TMT Client Alert
Singapore

Client Alert

2022年 2月

For more information, please contact:

Ken Chia
Principal
+65 6434 2558
ken.chia@bakermckenzie.com

Andy Leck
Principal
+65 6434 2525
andy.leck@bakermckenzie.com

Ren Jun Lim
Principal
+65 6434 2721
ren.jun.lim@bakermckenzie.com

Stephanie Magnus
Principal
+65 6434 2672
stephanie.magnus@bakermckenzie.com

Daryl Seetoh
Senior Associate
+65 6434 2257
daryl.seetoh@bakermckenzie.com

Alex Toh
Senior Associate
+65 6434 2783
alex.toh@bakermckenzie.com

日本語でのお問い合わせは、井上まで:

Yoko Inoue (井上 洋子)
+65 6434 2605
yoko.inoue@bakermckenzie.com

シンガポール：SMS フィッシング詐欺取締り対策の導入

概要

シンガポール当局は、デジタルバンク利用者を狙った SMS フィッシング詐欺が横行している最近の風潮に対し、さまざまな措置を講じて対処しようとしている。マルチステークホルダー・アプローチは、金融、電気通信、内政の各部門を監督する複数の政府機関と、シンガポール銀行協会（ABS）等の業界団体が関与するアプローチである。

最近の主要な展開をいくつか以下に掲げる。

重要なポイント

- シンガポール金融管理局（MAS）および ABS は、シンガポールの金融機関のために従来以上に堅牢な措置を導入・実施することにより、デジタルバンキングのセキュリティを強化しようと考えている。
- 情報通信メディア開発庁（IMDA）は、シンガポールの電気通信事業者、金融機関、SMS 事業者（アグリゲーター）に対し、「シンガポール SMS 送信者 ID 保護登録機関」（Singapore SMS SenderID protection registry）への登録を義務付けることを検討している。
- 国家犯罪対策協議会（NCPC）と政府テクノロジー局が開発した詐欺シールドアプリも、詐欺からの保護を求める消費者が利用できる手段となる。

  MAS はこの問題に関して告知や通達をまだ発行しておらず、今後新たな情報・指針を提供する可能性がある。

詳細情報

最近の SMS フィッシング詐欺の事例

最近、特に銀行の顧客を狙った SMS フィッシング詐欺が多発している。

2020年後半には、悪意ある行為者が被害者を誘導し、SMSのワンタイムパスワード（使い捨てパスワード；略称 OTP）を利用して 50 万シンガポールドルに及ぶ詐欺的なクレジットカード取引を実行し、銀行の顧客 75 名に損害を与えた。[1]

さらに、2021 年 12 月には、シンガポールの大手金融機関の 470 名近い顧客が、SMS フィッシング詐欺により 850 万シンガポールドル以上を失っている。

最近発生した事例の大半では、以前に銀行から送られた合法的なテキストメッセージと同じスレッドに偽の SMS が表示され、OTP の入力が求められ、取引に関する注意喚起がなされていた。詐欺師たちは銀行になりすまし、送信者 ID を銀行の ID と同じものに設定し、偽のメッセージが顧客のモバイルデバイスで本物と同じスレッドに表示されるようにした。これら偽のメッセージは、顧客の銀行口座またはクレジットカードに問題が発生したと偽り、表示されたリンクをクリックするよう顧客に指示、偽のウェブサイトに誘導するか、顧客の銀行取引に関する詳細情報を要求した。

このような SMS 詐欺が成功したのは、第 1 に、偽のメッセージが以前に送られた合法的なメッセージと一緒にグルーピングされてしまったため、偽メッセージが瞬く間に本物そっくりに変身してしまうからである。第 2 に、詐欺師が発信した偽の SMS に表示された偽装リンクは、実際の URL を隠蔽するために短縮されていることが多く、被害者がリンクの信頼性をチェックするのが困難だという事情がある。第 3 に、偽のリンクによって導かれる偽の銀行ウェブサイトの方も、やはり本物そっくりに作られているからである。

SMS 詐欺の問題はシンガポールに限った話ではない。フィリピンでは、未承諾の SMS メッセージを受け取ったモバイルユーザーからの報告が国家プライバシー委員会に寄せられており、これらのユーザーは、SMS の連絡先情報に従って新型コロナに関する接触者追跡情報や健康状態申告書を提供してしまったと主張している。カナダ政府も SMS 詐欺の問題に注目することとなった。フィリピンのケースと同様、詐欺師たちが新型コロナのパンデミックを利用して儲を企て、経済的弱者であるカナダ国民を対象とした「カナダ緊急対応給付」、「カナダ復興給付金」といった支援プログラムに自分たちが参画しているかのように装って、不正な SMS を送信したからである。この件で送られたメッセージには、受け手を一見合法的なサイトに誘導するリンクが含まれており、詐欺師たちは偽装したサイトを通じてユーザーの個人データを盗んだり、モバイル用のマルウェアを仕込んだり、詐欺を働いたりすることができる。

