



THREAT INTELLIGENCE RESEARCH

SMISHING REPORT

JULY 2022



PORGiESOFT
Tech

TABLE OF CONTENTS

About PORGiESOFT	3
Executive Summary	4
Introduction	5
Smishing Threat Landscape	6
Smishing Attacks	7
• Research Highlights	8
• Classes	9
• Levels	12
Insight into UK Smishing Attacks	15
Conclusion	16



ABOUT PORGiESOFT

PORGiESOFT is on a mission to use AI to make everyday time-consuming tasks in fraud detection and education easier and faster, we're building smart machines that can quickly carry out routine tasks and adapt in the process. We are a tech startup based in Cambridge, but we actively deploy our AI products across several countries. We were founded in 2018.

To effortlessly detect and report cyber-fraud to impersonated organisations in real-time and to protect consumers, we've built SenseText™ - a powerful fraud detection platform. Powered by our natural language processing technology, SenseText™ empowers businesses with smishing cyber-fraud detection capabilities and enables everyday consumers to be able to quickly run hundreds of automated checks on text messages allowing them to carry out transactions with more confidence.

www.porgiesoft.com

EXECUTIVE SUMMARY

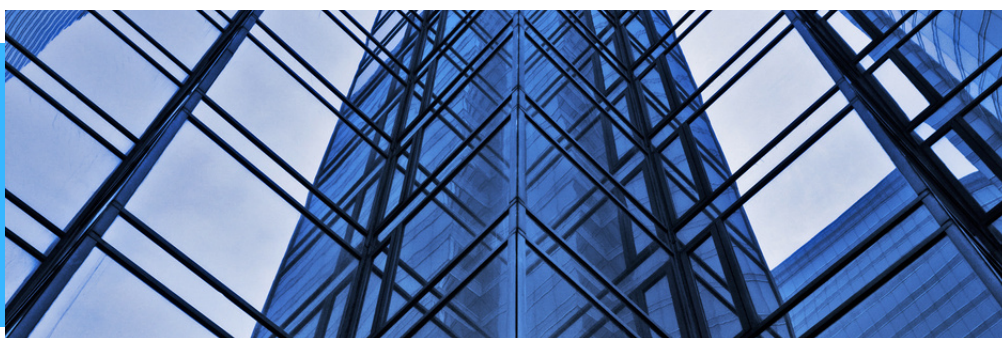
The mission of the National Cyber Security Centre (NCSC) – a part of GCHQ – is to make the UK the safest place to live and work online. Part of the focus of the NCSC's Growth Fund is to help solve problems that are related to the mission. PORGiESOFT (a tech startup) is one of the NCSC For Startups Alumni, working to solve one of the UK's most important cyber challenges around smishing.

Smishing is closely connected to cyber-fraud and attempts to defraud UK consumers. In 2020 and in the first-half of 2021, around 60% of Britons were targeted according to the Guardian. Due to the recent 700% rise in smishing attacks, combined with the inability of around 95% of consumers in the UK to reliably detect scam texts and the resulting losses from cyber-fraud, there was a need to develop technology to make it easier for consumers to detect these messages. Scam messages also look more convincing than ever, making them harder to detect.

The Growth Fund was used to carry out research around smishing to better understand, closely study and investigate the extent of the smishing threat in the UK. This report presents a summary of the PORGiESOFT's research activities during the project. It is designed to help interested parties to better understand not just the current trends, but the historical state of the smishing threat in the UK.

At a lower level, the report addresses the classification of smishing attacks into classes and levels. The report shares insights into various types of attacks – *what* bad actors are using to attack and *who* they are impersonating. Banks, Parcel Delivery Companies and Government are historically identified as the most impersonated organisational entities. The research revealed new attacks designed around phone numbers only, a prompt to reply with one word or no ask to respond.

The benefits of the Growth Fund have included helping PORGiESOFT to carry out research and development activities around smishing. The Growth Fund resulted in the development and acceleration of (x5) five smishing anti-fraud products and services including building a robust smishing threat intelligence capacity. The research and development activities have contributed to improving UK consumer confidence and online safety as well as gradually raising awareness around cyber-fraud. All of these initiatives contribute to the NCSC's mission.



Smishing (also known as SMS-Phishing) is a type of attack where phishing is carried out over SMS. A bad actor impersonating a legitimate organisation or claiming to be another person, typically tries to trick a person into giving away details that are then used to carry out cyber-fraud, download malware or steal sensitive data.

