RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AFD-R06**

The Science of Scams: Deconstructing How Criminals Steal Cash

Erin Englund

Threat Analytics Lead, NA
BioCatch
Erin.Englund@biocatch.com

Ayelet Biger-Levin

SVP Market Strategy
BioCatch
Ayelet.levin@biocatch.com

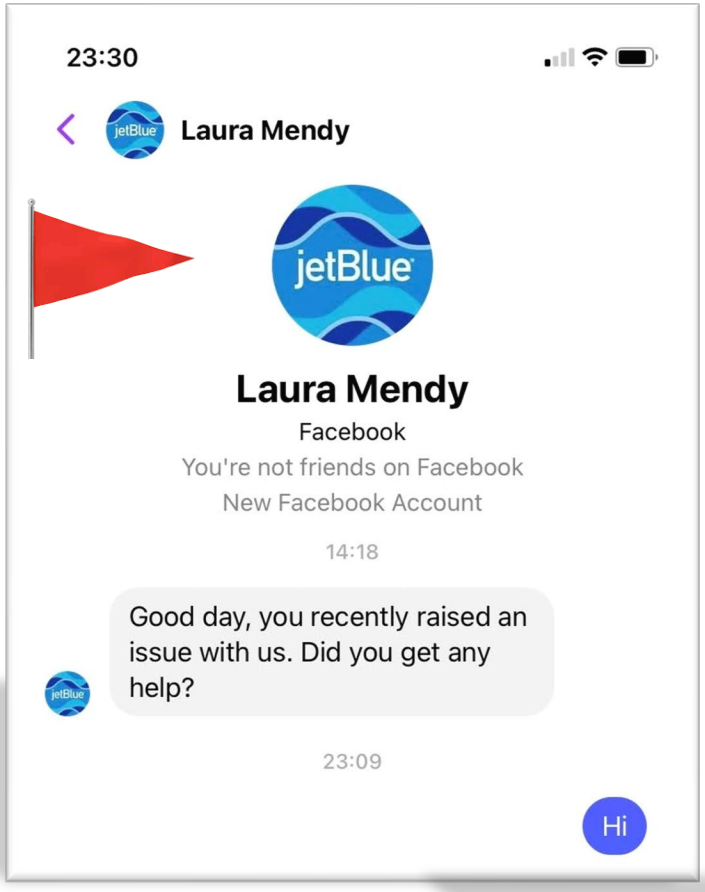
Disclaimer

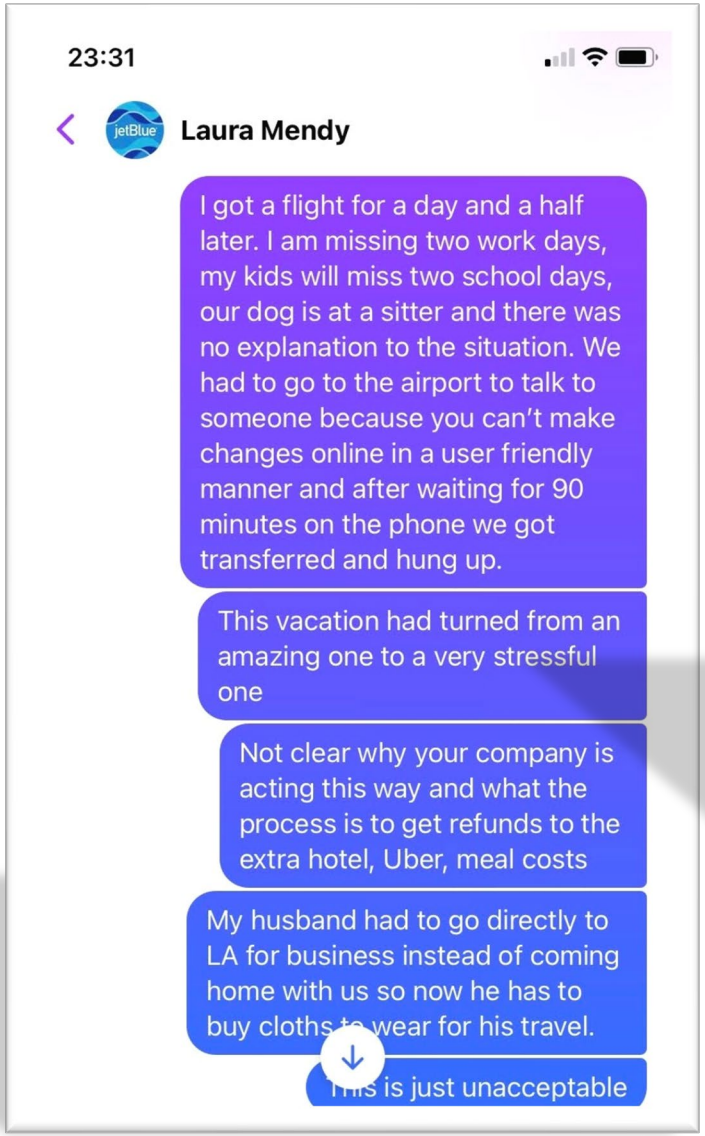
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

