Securitas Intelligence Unit

Smishing scams

9 September 2021

Intelligence@securitas.uk.com

This report is subject to GDPR and data retention policies in line with such regulations.

Securitas provides the intelligence reports for the recipient's business internal use. Securitas accepts no responsibility for any decisions taken by the recipient on the basis of the analysis offered in this report. Use of Securitas' name, brand names, logos, taglines, slogans, or other trademarks without written permission is strictly prohibited. Disclosing, copying, distributing or use of any part of the reports electronically or otherwise other than for the strict purpose for which it has been provided is strictly prohibited. Securitas Security Services (UK) Limited is a limited company registered in England & Wales. Registered number: 01146486. Registered Office: St James House, 13 Kensington Square, London, W8 5HD © Securitas Security Services (UK) Limited 2018.

Priority Intelligence

- **SMS text message scams – known as ‘smishing’ – have increased throughout 2021.**
- **Smishing messages are becoming increasingly sophisticated and credible, making them harder to identify.**
- **Scammers are opportunistic and will use real-world events as a means to target their operations.**
- **Tactics and techniques used by scammers have evolved, with new technologies allowing them to target more potential victims than ever.**
- **The Securitas Intelligence Unit assesses with HIGH CONFIDENCE that the threat posed by smishing will continue for the foreseeable future, despite attempts by law enforcement to disrupt criminal operations, with scammers continuing to exploit real world events to target potential victims.**

Background

SMS text scams, known as ‘smishing’ (SMS Phishing), is a specific form of phishing whereby a scammer sends an SMS text message with the intention of deceiving the recipient into providing their personal details via a direct reply or enclosed link (i.e. visiting a malicious website), or alternatively, downloading a Trojan horse, virus, or other malware onto the receiving device.

These types of scams have been part of the scammer’s repertoire for many years, originally evolving from phishing emails. However, the number of different scams, their credibility, and the number of scammers operating them has increased significantly throughout 2020 and early 2021, in particular leveraging COVID-19 to target the general public.

The COVID-19 pandemic and ensuing lockdowns has resulted in a significant increase in online activity. Criminals, both domestic and global, have taken advantage of this situation by exploiting increased social media usage, increased online shopping, COVID-19 related financial support (i.e. furlough, grants, loans), self-isolation notifications, and the vaccination rollout. This includes smishing campaigns deliberately designed to target those who may be expecting deliveries or COVID-19 related health alerts.

According to research, over half of British people (53%~) have been targeted by scams since lockdown began, with almost a third having fallen victim. Advancements in technology now allow for legitimate businesses (and by extension scammers) to send upwards of 30,000 texts per minute, with the average person expected to receive 4 automated text messages per week.

SMS text scams are among the most prevalent scams in the UK, with the average age of victims being under 35 years of age. However, as people are spending more time indoors, and mobile phone usage has increased, the 45+ age group has been increasingly at risk.

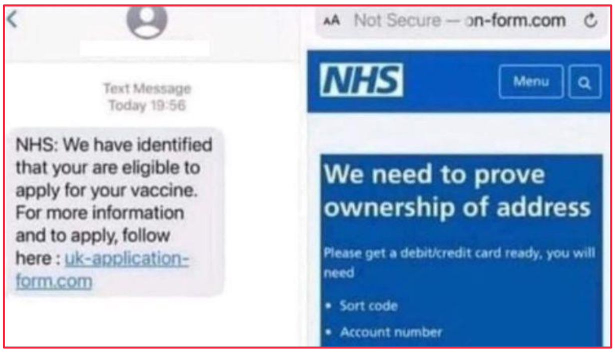
Smishing is not exclusive to the UK, with scammers targeting victims worldwide. For instance, a European manufactured malware named ‘Flubot’ is actively targeting members of the public in Australia. Typically targeting Android users, a scam text message notifies the user of a new voicemail requiring the user to download an external app via a phishing link. By pressing the link, the app is downloaded giving the scammer(s) access to personal and payment details. Scamming in Australia, including smishing, has resulted in an unprecedented number of victims totalling nearly AU$32 million lost (£16 million).

Situation in detail

COVID-19 scams

Scammers have preyed on changing procedures and communication methods, targeting victims with COVID-19-related scams including fake COVID-19 updates, offering paid for vaccines, directing people to fake vaccine booking sites and / or fake test and trace messages.

All of these are designed to take advantage of the current pandemic and encourage people to press the link embedded within the text.



