KAVYA SRINIVAS MURTHY

SOCIAL ENGINEERING AND PHYSICAL INTRUSIONS

SMS SPOOFING:

98% of cyberattacks are created using one or more elements of social engineering, like spoofing and smishing, but less than 35% of the population knows what it is. Let's see what SMS spoofing is, how it works, and how we can protect ourselves from it:

What is SMS spoofing:

SMS spoofing is changing sender details like a phone number and/or contact name for fraudulent purposes. We cannot block a spoof text or reply to it. The whole idea behind spoofing is impersonation.

For an instance, we receive a text from someone we think we know them, but in the end, things end miserably. The name and/or mobile number are only similar to the ones people have in their contact list, but not the same.

Sometimes numbers are changed altogether. SMS spoofing is also known as "SMS originator spoofing" because it changes originator sender details.

How does SMS spoofing work?

SMS spoofing changes phone numbers and/or contact details to mislead mobile users. Victims receive a text that appears to be sent by someone they know like family members or friends or people in their contact list. This type of cybercriminal activity involves falsifying data to obtain an illegitimate advantage.

The internet has been invaded with tools that alter names and mobile phone numbers. All it takes is one download, and fraudsters can send text messages from whatever number they choose, using names of well-known companies or even banks. (For example: Octopush app which can be used to send fake sms)

Some businesses even offer spoofing online services, but this borders on illegal. As long as the law remains uncertain, anyone can find their way around it and "help" scammers trick innocent users. Most such platforms offer their services at very low prices, which makes the scam even more attractive.

How do fraudsters/attackers use spoofing to get sensitive user information?

Fraudsters often change one letter, number, or symbol in the Sender details, to make their message seem valid. An example would be changing the letter L to an I to make it look like a company like PayPal is contacting you. Once you believe the message came from a trusted source, chances are you'll click on the embedded link they sent and offer all the personal information they need.

Spoofing is not restricted to texts. It is also done via email, caller ID, or GPS receivers. The most common type of spoofing involves sending emails or texts to show a potential problem with a recent purchase you made or even a recent transaction.

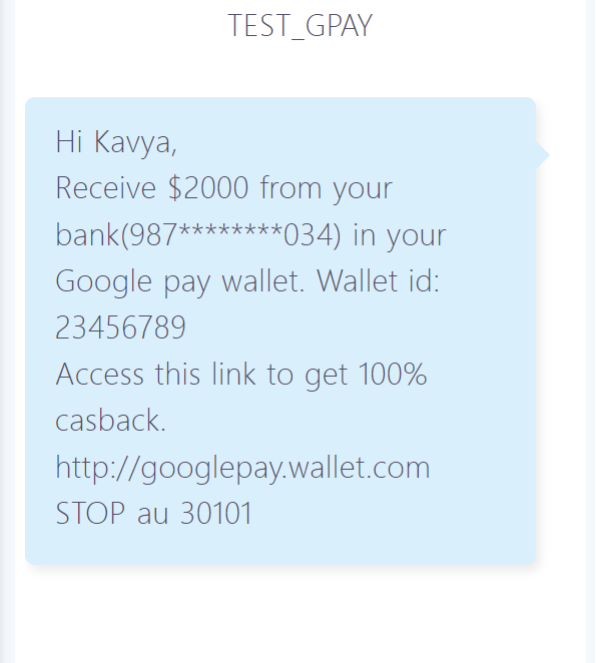
Fraudsters don't randomly target people; they target the ones who are waiting for delivery confirmations, bank transactions that are still pending, etc. They are more likely to click on links

leading to malware or fake login pages simply because they are expected to take action. Identity theft, data breaches, and financial loss are only one click away.

Types of SMS Spoofing:

1. Fake money transfers

Online shopping is one of the main areas where fraudsters operate. They visit online stores, add multiple items to their cart and then “attempt” to make the payment via bank transfer. If they have access to the number, the store uses to get bank updates, the scam is complete. They then send a spoofed text message, impersonating the bank, which “confirms” that the transaction has been made.

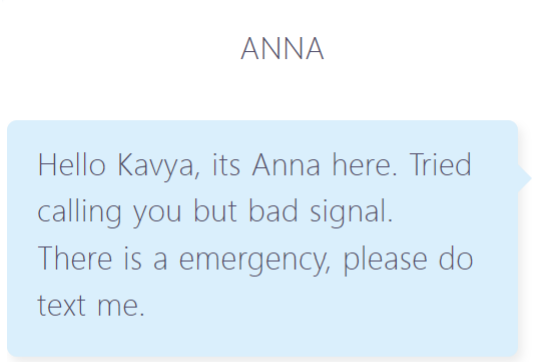


2. Fake sender IDs

Pretending to represent a well-known company can be highly productive, as it takes little to no effort. Let’s say you know someone’s vehicle insurance will expire, and they will have to renew it. Scammers can use this information to con people into renewing their insurance but redirect them to a site that has nothing to do with their insurance company.