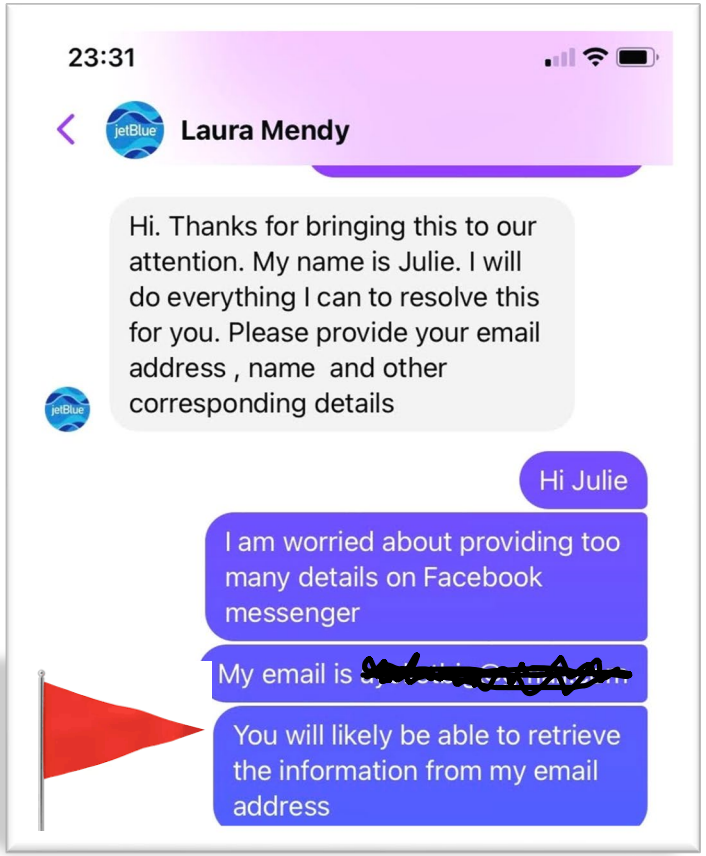
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Can it happen to you? Can it happen to me?

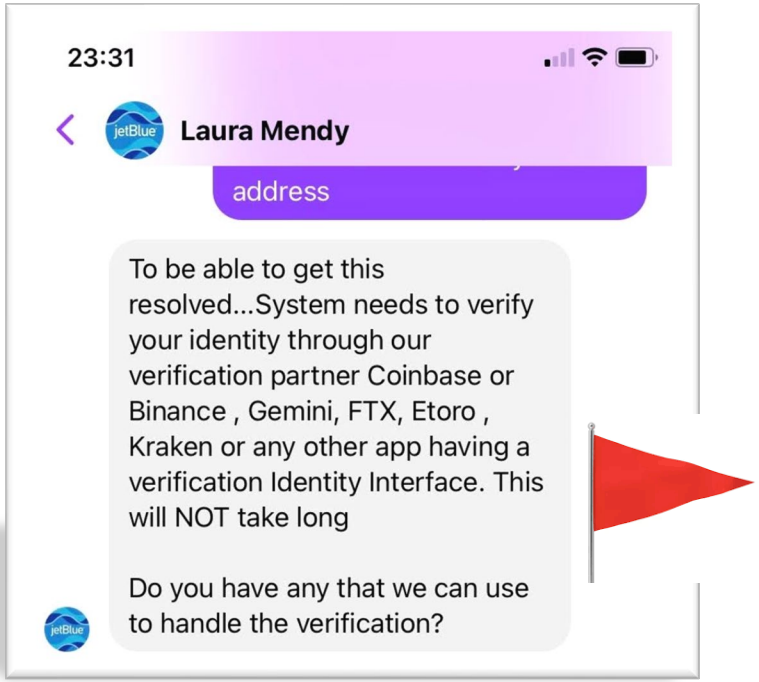
Can it happen to you? Can it happen to me?

