

法人口座を狙ったフィッシング詐欺にご注意ください

2024年12月11日
株式会社 SBI 新生銀行

警視庁から法人口座を狙ったインターネットバンキングの不正送金被害が多発しているとの注意喚起がありましたので、銀行を騙った不審なメール・電話にご注意ください。

当行は絶対に電話、メール、FAX、SMS 等のいかなる方法によってもお客さまの認証情報（ログイン ID、ログインパスワード（暗証番号）、ワンタイムパスワード等）をお伺いすることはありません。それらの提供を求められても、**絶対に回答しないでください**。なお、不審な電話、メール、FAX、SMS 等があった場合は、相手の担当者の部署・氏名等を聞いた上で、折り返し連絡するなど慎重にご対応いただくか、もしくは「ご照会窓口 SBI 新生コーポレートコールセンター（法人ご契約者さま専用）」にお問い合わせください。

【参考：発生事例】 事例詳細は（別紙）を参照ください。

- ・ 銀行を騙ったフィッシングサイトの QR コードや URL が記載された FAX やメールが送られてくる。
 - ・ 銀行担当者を名乗る者からの電話があったのでメールアドレスを伝えたところ、フィッシングメールが送られてくるようになった。
- ※ 銀行を騙った自動音声の電話がかかってくる場合や、「インターネットバンキングの電子証明の期限が切れているので、更新してもらいたい」といった内容の連絡をしてくることもあります。

犯罪者は、本物そっくりな偽サイトに誘導し、送金に必要な口座情報（ログイン ID、ログインパスワード等）を盗み取ったうえ、お客さま本人になりすまして口座から不正に送金します。万一、お客さまの認証情報（ログイン ID、ログインパスワード（暗証番号）、ワンタイムパスワード等）を回答してしまった場合は、「ご照会窓口 SBI 新生コーポレートコールセンター（法人ご契約者さま専用）」にご連絡いただき、お客さまの所在地管轄の警察署へご相談ください。

〈本件に関するお問い合わせ先〉

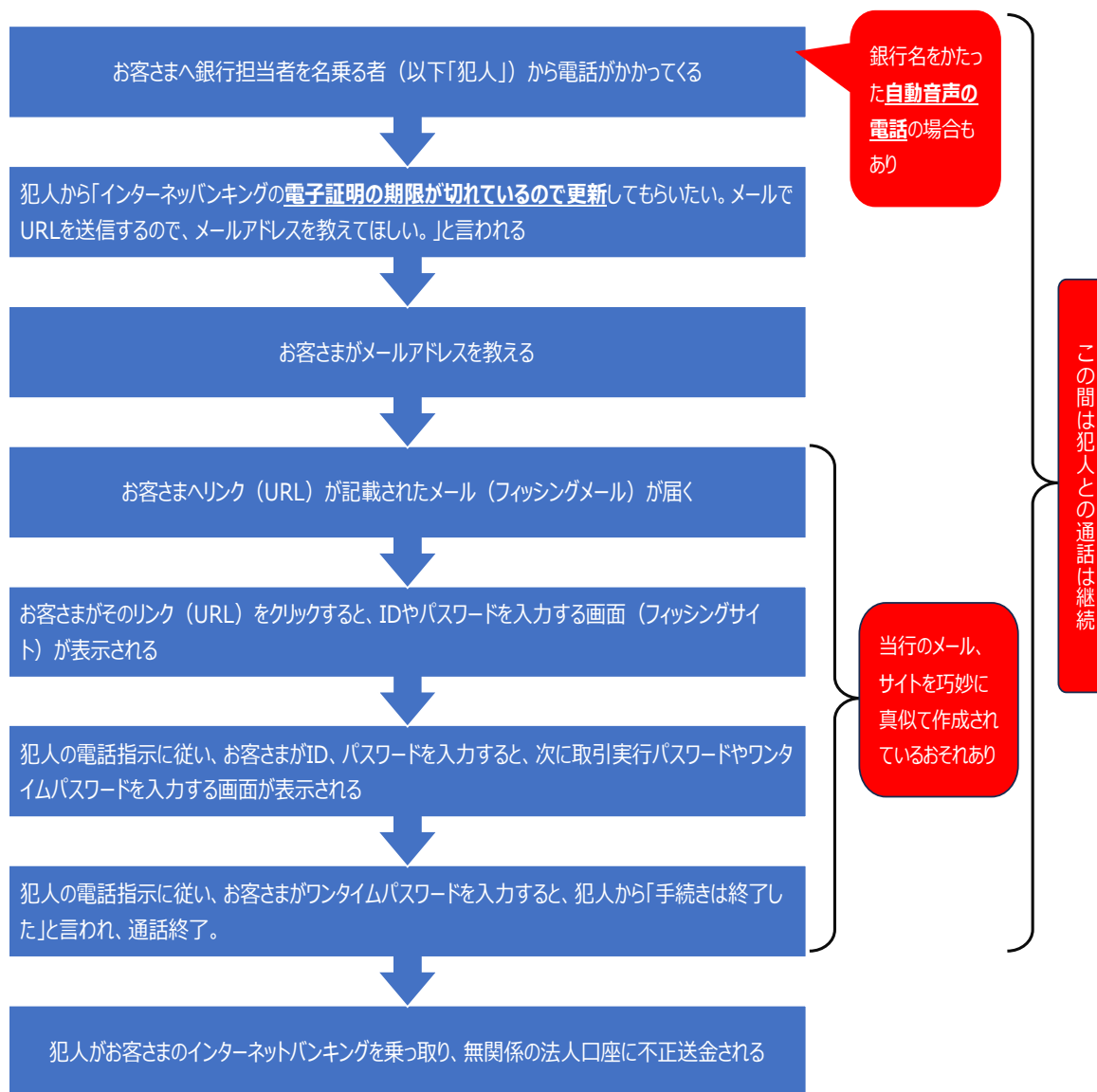
SBI 新生コーポレートコールセンター

電話番号：0120-511-025（銀行営業日 9:00～17:00）

※メニュー番号「4」をご利用ください。

(別紙)

<参考：発生事例> 警視庁通達から一部抜粋



※ 偽メール・偽サイトは本物そっくりで非常に巧妙に作られており、見分けることが非常に困難です。不審に感じたらメールに記載のURLやQRコードにはアクセスしないでください。

<こんなケースも…>

・「口座利用制限のお知らせ」という案内が送付され、それを解除するためのリンク（URL）やQRコードを合わせて送付されるケースもあるようですが、これらもフィッシング詐欺の手口の一つです。