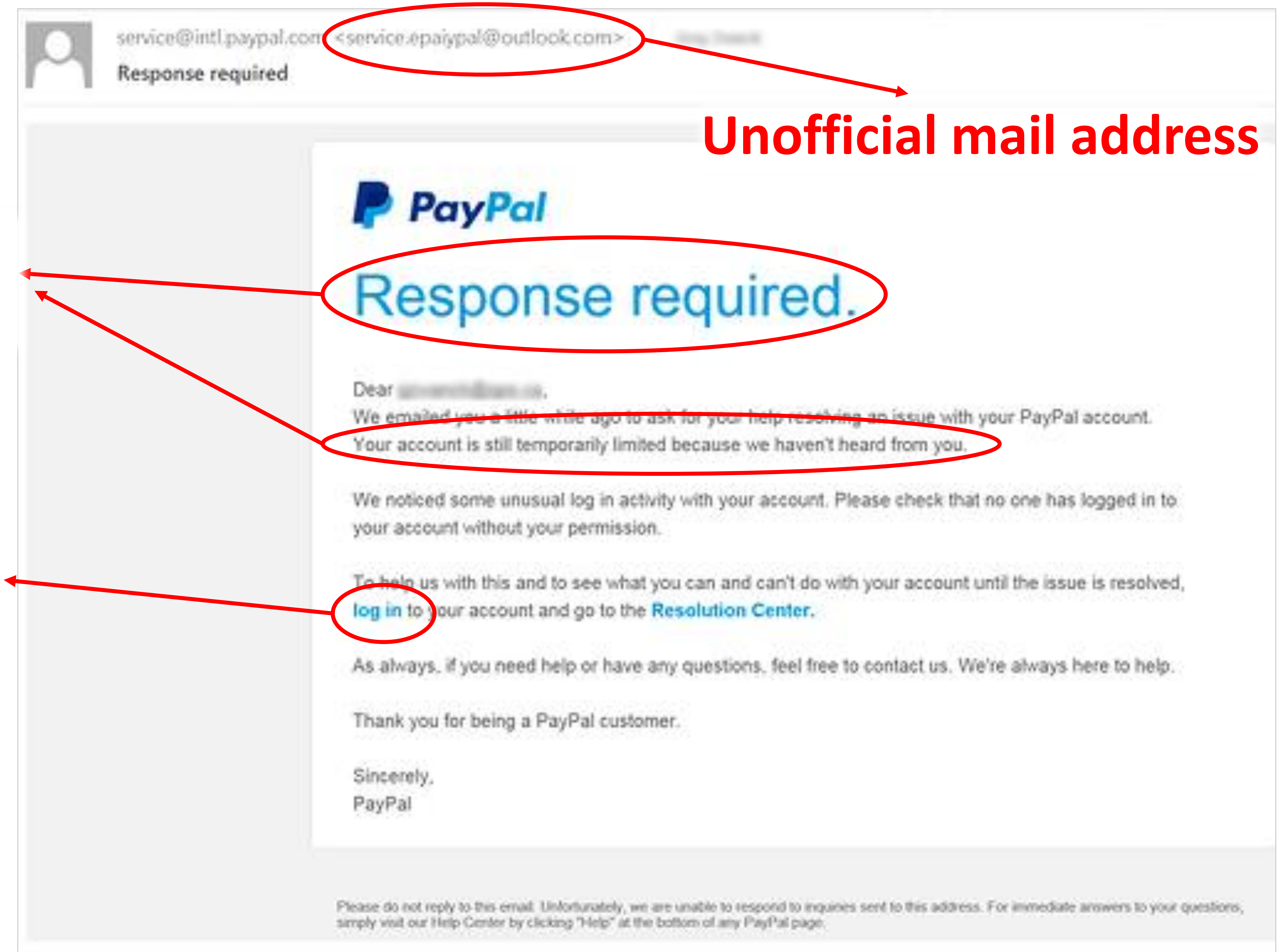
Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Best Practices
Phishing

Need for performing an operation shortly

Link not to be clicked



Thank you for the attention!

Marco Pernpruner
mpernpruner@fbk.eu

https://stfbk.github.io

Questions?

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY

ST SECURITY & TRUST

FINSEC