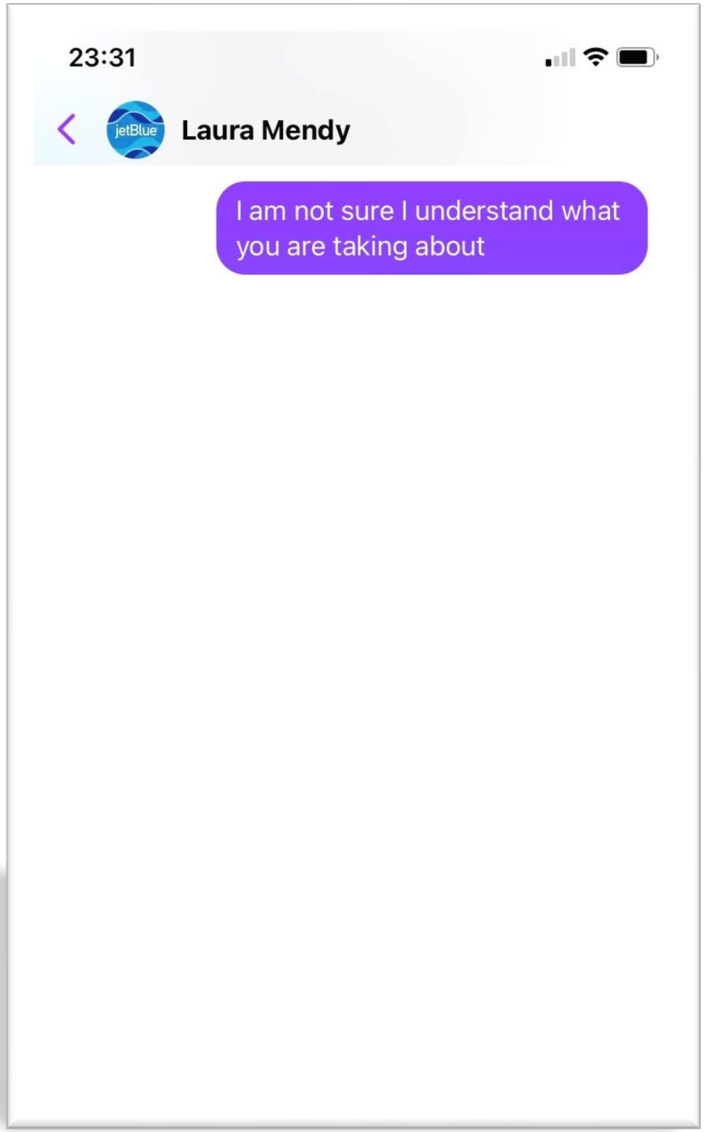






Can it happen to you? Can it happen to me?





The Cost of Social Engineering

$1.6B

Total reported crypto scam losses in 2021 over x7 more than 2020

$6.9B

Lost to online scams in the US in 2021

£355.4

Total Losses to APP Fraud, H1, 2021, Increase of 70% YoY

145%

Increase in scam calls reported by ScamWatch in 2021, Australia, total $851M

$956M

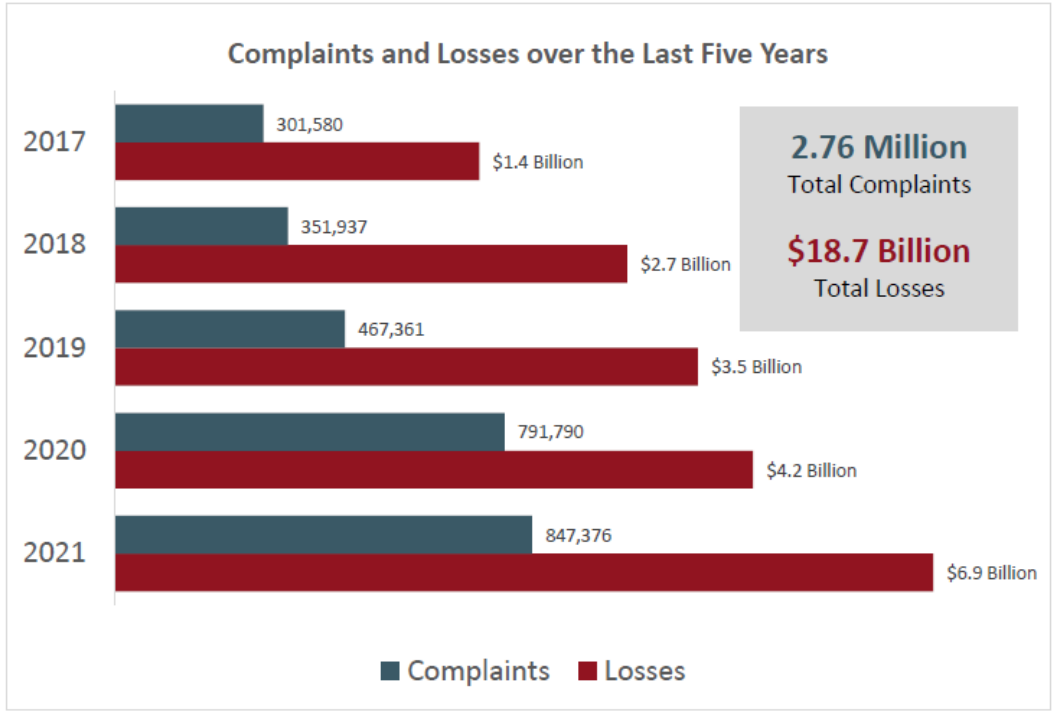
Reported losses to Confidence Fraud/Romance scams 2021 from 24,299 victims to ICC