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

We need to prove ownership of address

Please get a debit/credit card ready, you will need

- Sort code
- Account number

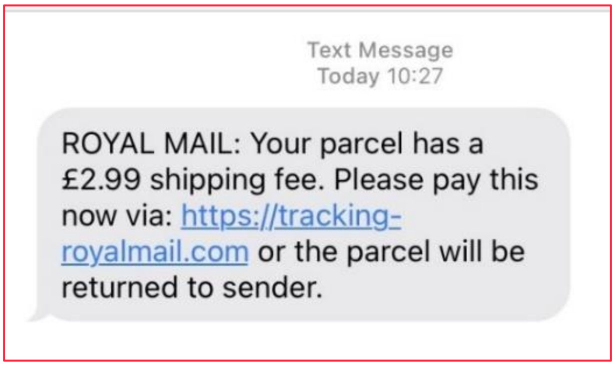
The link will typically take the victim to a fake version of a trusted website, designed to look authentic with relevant logos and wording that has been created to harvest as much personal information as possible. This may include, but not limited to, usernames / passwords, bank details and mother's maiden name – information that victims would ordinarily expect to input to access genuine sites. The use for this information can vary, ranging from directly stealing from a victim's bank account, to applying for credit cards and loans using the victim's details, or even selling stolen details via the Dark Web.

Delivery scams

One of the fastest-rising and most-reported scams involves the victim receiving a text purporting to be from delivery companies such as Royal Mail, DPD, Yodel or similar courier companies, requesting payment for shipping fees, or to prevent a parcel being returned to the sender.

Whilst this scam has existed for some time, 2020 saw an increase of more than 1,000% on previous figures, with that figure further increasing by a factor of 6 during the first half of 2021. The increase in activity is due to the increased success of these scams, likely due to the rise in online shopping during the period coinciding with genuine extra fees being applied to EU imports following Brexit.

The texts use specific wording that is designed to install a sense of urgency and cause people to click the link to avoid missing a delivery or incurring further charges.



Text Message
Today 10:27

ROYAL MAIL: Your parcel has a £2.99 shipping fee. Please pay this now via: https://tracking-royalmail.com or the parcel will be returned to sender.

'Recovery' scams

Another recent tactic being employed is recovery fraud in combination with a smishing or phishing attack. After initially paying the 'fee' or otherwise entering details to secure the release of the package, the scammer will then call the victim posing as their bank and informing them that they have been scammed and their bank account has been compromised. The 'bank' will suggest transferring funds to a 'safe' account, which the scammers will allegedly be unable to access. Unbeknownst to the victim, the scammers own the 'safe' account, and the victim will have transferred all of their funds directly to the scammers.

Other examples of smishing scams

WhatsApp fraudulent friend – The victim receives a text message including a 6-digit WhatsApp code. A scammer posing as a friend will then message the victim to say they are trying to log into WhatsApp and have accidentally sent the victim their access code. They will ask the victim to follow steps to gain the code, screenshot it and return the code to the scammer.

In reality, the victim is sending the scammer their own code, giving the scammer access to their WhatsApp account where they will likely ask contacts to send money.

Scam calls – Albeit not an explicit smishing scam the national Fraud Intelligence Bureau (NFIB) is warning individuals of calls from numbers similar to their own, with the first 7 digits matching the victims. The calls impersonate government organisations or law enforcement agencies, asking the recipient to "press 1" to speak to an advisor, or police officer, about unpaid fines or police warrants.

These have also been reported on messaging apps such as WhatsApp.

Government and law enforcement agencies will not notify you about unpaid fines or outstanding police warrants by calling or texting. Do not respond to any calls or texts about these.

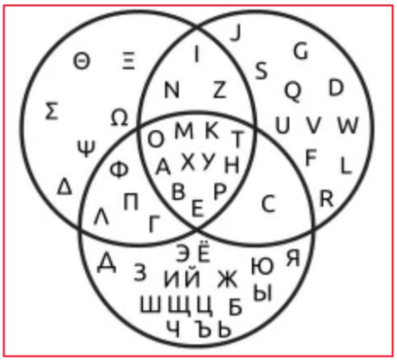
Homograph attacks

Amidst the increase in phishing and smishing activity, there has been an increase in malicious actors using characters that look alike to deceive victims into clicking malicious links.

Examples of this include using capitalised letters, such as in the Royal Mail scam:

- **Legitimate:** royalmail.com
- **Swapped characters:** royaimaii.com
- **Swapped characters capitalised:** royaIrnail.com

Another example includes using characters from other scripts, such as Cyrillic.



The venn diagram depicts an example of the intertwining characters found in the Greek, Latin and Cryllic alphabets.

Examples of this include swapping Latin characters with Cyrillic or Greek alphabet characters:

- **Legitimate:** bank.com
- **Swapped latin ‘a’ for cyrrilic ‘a’:** bank.com

This type of attack is called an IDN homograph attack, or script spoofing.

Registering a homographic domain name can be considered a form of typosquatting, as both tactics utilise deception to pose as legitimate websites to trick victims into accessing the site.

SIU Comment: However, whereas typosquatting exploits common mistakes (such as misspelling or incorrect domain i.e. .com vs .org) which has a greater chance of opportunistic success, homograph spoofing is more targeted, but unlikely to achieve opportunistic success from someone entering a cyrillic character as opposed to a latin character when entering a website url.