Smishing is becoming more sophisticated and may culminate in additional fraudulent impersonation phone calls (vishing), or emails (phishing). Smishing attacks have intensified over the last 2 years and new waves of attacks have been triggered by current events, as these events make smishing attacks more relevant and believable.

According to Ofcom over 45 million people were targeted by smishing texts and calls in 2021. Ofcom also reported that around seven in 10 people (71%) said that they had received a suspicious text. A typical smishing text is illustrated below -



NHS: You've have been in close contact with a person who has Omicron. Please order a Test Kit: <https://nhs-omicron-test.com>

Our threat intelligence research around smishing in 2022 was designed to better understand the historical and current state of smishing as well as to develop strategies to classify, prevent and subsequently detect smishing attacks.

OTHER CONNECTED TERMS:

- **Phishing:** This is a type of fraudulent practice primarily delivered via emails, in which cybercriminals attempt to get people to click on links within their emails, install malware, transfer some money or take some other unwise action that could result in serious losses.
- **Vishing:** This is a type of fraudulent practice delivered via phone calls or voice messages, in which cybercriminals try to trick people into clicking on links, install malware, transferring some money into a safe account or taking some other unwise action.
- **Fraud:** Fraud is when trickery or deceit is used to gain a dishonest advantage. Fraud is usually used to gain financial benefits.
- **Cyber Crime:** Cyber crime refers to any criminal activity dealing with computers or computer networks. Cyber crime can be very complex.



Research KEY FINDINGS

KEY FINDINGS:

Smishing is a growing problem globally, it is not only under-reported but threat intelligence around smishing is not well-coordinated.

Smishing text messages are just one of the numerous methods being used by bad actors to deceive victims. Research has revealed that it is usually part of a larger scheme to deceive and has been quite successful in luring victims in.

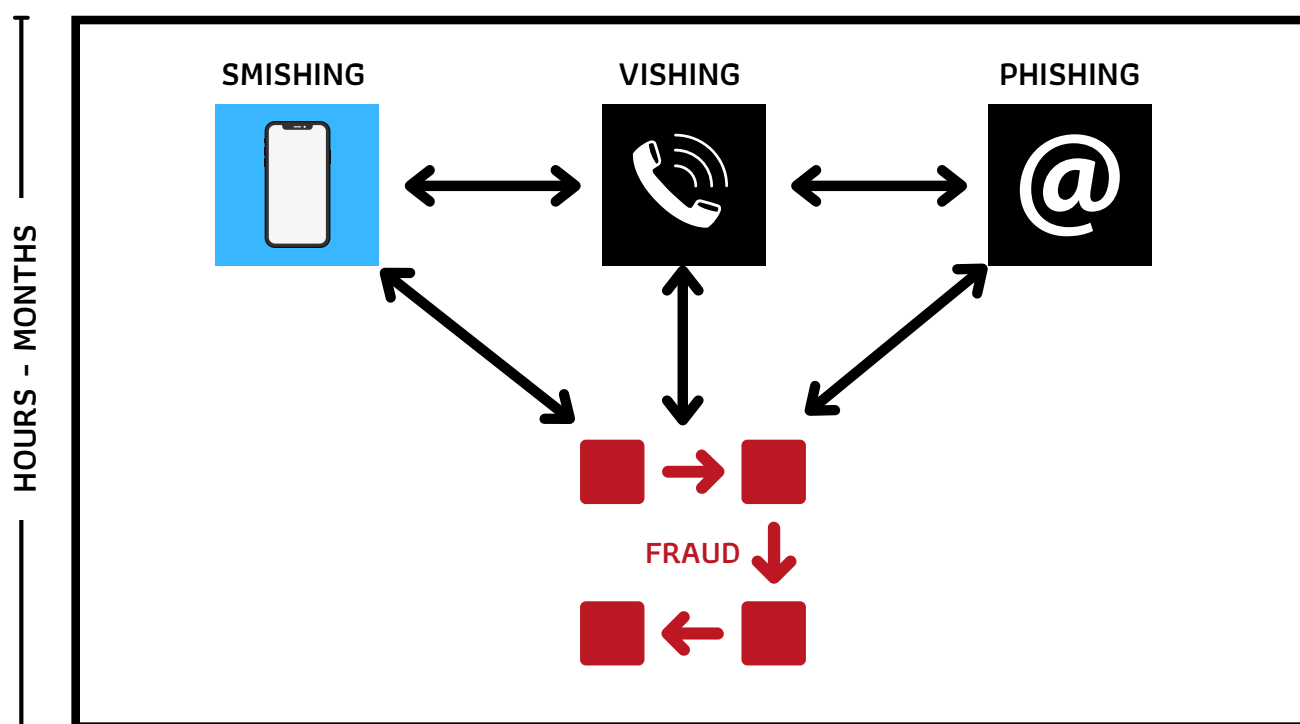
Smishing attacks are sometimes cleverly combined with other social engineering attacks like vishing and phishing to deceive, persuade and convince victims.