Scams have significantly accelerated in the last two years

IC3 COMPLAINT STATISTICS

LAST 5 YEARS

Over the last five years, the IC3 has received an average of 552,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[3]



2020: A year of lockdown, move to EVERYTHING online, and scams

Source: UK Finance (2021).

Types of Social Engineering

Credential Harvesting (offline)

Phishing/Vishing/Smishing

Data harvesting by means of email, phone, or SMS. Victims are tricked into providing personal info or credentials to the scammer.

Real-Time Attacks

Malware & Remote Access Tool Attacks

Victims are tricked into installing malware of a remote access tool by way of social engineering

Authorized Push Payment Voice Scams

Victims are coerced into sending a payment directly to the fraudster. Scammers use methods to create an emotional response from the victim.

RSAConference2022

Psychology of Scams

Who Are Victims?

Criminal Scam Tactics and Triggers by Generations

AGE 11-24

TACTICS:
Social Media Requests, Chat Bots

TRIGGERS:
P2P Payment Messaging, Social Friend Requests, Mule Recruits

AGE 24-40

TACTICS:
Robocalls, Text

TRIGGERS:
Rewards, Parcel Tracking, P2P Transfer Confirmations

AGE 41-65

TACTICS:
Email, Robocalls, Text

TRIGGERS:
Financial Info, Interest Rates, Parcel Tracking

AGE 57-75

TACTICS:
Robocalls

TRIGGERS:
IRS, Health Care, Social Security

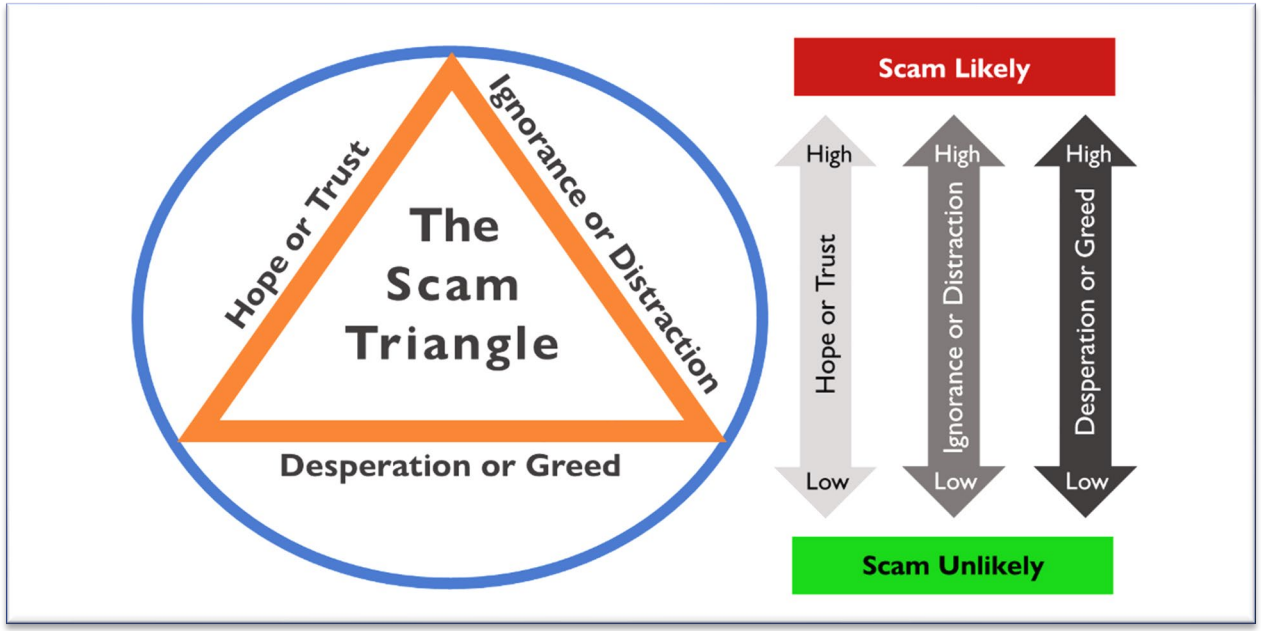
JAVELIN

"Scammers don't target one group over another, they target all people of all backgrounds, ages and income levels across Australia."