3. Harassment (stalking, pranking, family emergency, etc.)

Scare tactics are very common among scammers, who often send texts telling families that someone close to them is in the hospital or has been arrested. And create a emergency situation, and make people panic and access the link.



How to prevent SMS spoofing?

- Never access SMS links. Always call the institution that requires this, in case anything looks suspicious. Banks never ask for sensitive details via SMS; they either require you to log in to their platform using your dedicated username and password or ask to see you personally at one of their offices.
- Carefully analyze sender details. Many spoofed messages contain grammatical errors or subtle changes in Sender Name and/or Number. Watch out for the small things before replying to any text message, especially if something seems off, like if the message contains an unusual request from someone you know or an institution you are in contact with.
- Never respond to imperative messages. Scammers usually want you to react on the spot because you might discover scam if you take your time. Whenever you receive a text that includes a sense of urgency, you should be suspicious.

- Always have a spam filter for your email address. This will redirect most spoofed messages to Spam.
- Never access sites with “No Lock” (Unsecure) symbols or unencrypted URLs (HTTP instead of HTTPS) and always check to see the URL before clicking on it; you can do this by hovering over it or by holding your finger on the link for a few seconds if you are using a mobile device.
- Install a high-performance antivirus app for multi-layered protection on your phone and desktop.

Legal uses of SMS spoofing for business:

Although SMS spoofing has a bad rep, it can be used for legal purposes as well.

These include bulk SMS messaging, official messages, and instances where it is paramount to protect someone’s identity. Like sending bulk SMS campaigns. Companies connect with their target audience to promote their products or keep clients updated with upcoming events using mass text messaging.

Broadcast official messages. Another legal use of SMS spoofing involves official messages. Banks and prominent service providers spoof their messages to inspire trust. However, this can often backfire, as hackers can use famous financial institution names to request sensitive information from unsuspecting users. So it is best to double-check with your bank before sending out any information of the sort and never access embedded links from SMS messages.

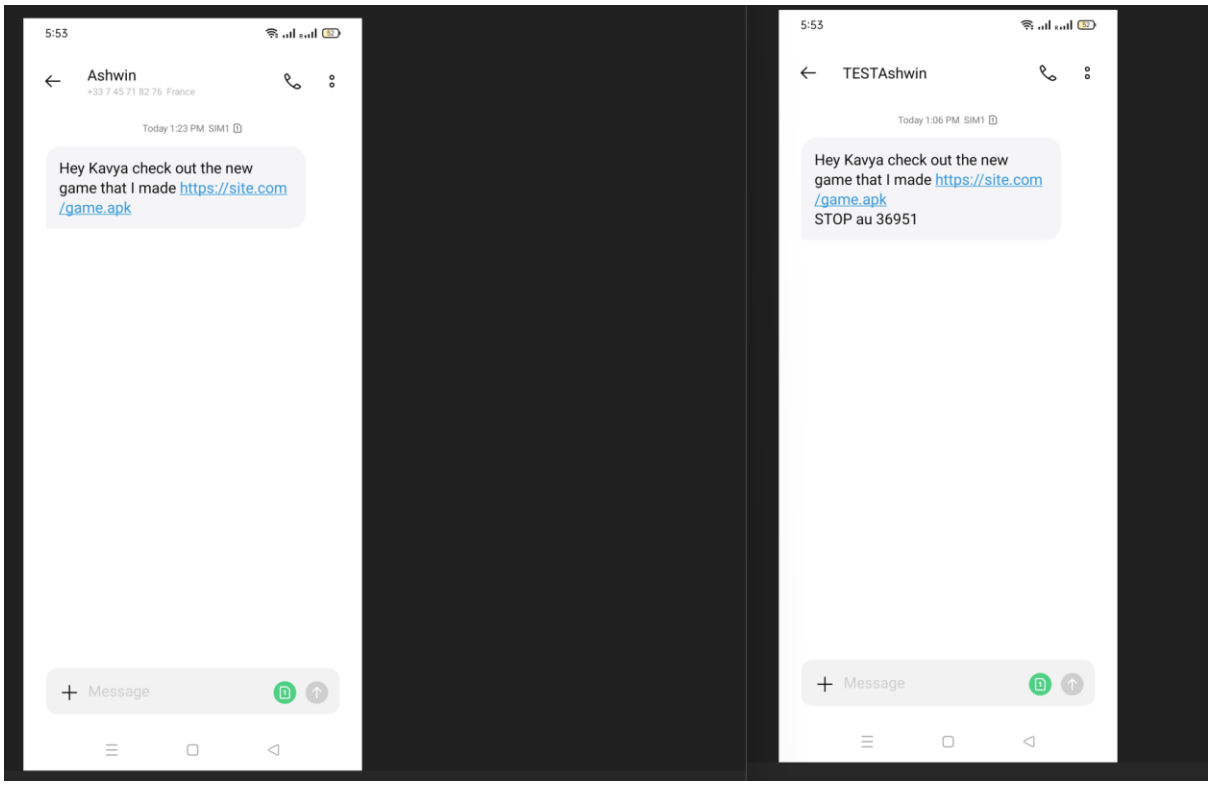
Preserve anonymity. Some people would rather remain anonymous when sending out text messages. They use spoof texts to send anonymous tips to the Police or other institutions while their identity remains protected.

