

FRAUD INTELLIGENCE

Smishing and evolving threat actor tactics

JUNE 21, 2024 - By Gina Ojaokomo - SVP Threat Intelligence

What is smishing?

Smishing refers to SMS-phishing attacks where scam messages are sent via SMS. Instead of longer scams being delivered via emails, it's scams being sent via text messages. Such messages usually contain a link and impersonate legitimate organisations. Threat actors use various manipulative techniques to convince and trick recipients of smishing messages.

GOV.UK: You are eligible for a discounted energy bill under the Energy Bills Support Scheme. You can apply here: <https://energy.support-rebate.com>

Fig 1 - Legacy smishing message

Emerging tactics

Smishing messages traditionally used to contain only links, but threat actors have adapted their tactics to include confusing linkless messages that use phone numbers or that ask for one word or letter replies without any URLs included initially. Some recent messages we've noticed have only contained one word - "Hi", once the recipient engages with the threat actors by replying they then send further messages sometimes offering work opportunities or acknowledging a non-existent job application.

End Game for Smishing Threat Actors

The end goal for threat actors is to pique the interest of recipients of the smishing messages and to get them to engage with them. This could be by clicking a link, calling a phone number or replying to a message. The recipient then receives follow-up interactions

FRAUD INTELLIGENCE

from the scammers that recipient's bank account has been compromised due to the previous smishing message they engaged with and that they need to take some risky action, such as to transfer money to a safe account. Our threat intelligence analysis established a strong link between smishing messages, vishing (subsequent phone calls from threat actors) and Authorised Push Payment (APP) fraud.

How to avoid becoming a victim of smishing scams

Here are 3 practical tips to avoid falling for smishing scams

- 1. Don't be eager to click on links** - Some organisations follow poor B2C/A2P SMS practices and use URL shorteners to shorten links, further confusing end-users. Please don't click on links included in text messages. It's better practice to type in the URL into a browser yourself or visit the organisation's website via another means.
- 2. Be wary if you receive a message out of the blue** - Such messages may be just be a notification that there's been a transaction on your account, but remember smishing scam messages are designed to prompt you to engage.
- 3. If in doubt, contact or phone your bank using another method** - You can call your bank using the number on the back of your bank card or on their website. If you're based in the UK you can also call 159, which is a fraud hotline that will connect you to your bank's fraud prevention service. You can also visit the bank's branch in person. Some banks like Monzo, have a feature in their app where you can check if it's really someone from the bank's team that's calling.

PORGIESOFT Security provides advanced fraud intelligence, scam listening and analysis of emerging smishing threats. Our vision is to be a world-class leading authority in the detection and prevention of cyber-fraud, inspecting language as data.

PORGIESOFT LTD

PORGIESOFT LTD is a company registered in England and Wales. Registered Number: 11660739

Registered Address: Future Business Centre, King Hedges Road, Cambridge, United Kingdom. CB4 2HY

PORGIESOFT SECURITY is an anti-fraud cybersecurity firm based in Cambridge, with our team working around the world. We're an NCSC (a part of GCHQ) For Startups Alumni Startup. We specialise in fraud intelligence - combining research data, threat intelligence (phishing, smishing), OSINT, transaction analytics and artificial intelligence to prevent fraud helping consumers and businesses stay safe online.