デジタルバンキングのセキュリティ強化措置

このような事態を受けて、2022 年 1 月 19 日、MAS と ABS は、デジタルバンキングのセキュリティ強化のために一連の追加措置が今後数週間以内に導入されると発表した。シンガポールの銀行が MAS と協議の上導入する措置には、以下のが含まれている。

a. リテール顧客に送付する e メールまたは SMS からクリック可能なリンクを削除する。
b. 顧客に振込通知が送信される金額の上限を、デフォルトで 100 シンガポール以下に設定する。

c. モバイルデバイスの新たなソフトトークン（使い捨てパスワード払い出しソフト）が有効化されるまでに 12 時間以上の猶予を持たせる。
d. 顧客の携帯番号または e メールアドレスの変更請求があった場合には、常時、銀行に登録されている既存の携帯番号または e メールアドレスに当該請求を通知する。
e. 追加の安全措置（顧客の主な連絡先の詳細など、主要なアカウント情報変更に関するリクエストを実施する前にクーリングオフ期間を置く等）。
f. 十分なリソースを備えた専従の顧客支援チームを設け、詐欺の恐れのある取引に関するフィードバックを優先度に従って処理する。
g. 詐欺に関する教育をもっと頻繁に実施し、警戒を促す。

これらの措置は、偽物の SMS メッセージに含まれる偽装リンクの罠に対処するとともに、詐欺的な取引や銀行口座の不正な操作の企てがあった際に顧客に直ちに通知する可能性を高めるものである。MAS はさらに、大手金融機関の詐欺監視メカニズムが対する精査にも力を入れており、高まりつつあるオンライン詐欺の脅威に十分に対処できるよう、監視を強化している。

シンガポール SMS 送信者 ID 保護登録機関

2022 年 1 月 20 日、IMDA は、「シンガポール SMS 送信者 ID 保護登録機関」（Singapore SMS SenderID protection registry）と称する国家的な登録機関を立ち上げるという構想を発表した。IMDA は、シンガポールのすべての電気通信事業者、金融機関、SMS 事業者（アグリゲーター）に対し同機関への登録を促しており、報道によれば、近いうちに上記の企業および団体は登録を義務付けられる可能性があるという。

送信者 ID とは、数字の代わりに言葉やフレーズを表示して SMS メッセージの送信者の特定を可能にするものである。詐欺師たちが登録済みの送信者 ID を用いてメッセージ送信を試みると、その ID を登録している組織は、それらメッセージのブロックを選択して送信を阻止することができる。これにより、詐欺師が銀行その他の組織になりすますことは妨げられる。ID 登録は、最近起こったインシデントのほとんどに見受けられる状況に的を絞った対策である。

「シンガポール SMS 送信者 ID 保護登録機関」は、昨年 8 月から試行段階に入っており、OCBC 銀行、ラザダグループ、シンガポールポストなどの大手事業者が既に登録を済ませていると報じられている。

だが、SMS を全く使わず、その代わりに独自のアプリ、ポータル、ウェブサイトを利用して顧客にメッセージを伝えるというアプローチの方が銀行にとって有益である、と専門家らは主張している。特に、ID を登録しても不正操作を行う余地はまだ残されている（たとえば、詐欺師たちが「"Bank"」を「""」に代えるなどの方法で送信者 ID を少しだけ変えるのは簡単なことだ）という現実を考えれば、こうした専門家の主張

は正鵠を射ている。

さらに、登録機関が成功を収めるか否かは、上記の事業者や団体が参加するか否かにかかっている。登録の義務化を希望するオンライン請願書に 2,100 人を超える人々の署名が集まってはいるが、登録はまだ義務づけられていない。

ID 登録以外の IMDA の構想には、なりすましに使われる番号や国際電話の接頭番号の付いた番号をブロックして「+」の文字を表示し、それが詐欺目的の電話である可能性があることを公衆に警告する、というものもある。

詐欺防止

もう一つの保護手段として、詐欺防止アプリ「Scam Shield app」がある。これは、国家犯罪対策協議会（NCPC）と政府テクノロジー局の 1 ユニットであるオープン・ガバメント・プロダクツ・チームが共同で開発したアプリである。このアプリは、人工知能を用いて詐欺的なメッセージをふるい分けるものであるが、それと同時に、ユーザーが報告した番号や、シンガポール警察が作成したリストに記載されている番号からの電話をブロックすることもできる。アプリの提供が開始された 2020 年 11 月から 2021 年 8 月までに同アプリがブロックした電話番号はおよそ 8,600 件に達しており、ユーザーらは同アプリを通じて疑わしい SMS メッセージ 140 万件を報告している。

このアプリの機械学習モデルは、詐欺的なテキストの中で頻繁に使われる「貸付」（loans）、「賭け」（gambling）、「返済」（repayment）といった言葉を認識するように訓練されている。これらの語が認識されると、その語が相互的な組み合わせの中でどのように使われているかを判断する。

すべての偽メッセージをふるい分けようとする場合、このアプリが常に効果を発揮するとは言い切れない。伝聞によれば、アプリを回避する方法も存在するようである。詐欺師を見分ける唯一の手段として専らアプリのみに頼ることがないよう、ここで警鐘を鳴らしておきたい。

詐欺の脅威を根絶することは不可能であろうし、特に詐欺師たちの適応の速さを考えれば到底無理な話であるが、詐欺に遭遇しやすいオンラインバンキング利用者（少なくともその一部）に対して、詐欺師に対抗するための防壁を提供することはできるだろう。以上に挙げた措置と併せて、MAS も常に言っているように、顧客自身の用心が何よりも重要であるという事実に変わりはない。

[1] https://www.mas.gov.sg/news/media-releases/2021/sms-one-time-passwords-diverted-to-perform-fraudulent-card-payments

www.bakermckenzie.com

Baker McKenzie Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100