TYPICAL SMISHING EXAMPLE: THE VICTIM

1. Receives a **smishing** text to order a test kit
2. Clicks on the link to visit a fake website and enters their personal details
3. Receives a **phishing** confirmation email
4. Receives a **vishing** phone call from a fake bank customer representative
5. Is pressured into transferring funds to a fraudulent "safe bank account"



ORIGIN: BAD ACTOR



TARGET: VICTIM

- Employee
- Consumer

Research

KEY FINDINGS



KEY FINDINGS:

The emotional state of victims is an important factor influencing the success rate of smishing attacks, based on real-life examples. When under a lot of stress or immediately after a life event, victims might be more susceptible to smishing attacks and fraud.

SMISHING ATTACKS

Overview

Smishing attacks in the UK over the last decade has been targeted mainly at consumers. Why? According to recent statistics, 87% of UK households shopped online in 2020. With the increase in online shopping and as more banks close local branches, communication with consumers is projected to rely more and more on communication channels like SMS. This indicates that more genuine customer communication such as bank account notifications and online retailer delivery updates will likely be sent via SMS. However, as SMS is perceived to be more trustworthy than emails, there is a risk that cybercriminals will capitalise on such opportunities and impersonate organisations that have a significant online presence.

This section of the Smishing report briefly presents:

- Research Highlights
- Attack Labelling – Classes
- Attack Labelling – Levels



RESEARCH
HIGHLIGHTS |

OSINT (Open Source Intelligence) was primarily used to drive the research. Smishing datasets were subsequently analysed to further investigate smishing attacks and to produce actionable intelligence reports. Secondary methods used included conducting interviews with financial crime/fraud teams and the research was supplemented by investigating real-life cases of smishing attacks that culminated in cyber-fraud.

MOST IMPERSONATED
BRANDS

We analysed thousands of smishing attacks to identify the most impersonated brands in the UK, based on cumulative historical and current trends -

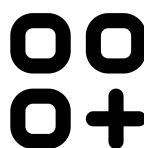
- 1 **Royal Mail**
- 2 **HMRC**
- 3 **HSBC**
- 4 **GOV UK**
- 5 **DHL**



200+ Smishing/Vishing Phone Numbers



2800+ Smishing URLs, 600+ unique



9 Classes Created

13 Levels Created



3k+ unique fingerprints produced



3k+ smishing attacks indexed

BRANDS NEVER
IMPERSONATED

These brands despite being popular were never impersonated in any smishing attacks -

- 1 **Ocado**
- 2 **Deliveroo**
- 3 **ASOS**
- 4 **Admiral**
- 5 **Starling Bank**

Research
KEY FINDINGS








KEY FINDINGS:

- 99% of smishing attacks were in English Language, with only a very small proportion in other foreign languages
- Amongst the top 10 most impersonated organisations were - Hermes, Apple and the Government



CLASSES: To better understand smishing attacks, classes were created to categorise the techniques that bad actors were using in smishing attacks. Smishing datasets were labelled accordingly and further statistical analysis was carried out on the smishing datasets.

As a new attack analysis model was developed, attacks were grouped into 9 various classes - based on the techniques detected in the smishing message.

