What Drives SMiShing Susceptibility?
A U.S. Interview Study of How and Why Mobile Phone Users Judge Text Messages to be Real or Fake

Sarah Tabassum, Cori Faklaris, and Heather Richter Lipford

Aug. 13, 2024

USENIX Symposium on Usable Privacy and Security (SOUPS 2024), Philadelphia, PA, USA

Center for Cybersecurity Analytics and Automation

SPEX
SECURITY + PRIVACY EXPERIENCES GROUP

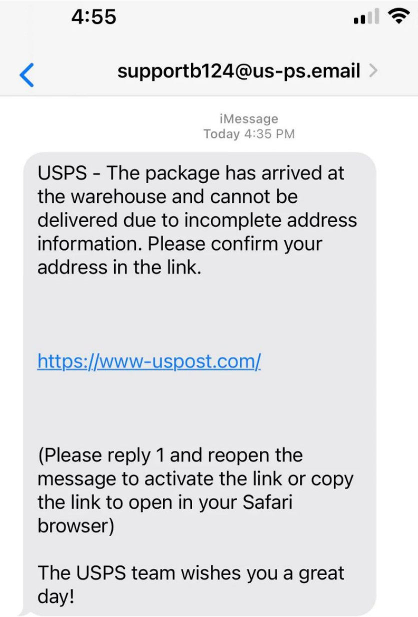
UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Key Takeaways

- SMS header info alone is not sufficient; trust relies on sender knowledge, context, links, personalization, format.
- Improved UI design with warning signs and filtering mechanisms can help users identify fraudulent SMS more efficiently.
- Cybersecurity training and education enhance users' ability to identify SMiShing text messages.

What are SMiSh? Why are They a Problem?

- A cyber attack where a **fraudster sends deceptive messages via SMS** to a phone, to **steal $$ or credentials** *(El Ayeb et al., 2020).*
- **Banks**, **delivery companies**, **retailers**, and **communication providers** are commonly impersonated *(Scroxton, 2021).*
- FTC data for 2022 shows that consumers reported **losses of $326 million to text scams**, an increase of **279%** since 2020



USPS - The package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link.

https://www-uspost.com/

(Please reply 1 and reopen the message to activate the link or copy the link to open in your Safari browser)

The USPS team wishes you a great day!

Example of a Common SMiShing Text: Fraudulent USPS Message Attempting to Steal Personal Information

What We Know from Phishing

- Impersonate **legitimate entities, request sensitive information**, and often **contain malicious links** *(Jakobsson, 2007; Blythe et al., 2011; Hong, 2012).*

- Susceptibility influenced by **email format, logos, sender recognition, URLs, message content,** and **situational context** *(Jakobsson, 2007; Alsharnouby et al., 2015; Curtis et al., 2018; Downs et al., 2006; Petelka et al., 2019; Downs et al., 2007; Egelman et al., 2008; Sheng et al., 2010; Jalali et al., 2020).*

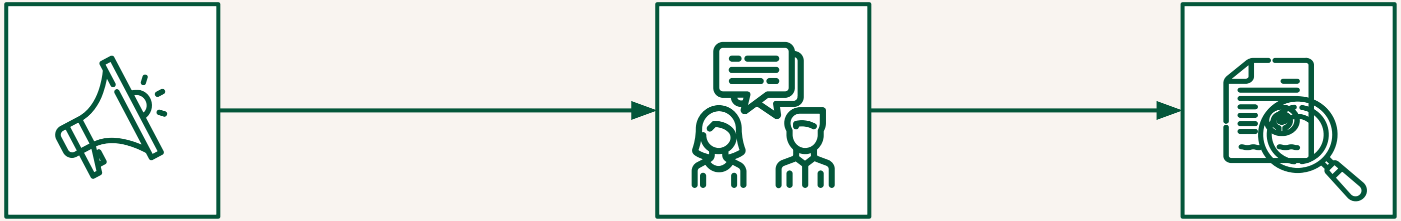
- **Younger individuals, especially females**, are more vulnerable to phishing *(Sheng et al., 2010).*