ABA CEO Anna Bligh

Why Are They Falling For It?

- Lack of Awareness
- Loneliness
- Fear
- Easy Money



Source: The Knoble, May 17, 2022

Types of Social Engineering

Unauthorized Payments

Account Takeover

- Unauthorized 3rd party is actively sending and authorizing payments
- Resulting from credential harvesting scams or real-time attacks
- Bank's responsibility is clear
- Fraud controls more established

Authorized Payments

Authorized Push Payment Voice Scams

- Victim is sending and authorizing payments
- Bank's responsibility varies by region
- Since victim is authenticating the session, fraud controls are lacking
- Reputational risk to the bank

Consumer Protection - Regulatory Evolution

USA

- DEC 30, 2011 Regulation E – Unauthorized payments
- June 2021 – Clarification on Reg E to clarify cases of negligence
- December 2021 – P2P transactions
- Letter from lawmakers – April 2022
  - Zelle Fraud
- Class action lawsuits

UK

- 2019 – CRM for APP fraud – 9 Banks
- 2020 – PSR introduces confirmation of payee participation
- 28 April 2022: CRM + CoP
- 10 May 2022: New Bill enabling PSR to require banks to reimburse APP fraud – Pending

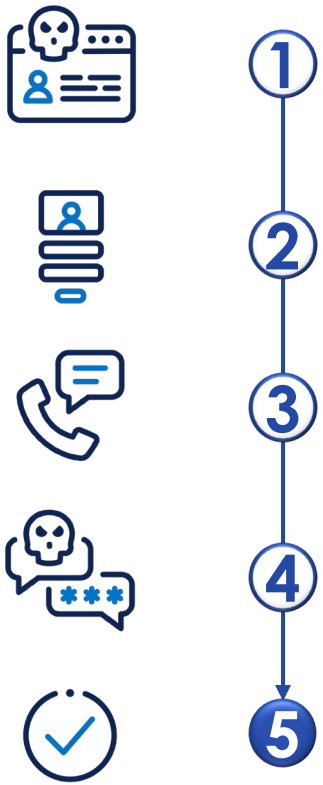
Australia

- October 2021 – Scams awareness campaign #BanksNeverAskThat

RSAConference2022

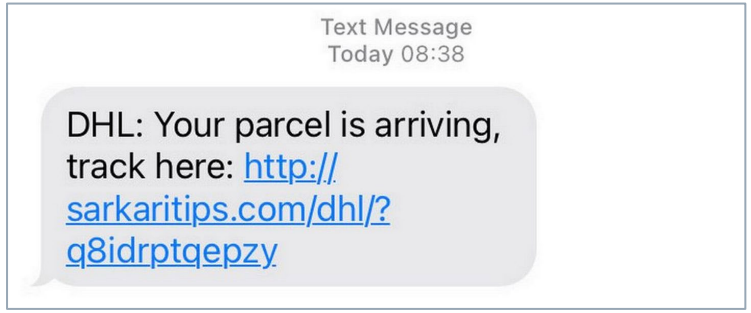
Deconstructing the Scams

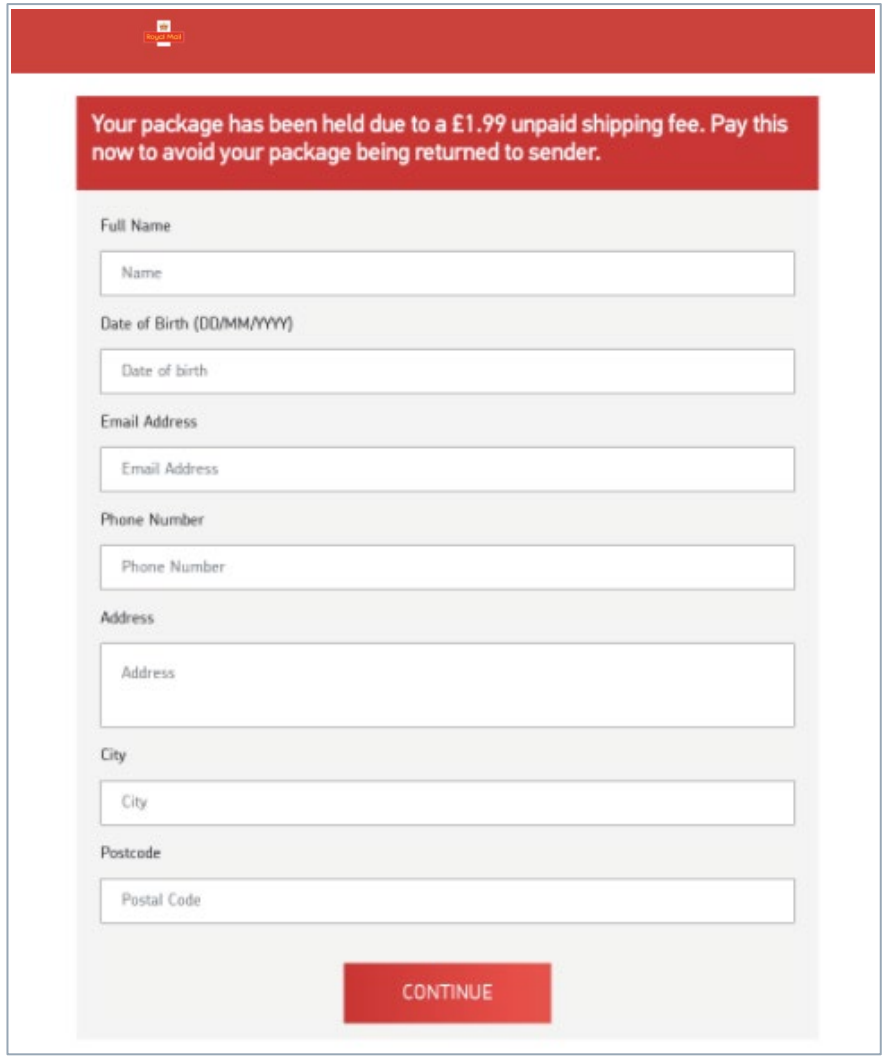
Anatomy of OTP Vishing Scam



Fraudster obtains legitimate user information on the dark web, or via phishing/smishing campaigns