SMISHING ATTACK - CLASSES								
A	B	C	E	F	M	U	Y	Z
							REPLY Y	REPLY YES
URL ONLY	URL & MONEYTARY DATA	PHONE NUMBER	EMAIL ADDRESS	FOREIGN LANGUAGE	MULTIPLE FRAUD DATA POINTS	UNKNOWN OBSCURE UNDEFINED	SINGLE CHARACTER REPLY	SINGLE WORD REPLY

Research
KEY FINDINGS



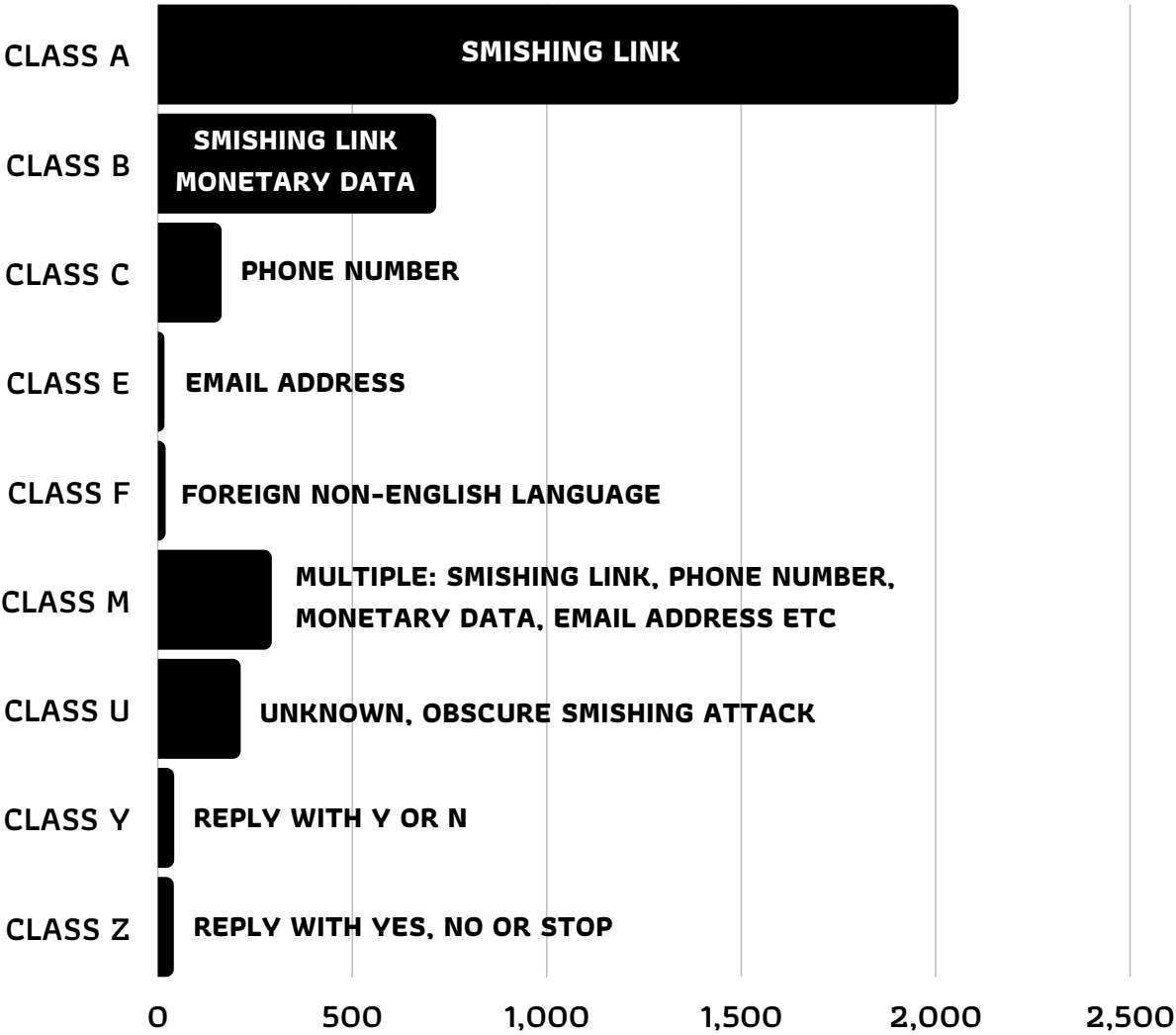
- KEY FINDINGS:**
- Nearly 80% of the attacks were Class A & B attacks - containing a smishing URL
 - Around 5% of the attacks were vishing-linked, containing phone numbers only

ATTACK LABELLING -
1. CLASSES |

The chart below summarises the historical smishing attacks analysed by our Threat Intelligence Research Team. The class feature of smishing attacks created by our technology team is closely linked to the technique bad actors are using to carry out smishing attacks. This page presents a summary of our findings.