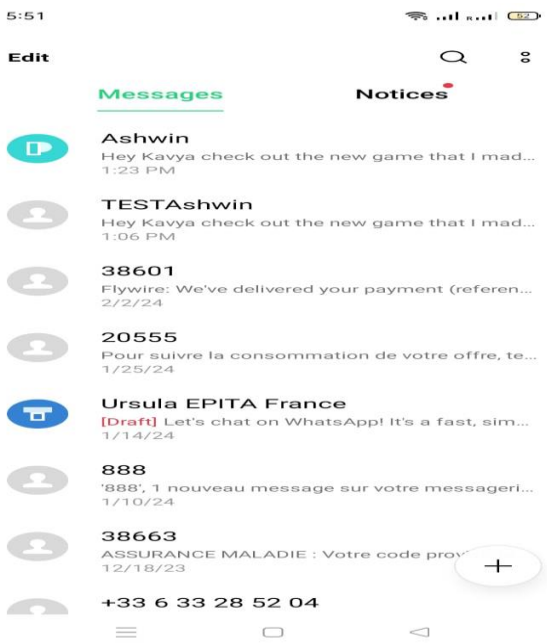
Conclusion:

Spoofing is a standard practice among scammers, but it is easily detected if you know where to look. If you are a victim of an SMS spoofing attack, it is best to contact law enforcement immediately. Always remember to keep your bank account and financial information safe by not replying to anonymous texts or even texts that seem acceptable at first glance.

Demonstration:

In this image of my phone screenshot, it shows message from Ashwin and TestAshwin(for example it shows TestAshwin, just to differentiate between legitimate sender like Ashwin (my friend in mycontact list), and TestAshwin is a message received from attacker who spoofed message as my friend and asking me to click on the malicious link.