The fraudster logs into the victim's bank account





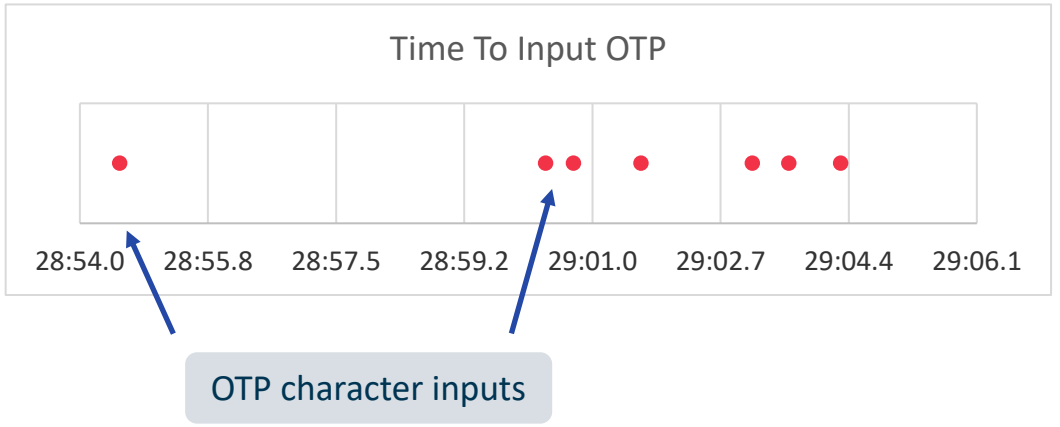
Anatomy of OTP Vishing Scam

1. Fraudster obtains legitimate user information on the dark web, or via phishing/smishing campaigns
2. The fraudster logs into the victim's bank account
3. Fraudster calls victim and convinces them to hand over the OTP codes
4. The victim dictates the OTP codes to the fraudster
5. The **Fraudster** completes the transfer

Device & Network

New device & network

Fraudster logs in with stolen credentials



Remote Access/Tech Support Scams

- Rapid year over year growth
- FBI Internet Crime Report*
  - 2019 - $54 million USD
  - 2020 - $146 million USD
  - 2021 - $348 million USD

Only ~0.07% of banking sessions are remote access

- Hybrid remote access scenarios – screen broadcast, where criminal is coaching the victim through the scam, whilst in view-only mode

(*)Tech Support Scams
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Anatomy of a Remote Access Scam

1. Fraudster contacts the Victim directly on the phone
2. Fraudster convinces the Victim to download a Remote Access Tool to their mobile device
3. Victim logs in to mobile banking
4. Fraudster takes control of session
5. The **Fraudster** completes the transfer

Anatomy of a Remote Access Scam

1. Fraudster contacts the Victim directly on the phone
2. Fraudster convinces the Victim to download a Remote Access Tool to their mobile device
3. Victim logs in to mobile banking
4. Fraudster takes control of session
5. The **Fraudster** completes the transfer