CLASS A - 58.0%, CLASS B - 20.1%,
CLASS C - 4.6%, CLASS E - 0.4%,
CLASS F - 0.5%, CLASS M - 8.2%,
CLASS U - 5.9%, CLASS Y - 1.1%,
CLASS Z - 1.1%

ATTACK CLASSES
CLASS A - 58.0%
CLASS B - 20.1%
CLASS C - 4.6%
CLASS E - 0.4%
CLASS F - 0.5%
CLASS M - 8.2%
CLASS U - 5.9%
CLASS Y - 1.1%
CLASS Z - 1.1%



ATTACK TYPE	DESCRIPTION	EXAMPLE
CLASS A	This class of smishing data only contains a smishing link . Together with some text, but NO fee or fine.	NHS: We have identified that your are eligible to apply for your vaccine. For more information and to apply, follow here : uk-application-form.com
CLASS B	This class of smishing data not only contains smishing links , together with some text, but also contain some monetary data - e.g. a fee, amount or fine.	Royal Mail: Your Package Has A £2.99 Unpaid Shipping Fee, If You Do Not Pay This Your Package Will Be Returned To Sender, http://redelivery-settlement-fees.com
CLASS C	This class of smishing data only contains phone numbers , together with some text.	Hello. We're TSB We have noticed unusual activity on your account. Please call TSB fraud prevention on 03333350175 (UK) or +44(0)3333350175 (abroad).
CLASS E	This class of smishing data only contains an email address . Together with some text.	
CLASS F	This class of smishing data is worded in a foreign non-english language. Such as french, polish, spanish etc.	
CLASS M	This class of smishing data contains a combination of multiple parameters - at least two (e.g. a link, a fee to pay, a phone number or an email address). Together with some text.	
CLASS U	This class of smishing data is unknown , hard to define or incredibly complex due to various reasons. For example, the message may contain a valid link but may make false claims.	We would like to inform you that you have been recorded as leaving your home on 3 occasions yesterday. A fine of £35 has been added to your gov.uk account. For further information please visit gov.uk/coronavirus-penalty-payment-tracking . Protect the NHS. Save lives.
CLASS Y	This class of smishing data only contains an encouragement to reply with a one character response, such as reply with - Y . Together with some text.	Tide Bank Fraud Alert: We need to verify an online transaction of £189.93 to Argos on 11/02 at 16:05 . Reply "Y" if you authorised the transactions or "N" if you did not.
CLASS Z	This class of smishing data only contains an encouragement to reply with a one word response, such as reply with - YES or STOP . Together with some text.	

LEVELS: Attack levels were modelled to classify the category of impersonated organisations that bad actors were using in smishing attacks. Smishing datasets were labelled accordingly and further statistical analysis was carried out on the smishing datasets.

Attacks were grouped into 13 various levels or types of organisations.

BANK	B	SMISHING ATTACK - LEVELS
DIGITAL SERVICES	D	
FINANCIAL SERVICES	F	
GOVERNMENT	G	
HOUSEHOLD/RELATIVE	H	
MULTIPLE ORGANISATIONS	M	
PARCEL DELIVERY	P	
RETAILER	R	
SUPERMARKET	S	
TELECOMS COMPANY	T	
UNKNOWN	U	
VARIETY (APPS, SERVICES)	V	
STREAMING	X	