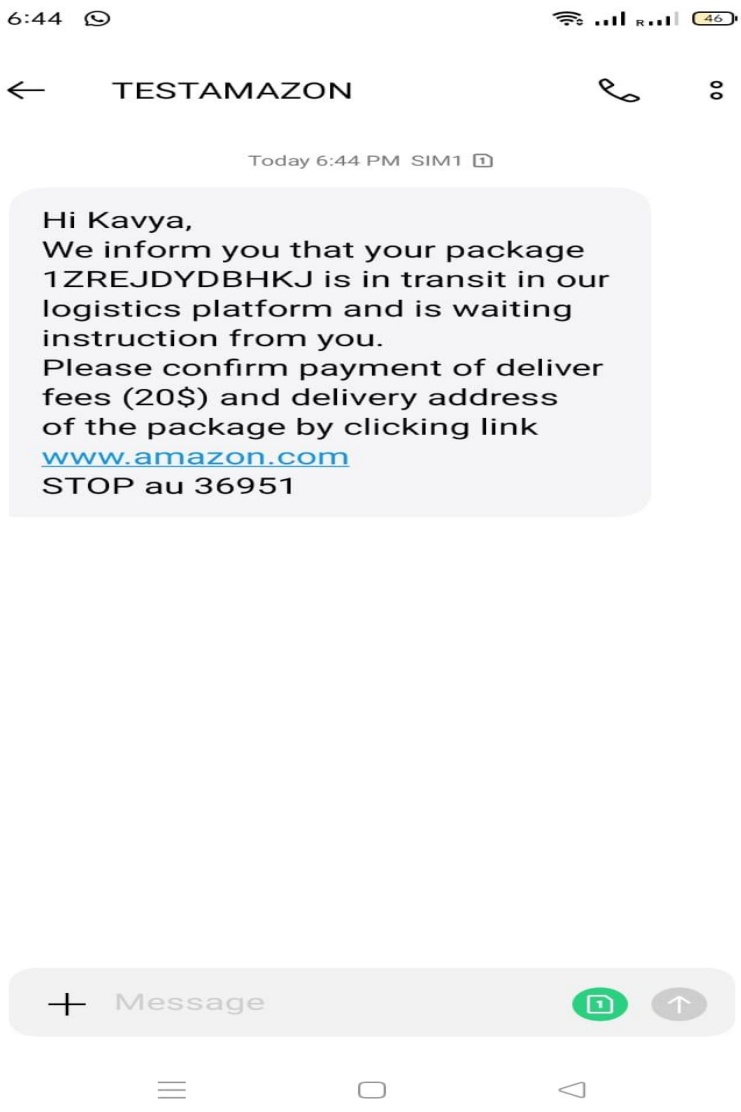


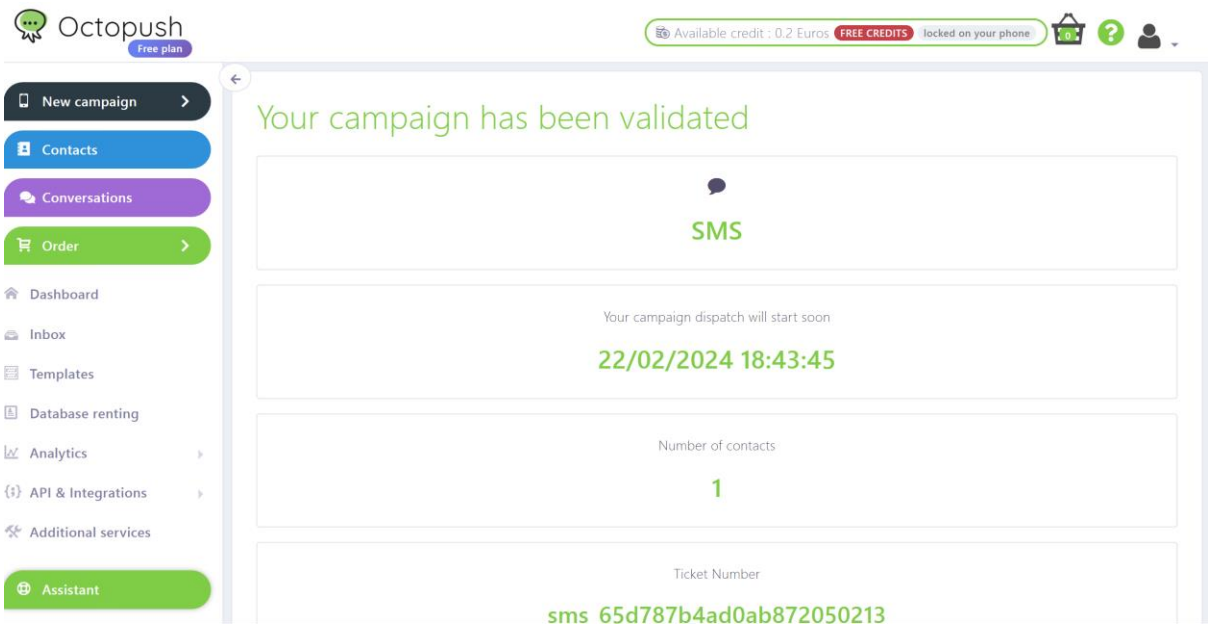


When I see both messages its hard to find (however here it diffrentiates testashwin, but in real case scenario even message comes alike from Ashwin)I would click it, even not by checking details sender, because legitimate Ashwin contact in first image dispalys his mobile number, but in second message its does not because its fake.

I have used OctopushApp to send spoof messages.

Other example of messages that could be spoofed messages by using app is:





SMS

Your campaign dispatch will start soon

22/02/2024 13:06:50

Number of contacts

1

Ticket Number

sms_65d736e94f846117763176

Please keep this ticket as a sending proof.

Click on "Analytics" To display the history page and display your statistics once they are available.

Ref: https://www.textmagic.com/blog/sms-spoofing-explained/

https://client.octopush.com/sms-campaign/create/sms-premium?from_draft=true