The venn diagram image provides an example of characters (homoglyphs) within the Cyrillic, Latin and Greek alphabets that may be exploited in homograph attacks.

A homograph attack uses a combination of characters orginating from different scripts, such as Latin, Greek and Cyrillic scripts, to deceive a potential vicitim into accessing a fraudulent website.

In other words, by manipulating the various characters of a URL, for example replacing a latin ‘a’ with a cryllic ‘a’ a scammer could mirror an official website and proceed to successfully scam the vicitim. End.

Advisory

Online fraud remains a challenge to police and law enforcement, and smishing is no different. Though enforcement agencies have had some success, notably with the arrest of 8 people linked to a series of Royal Mail smishing scams in May 2021, progress is limited in comparison to the volume of fraud taking place. Police and national agencies continue to work with the National Cyber Security Centre to take down the websites behind the frauds, however with many of these sites being registered outside of the UK, options for dealing with these websites can be limited, with a recent study finding that one domain hosting service was hosting over 200 separate websites designed to impersonate Royal Mail.

The more specific targeting of smishing attacks (such as basing its spoofing targets in areas that are likely to see high traffic and genuine reasons for SMS contact), plus the lower volume of attacks in comparison to email phishing means that victims are more likely to mistake a smishing attack for the real thing. Awareness of the increasing prevalence of SMS scams and care in checking the authenticity of any links prior to clicking them is key. If in any doubt, the user should visit websites directly (rather than following the links) and check any reference numbers or codes independently.

Standard phishing awareness advice applies equally to smishing messages, and users should check the following on receipt of any message asking them to click a link or enter details:

- Are they expecting the message? If it’s a delivery message, have they ordered anything lately? Have they had messages from this provider before, and have they been from this number?
- Does the message provide any specific detail unique to them such as their name, address, or customer number? Is this information correct?
- Does the link appear to be genuine? Check the spelling of the URL carefully. Beware of links that use lots of hyphens such as:
    - COVID19-NHS-vaccine.co.uk
    - Royal-maildelivery.net
    - DPD-missed-delivery.com
- Is the message attempting to place time pressure on the user?

If in any doubt, users should NOT click the link and should instead report the message by forwarding it to the relevant authorities. A free of charge worldwide spam investigating service allows users to forward suspicious texts to 7726 (spelling SPAM on phone keypads). The text is forwarded to a centralised security centre system enabling authorities to track and take action against spam operations.

If a user has clicked the link and has come to the realisation that the link was fraudulent the user should factory reset the device as well as updating all passwords used to access different apps on the device. The factory reset will remove all data unless backup mechanisms are in place, however, users should be mindful when asked to restore certain backups the data may be infected / compromised and is therefore recommended to not restore from any backups after the infection.

Intelligence assessment

The Securitas Intelligence Unit assesses with HIGH CONFIDENCE that the threat posed by smishing will continue for the foreseeable future, despite attempts by law enforcement to disrupt criminal operations, with scammers continuing to exploit real world events to target potential victims.

Smishing has seen an increase in uptake due to the ever-present nature of mobile phones in people's daily lives – a 2020 study found that SMS messages have an 'open' rate (where a message will be opened and read by the recipient) of over 98%, as opposed to around 20% for email. This increased visibility, as well as the more targeted nature of messages is leading to more people falling victim to these scams. This means the efficiency of smishing scams dramatically outweighs that of traditional email phishing. The SIU assesses with HIGH CONFIDENCE that as long as this remains the case, smishing will continue to grow in both volume of messages and sophistication of attacks.

The recent upsurge in smishing scams has triggered questions from some experts around the suitability of SMS messaging for official communication from businesses and governments due to the lack of security and verification tools in the system, and the ease with which criminals can impersonate legitimate entities. However, due to the lack of a suitable alternative and the prevalence of mobile phones making them a key tool for contacting large groups of people simultaneously, it is unlikely that the platform will be dropped for official use in the near future.

With people increasingly using their phones whilst multitasking or travelling, it may only take a brief lapse in attention or concentration for an error to occur. The increasing sophistication involved in these scams, as well as an increase in governments and businesses using SMS messaging for genuine alerting means that people are increasingly being caught out by these scams.

As with regular phishing attacks, awareness and alertness are key to avoiding falling victim to these scams, and businesses are encouraged to educate their employees on the dangers of smishing due to the risk of personal details such as passwords becoming compromised, as many individuals will use a small number of passwords for both personal and work accounts.

Intelligence Cut Off Date (ICOD):	2359hrs, 8 September 2021.

LANGUAGE OF PROBABILITY							
Term:	Remote	Highly unlikely	Unlikely	Realistic / Possible	Likely / Probable	Highly likely	Almost certain
Probability:	0-4%	10-20%	25-35%	40-50%	55-75%	80-90%	95-99%