Research
KEY FINDINGS

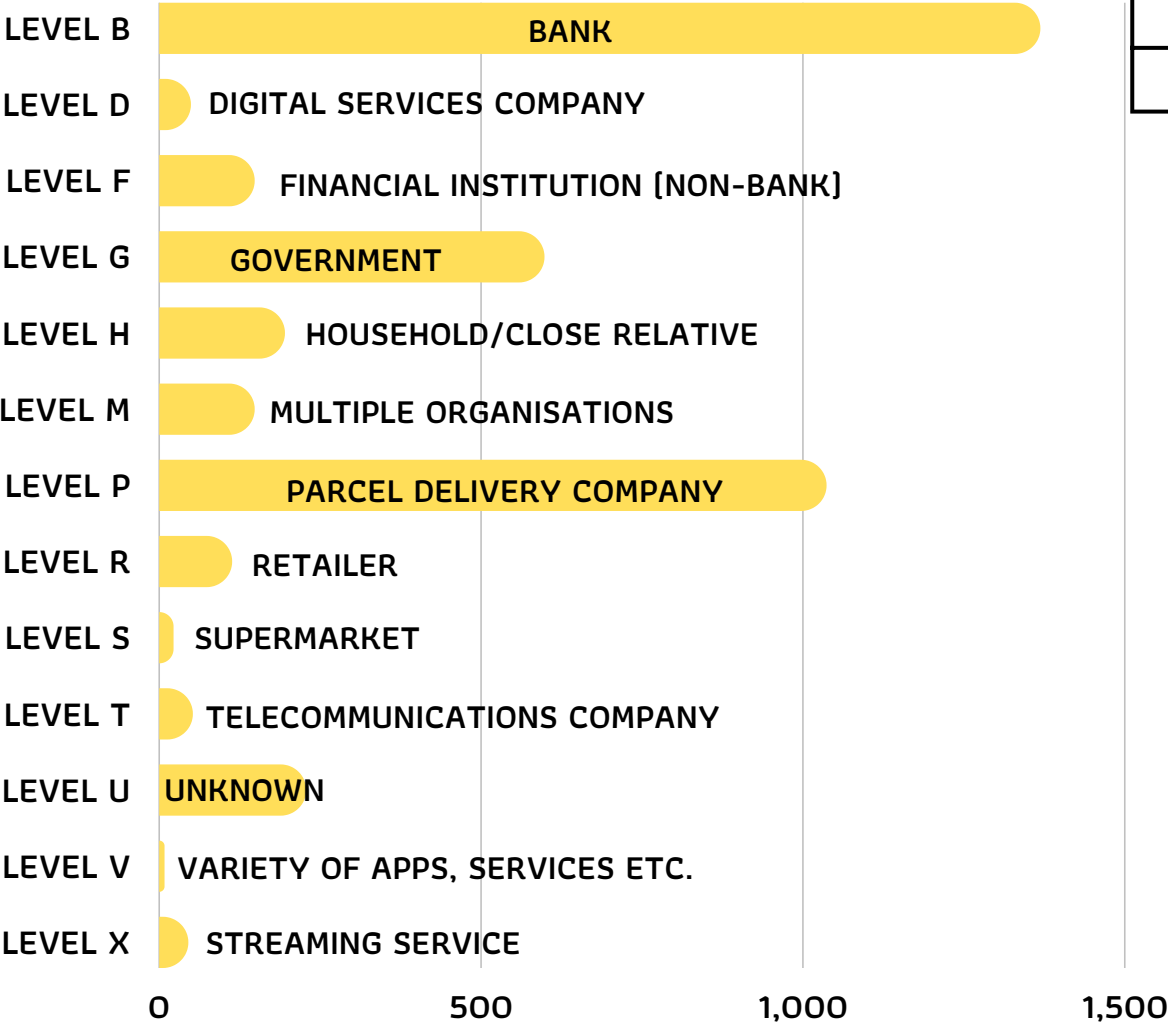


- KEY FINDINGS:**
- Around 81% of the attacks were Class A, B & M attacks - containing a smishing URL
 - Around 5% of the attacks were vishing-linked, containing phone numbers only

ATTACK LABELLING -
2. LEVELS |

The chart below summarises the historical smishing attacks analysed by our Threat Intelligence Research Team. The level feature of smishing attacks represents the type of organisation bad actors are impersonating. After analysing these attacks, this page presents a summary of our findings -

- 39% of historical attacks impersonated a Bank (Level B), closely followed by Parcel Delivery companies (26% - Level P) and Government (16% - Level G).
- Current trends indicate that smishing attacks impersonating a Parcel Delivery company (Level P) are the most popular type of attack.

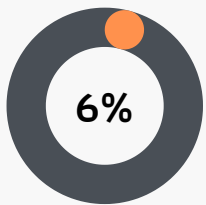


ATTACK LEVELS
LEVEL B - 39.4%
LEVEL D - 1.8%
LEVEL F - 2.9%
LEVEL G - 16.3%
LEVEL H - 0.8%
LEVEL M - 1.8%
LEVEL P - 26.3%
LEVEL R - 3.0%
LEVEL S - 0.6%
LEVEL T - 2.5%
LEVEL U - 2.7%
LEVEL V - 1.4%
LEVEL X - 0.5%