- **The Gap:** Uncertainty in Transfer to SMiShishing
    - **Personalized SMS** increase perceived legitimacy, but SMS lacks email's trust indicators like **detailed header info** and **visual cues**, making urgent action scams more effective *(Rahman et al., 2023; Clasen et al., 2021; Cahill, 2023).*

Research Questions

- **RQ1:** How do individuals perceive the credibility of SMS messages and make trust decisions?
- **RQ2:** What individual factors *(such as demographic characteristics)* and design factors *(such as visual cues and message content)* influence these trust decisions?

Study Approach



Recruitment Process

Via Facebook, WhatsApp, LinkedIn, Craigslist **(n=15)** and UNCC email listservs and flyers **(n=14)**

Criteria: Aged 18+, mobile phone users, able to attend in-person interviews

Interview Sessions

~50 minutes in-person sessions with n=29 (16 females, 13 males) in Charlotte, NC

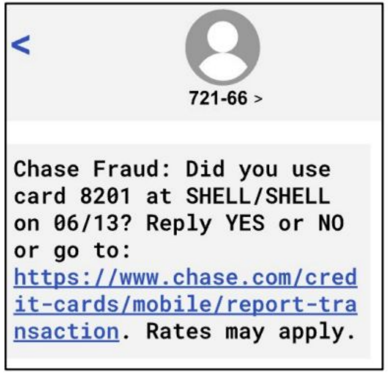
Activities: Discussed personal experiences with suspicious SMS, Analyzed SMS pairs and explored identification methods

Data Analysis

Analyzed interview data for legit and suspicious cues using thematic analysis and inductive open coding

Interview Participants Share Details on Trust Decisions

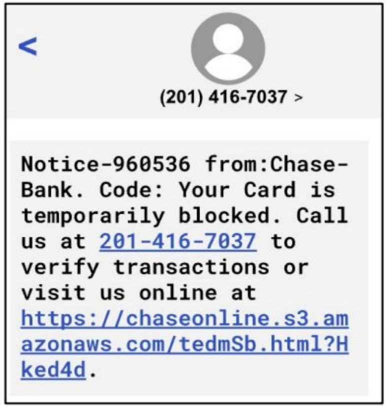
- Showed 3 out of 6 pairs of legit and fraud texts to elicit reactions
- Presented SMS pairs mainly impersonated banks *(e.g., transaction verification, card alerts)* and other services *(e.g., delivery services)*



<
721-66 >

Chase Fraud: Did you use card 8201 at SHELL/SHELL on 06/13? Reply YES or NO or go to: https://www.chase.com/credit-cards/mobile/report-transaction. Rates may apply.

Legit



<
(201) 416-7037 >

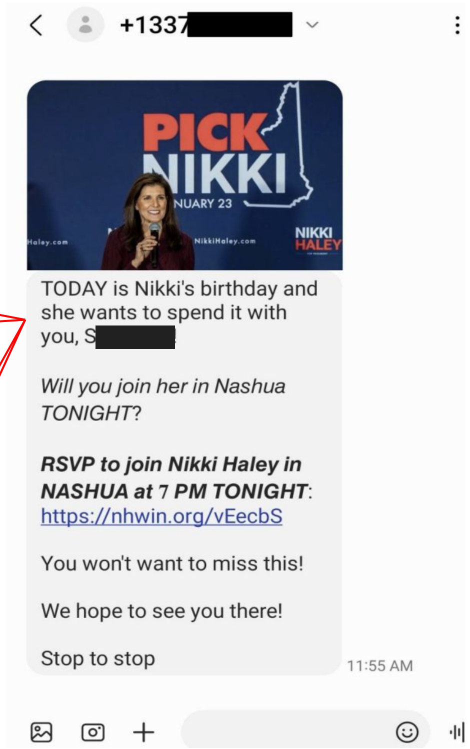
Notice-960536 from:Chase-Bank. Code: Your Card is temporarily blocked. Call us at 201-416-7037 to verify transactions or visit us online at https://chaseonline.s3.amazonaws.com/tedmSb.html?Hked4d.