Installed Applications

Device profiling at login

Risky apps installed including a Remote Access App for the first time

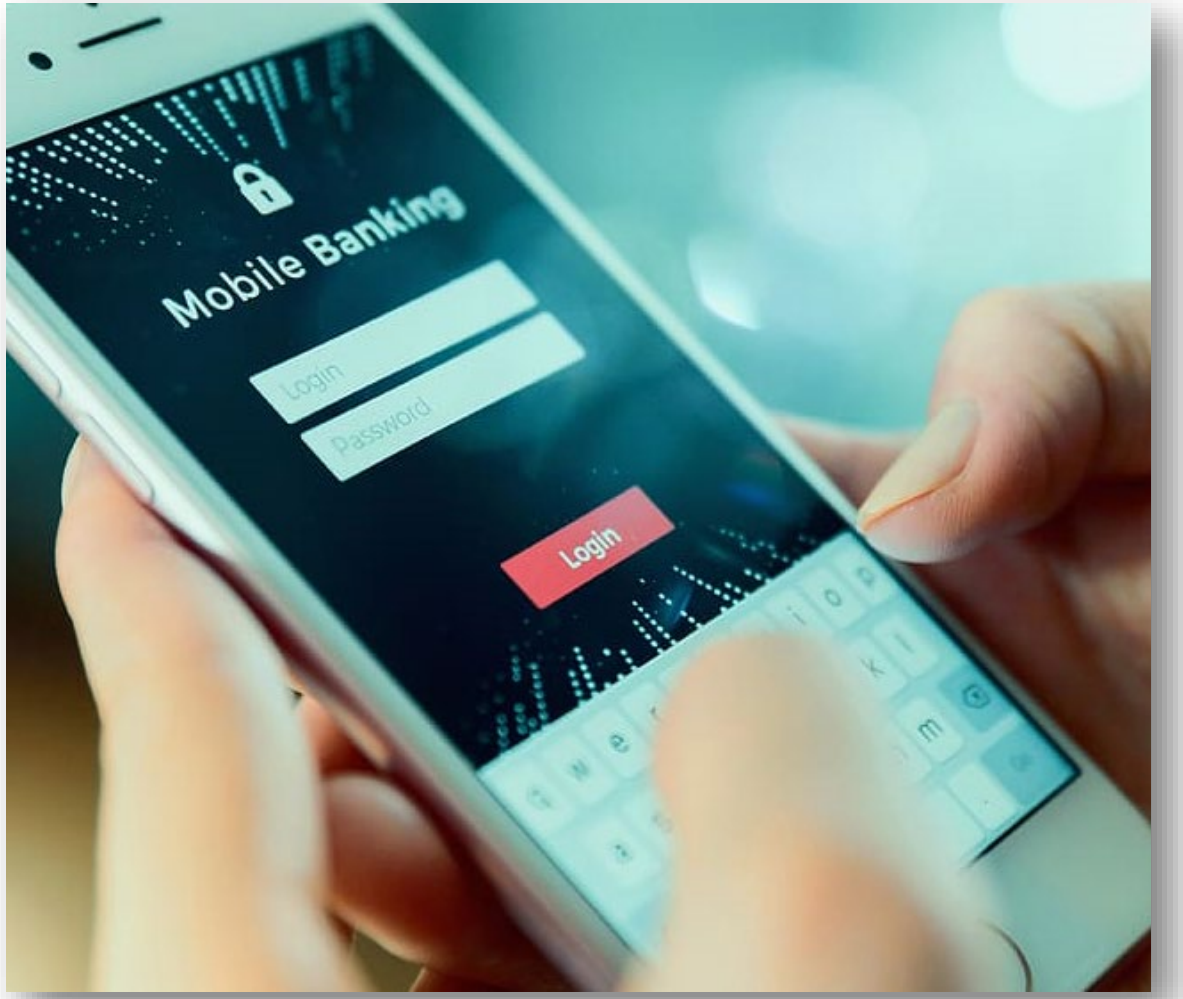
Device & Network

Consistent device and network profile of the genuine user

Biometric used for Banking App login

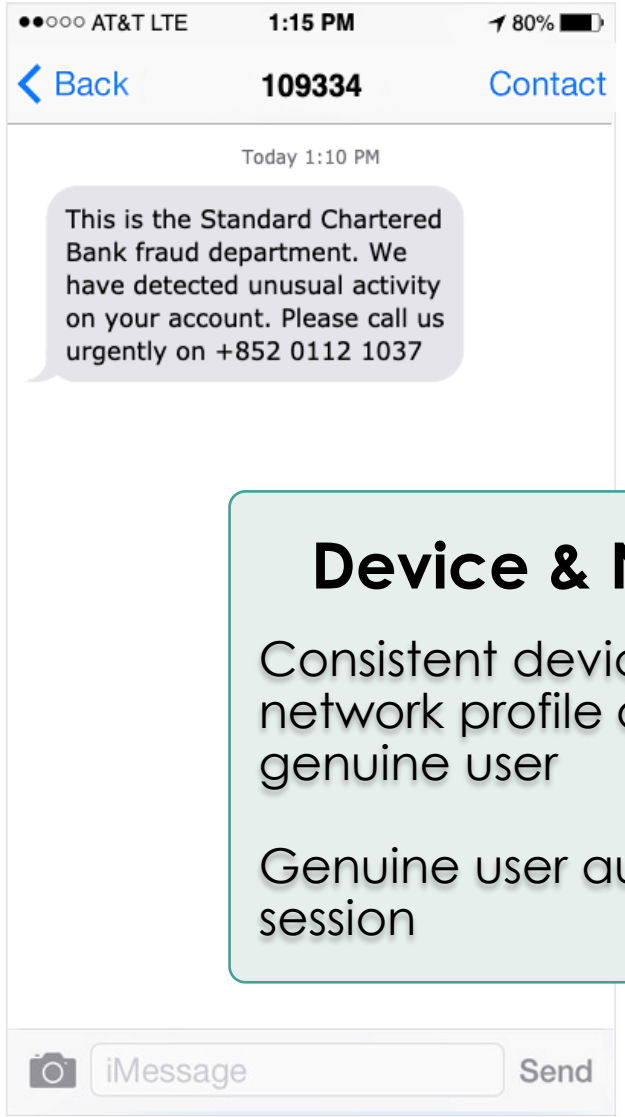
Teabot Mobile Malware

- Malware is downloaded after a smishing campaign or fake ad blockers
- Malware acquires broad permissions:
  - Read & intercept SMS
  - Delete applications
  - Use Accessibility Service to listen for opened apps and accept pop-ups automatically
- When an app in the target list is launched, Teabot starts an overlay attack



Anatomy of an Authorized Push Payment Scam

1. Fraudster hooks the victim via a Smishing campaign
2. Victim calls the fraudster in response to the SMS call to action
3. Fraudster impersonates a staff member from the bank, convincing the customer there is an urgent need to transfer funds
4. Victim logs into their bank account
5.
6.



Device & Network

Consistent device and network profile of the genuine user

Genuine user authenticates session

Anatomy of an Authorized Push Payment Scam

1. Fraudster coerces the victim on the purpose and details of the payment
2. The **Victim** completes the transfer

Payment Anomalies

03:36	Text Box › accoun...	› Left click	
03:36	10 seconds of inactivity		
03:46	Text Box › accoun...	› Typing	1111
03:47	6 seconds of inactivity		
03:54	Text Box › accoun...	› Typing	1
03:55	Text Box › accoun...	› Typing	1
03:56	Text Box › accoun...	› Typing	11
03:57	9 seconds of inactivity		
04:06	2 seconds of inactivity		
04:09	Text Box › accoun...	› Scroll d...	

High value payment to new payee

Mouse doodling while victim awaits instruction