ATTACK TYPE	DESCRIPTION
LEVEL B	Smishing attacks at this level impersonates a bank .
LEVEL D	Smishing attacks at this level impersonates a digital services company .
LEVEL F	Smishing attacks at this level impersonates a financial institution that's not a bank.
LEVEL H	Smishing attacks at this level impersonates a family member or someone pretending to be from the recipient's household or close family connections – such as mum, dad, daughter, uncle, auntie, son, cousin etc.
LEVEL G	At this level, smishing attacks impersonates a governmental organisation .
LEVEL P	This level of smishing attack is impersonating a parcel delivery company or a courier company.
LEVEL R	Smishing attacks at this level impersonates a retailer .
LEVEL S	Smishing attacks at this level impersonates a supermarket .
LEVEL T	Smishing attacks at this level impersonates a telecommunications company or provider of communication services .
LEVEL U	Smishing attacks at this level are unknown , obscure or incredibly complex.
LEVEL V	Smishing attacks at this level impersonates a variety of other apps, services etc. such as travel apps, restaurant apps, food apps, education, dating, fitness.
LEVEL X	Smishing attacks at this level impersonates a streaming service .

Insight into UK Smishing Attacks

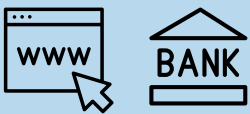
Despite the increase in Smishing in recent years, majority of consumers are not fully aware of the reporting channels in the UK. It is estimated that millions of these attacks occur in the UK every year, risk drivers have made these attacks more plausible.



The most sophisticated type of smishing attack - Class U.



71% of people (around 45 million) in the UK were targeted by smishing attacks in 2021.



Historically: The most popular type of smishing attack (35%) is - Class A, Level B.

RISK DRIVERS - SMISHING UK

300+ 4.9k+

Banks

Bank branches closed since 2015



97%
of the population in the UK have a Bank Account

LEVEL B

4.2BN

Parcels sent in 2021

£119BN

Online retail sales in 2021, 129% increase from 2015.

LEVEL P

12.2M

Customers required to submit self-assessment tax return in 2020-2021 tax year



40M+
Licensed vehicles in the UK

LEVEL G

SMS has historically proven to have a wide reach combined with an extremely high open rate, industry statistics show that over 95% of text messages are opened within 15 minutes. Retailers, Banks, and Delivery companies all heavily rely on text messages to share updates with consumers.

Due to the increase in cyber-fraud globally and the volume of messages (estimated 48 billion SMS/MMS sent in 2020 in the UK), business-to-consumer communication channels are at risk – particularly via SMS. Our research has shown that smishing attacks originating from bad actors are very sophisticated and have become more convincing than ever. Consequently, much can be done to further develop, improve and strengthen threat intelligence capabilities around smishing.

A holistic cross-industry approach is required to be able to not only tackle fraud, but to accurately detect and report fraud around smishing quickly. This includes an urgent need to closely monitor the connection between smishing, vishing and phishing.

STRENGTHENING SMISHING THREAT INTELLIGENCE

For every smishing attack in the UK: More can be done within cybersecurity to provide comprehensive answers to important questions such as - what, when, where, who, whom, which, whose, how and why.

Anti-Fraud: This term refers to the collection of strategies, technology and know-how used to prevent and stop fraud.

Fraud: This is when trickery or deceit is used to gain a dishonest advantage. Fraud is usually used to gain financial benefits.

MMS: Multimedia Messaging Service, this type of message contains some multimedia content such as pictures, audio and video to a mobile phone.

SMS: Short Message Service, this service enables text messages to be sent to a mobile phone.

Smishing: This is a type of attack via text message where a bad actor impersonating a legitimate organisation or claiming to be another person, typically tries to trick a person.

**Contact us to learn about our
anti-fraud smishing products.**

contact@porgiesoft.com

ACKNOWLEDGEMENTS:

Report written by George Brown, Chief Executive Officer and Chief Technology Officer. Contributions from Chloe Mann – Project Manager, Gina Ojaokomo – VP Threat Intelligence. Additional support from Global Threat Intelligence team.

Published by PORGiESOFT LTD
July 2022

DISCLAIMER:

All the information included in this report has been provided in good faith. However, while every effort has been made to ensure that all the information contained or referenced in this report is comprehensive, verified, accurate, thorough and complete – PORGiESOFT LTD does not accept any liability whatsoever for any omissions or incomplete statements. This disclaimer applies to this report and (wherever applicable) to all other source reports, statistics or studies by other organisations that have been referenced.

Get cyber-fraud insights in two clicks...

WWW.PORGIESOFT.COM

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



www.porgiesoft.com