Fraud

Example of a legit vs. fraud SMS pair presented to participants for evaluating their decision-making process

Cues for Suspicious Texts:

- If they contain links (28/29, 96.5%)
- Unknown sender (18/29, 62.1%)
  - either as only sign or combined with others, e.g., area code + unknown context
- Unofficial format (15/29, 51.7%)
- Misspellings (15/29, 51.7%)
- Out-of-context messages (6/29, 20.7%)
- Urging immediate action (4/29, 13.8%)



+1337[redacted]

TODAY is Nikki's birthday and she wants to spend it with you, S[redacted]

Will you join her in Nashua TONIGHT?

RSVP to join Nikki Haley in NASHUA at 7 PM TONIGHT: https://nhwin.org/vEecbS

You won't want to miss this!

We hope to see you there!

Stop to stop

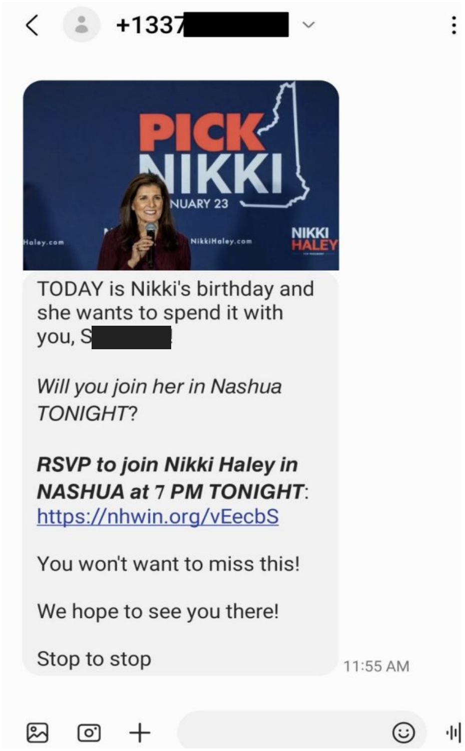
11:55 AM

Suspicious text message about a political campaign from an unfamiliar context and area code, reported by P4.

Cues for Suspicious Texts:

Quote from P4:

"I think this is a fraud...I don't know who Nikki is, I didn't sign up for that."



TODAY is Nikki's birthday and she wants to spend it with you, S[redacted]

Will you join her in Nashua TONIGHT?

RSVP to join Nikki Haley in NASHUA at 7 PM TONIGHT: https://nhwin.org/vEecbS

You won't want to miss this!

We hope to see you there!

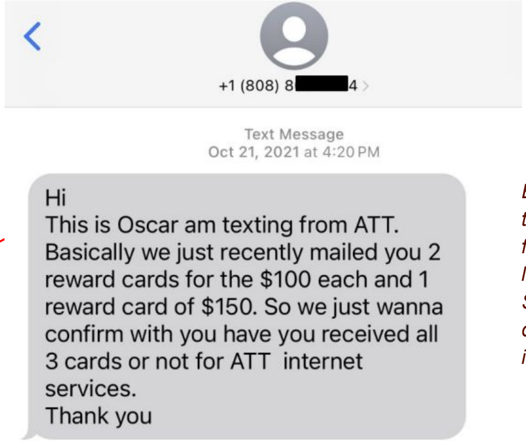
Stop to stop

11:55 AM

Suspicious text message about a political campaign from an unfamiliar context and area code, reported by P4.