Payee details dictated by fraudster

RSAConference2022

Mitigation Techniques

Mitigation Strategies

- Preventive
- Disrupts info harvesting

- Targeted
- Delays action
- Limits alert fatigue

- Risk-based
- Mitigates friction
- Layered approach ideal

- Stops attacks across channels
- Improves understanding of fraud MO's

Combining various strategies in a layered approach is best

Collaboration

“THE BANKING SECTOR CANNOT SOLVE THIS ON ITS OWN—THERE MUST BE A COORDINATED APPROACH ADOPTED ACROSS EVERY SECTOR IF THIS IS TO BE TACKLED EFFECTIVELY.” *

*“2021 Half Year Fraud Update,” U.K. Finance, September 2021

RSAConference2022

Summary and Q&A

What Have We Learned?

- Education campaigns are a good start but can lead to alert fatigue
- Strong authentication and device profiling is not sufficient protection
- Analyzing the entire user journey and layering multiple detection methods is key
- The attacks are increasing in frequency and sophistication – collaboration is essential
- The cost to the victim is devastating!

Apply What You Have Learned Today

- Next week you can:
  - Identify areas where your organization is vulnerable to social engineering attacks
- In the first three months following this presentation you should:
  - Map out the types of social engineering attacks that could target (or are already targeting) your customers
  - Define appropriate controls
  - Identify attack vectors (Phishing, Social Media Scams, etc)
- Within six months you should:
  - Present a plan to your executive team, focused on establishing defenses against social engineering attacks and their impact
  - Drive an implementation project to protect your critical gaps

RSAConference2022

Thank you