Cues for Legitimate Texts:

- Personalized info (14/29, 48.3%)
  - e.g., last 4 digits of their card
- Known context (11/29, 37.9%)
- Known sender (10/29, 34.5%)
- Official format (8/29, 27.6%)
- Also mentioned:
  - No call to action
  - No personal inquiries
  - Correct spelling and grammar

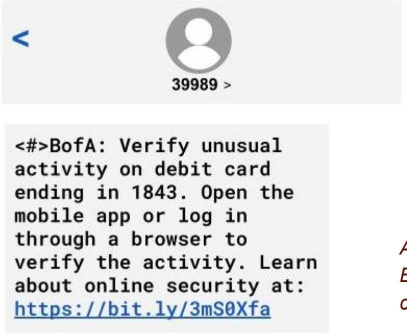


+1 (808) 8[redacted]4

Text Message
Oct 21, 2021 at 4:20 PM

Hi
This is Oscar am texting from ATT. Basically we just recently mailed you 2 reward cards for the $100 each and 1 reward card of $150. So we just wanna confirm with you have you received all 3 cards or not for ATT internet services.
Thank you

Example of a SMiShing text message P18 fell for while expecting a legitimate gift card. Scammers called but didn't ask for target info immediately.



39989

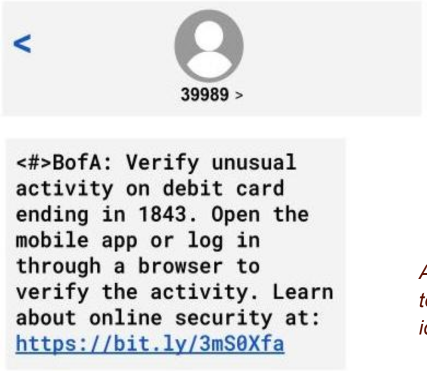
<#>BofA: Verify unusual activity on debit card ending in 1843. Open the mobile app or log in through a browser to verify the activity. Learn about online security at: https://bit.ly/3mS0Xfa

An example of a (simulated) BofA text that P7 + others correctly identified as legitimate.

Cues for Legitimate Texts:

Quote from P7:

"The pound sign … I feel like I've seen [Bank of America] messages that also use symbols in the beginning"



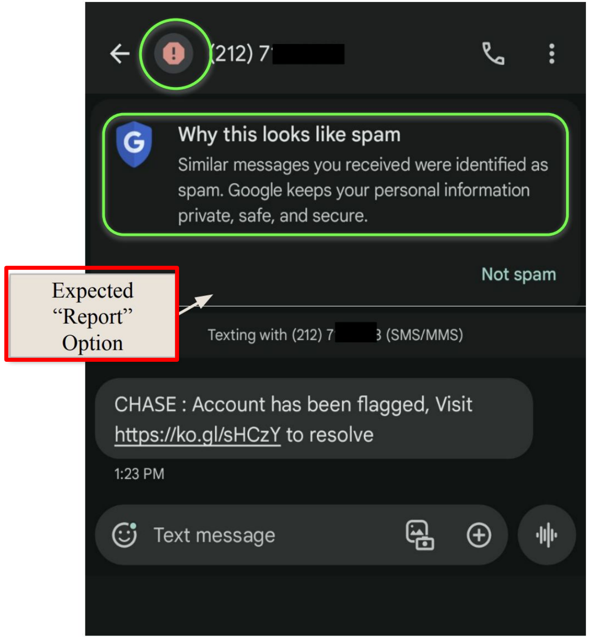
```
<#>BofA: Verify unusual
activity on debit card
ending in 1843. Open the
mobile app or log in
through a browser to
verify the activity. Learn
about online security at:
https://bit.ly/3mS0Xfa
```

An example of a (simulated) BofA text that P7 + others correctly identified as legitimate.

Android vs. iOS: Warning Signs Aid in Detecting Suspicious SMS

Android:

- Built-in spam filters with warning signs for suspicious messages.
- Participants appreciated the clear alerts but desired more accessible reporting options.



(212) 7[redacted]

Why this looks like spam

Similar messages you received were identified as spam. Google keeps your personal information private, safe, and secure.

Not spam

Expected "Report" Option

Texting with (212) 7[redacted] (SMS/MMS)

CHASE : Account has been flagged, Visit https://ko.gl/sHCzY to resolve

1:23 PM

P26 shared this example, highlighting Android SMS Spam Filters' warning signs in green, which were appreciated by participants. However, users desired more accessible reporting options

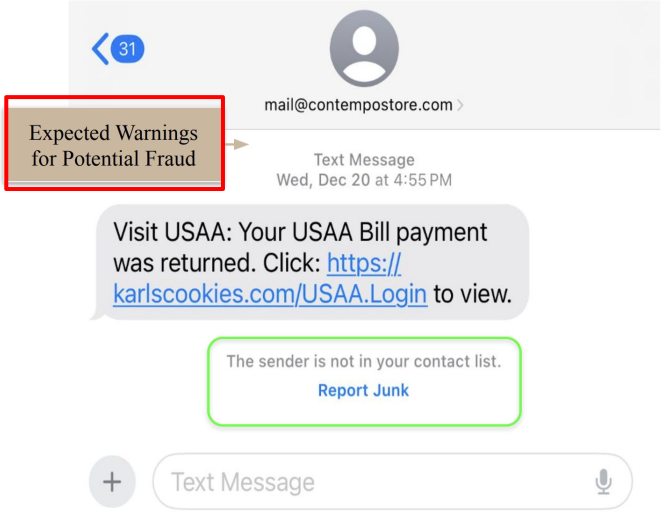
Android vs. iOS: Warning Signs Aid in Detecting Suspicious SMS

Android:

- ○ Built-in spam filters with warning signs for suspicious messages.
- ○ Participants appreciated the clear alerts but desired more accessible reporting options.

iOS:

- ○ Lacks spam filters and warning signs.
- ○ Relies on the *"Report Junk"* option for reporting suspicious messages.



Expected Warnings for Potential Fraud

Text Message
Wed, Dec 20 at 4:55 PM

Visit USAA: Your USAA Bill payment was returned. Click: https://karlscookies.com/USAA.Login to view.

The sender is not in your contact list.
Report Junk

Example of a smishing text message shared by P15. The 'Report Junk' option, highlighted in green on the iMessage interface, was useful for reporting. Participants expressed a need for warning signs to better identify potential fraud SMS.

Awareness, Age, and Verification Practices in SMiShing Detection

- **Impact of Awareness Training:** Interviewees with **prior awareness training in job or school performed better** at distinguishing legitimate from fraudulent texts.
- **Age Differences: Older participants did better** at identifying fraud SMS compared to younger interviewees.
- **Verification Practices:** Most interviewees stated they would **verify suspicious SMS directly with the bank or company.**

Recommendations

- **Distinguish Spam vs. Scam:**
  - Design tools and educational programs to help users tell apart legit promotions from scams.

- **Enhanced Security Features and Reporting Mechanisms:**
  - Promote advanced filtering features on mobile devices to detect and block SMiShing and make reporting fraudulent SMS easier.

- **Targeted Cybersecurity Training:**
  - Offer training, especially for younger users and those new to cybersecurity.

What is Left to do?

- **Enhanced Mobile Interfaces:** Studying more SMS visual styles and interfaces to understand their impact on SMiShing recognition.
- **Broaden SMiShing Categories:** Exploring various SMiShing types beyond financial scams.
- **Proactive Security Measures:** Collaborating with telecom companies to improve security, educate users, and monitor emerging SMiShing tactics.

What are Your Questions?

- SMS header info alone is not sufficient; trust relies on sender knowledge, context, links, personalization, format.
- Improved UI design with warning signs and filtering mechanisms can help users identify fraudulent SMS more efficiently.
- Cybersecurity training and education enhance users' ability to identify SMiShing text messages.

For more information:

- Email: *stabass2@charlotte.edu*
- Connect with me on LinkedIn: