各位

2024 年 12 月 6 日

三井住友信託銀行株式会社

**法人のお客さま向けインターネットバンキングを狙ったフィッシング詐欺にご注意ください**

国内において法人のお客さま向けインターネットバンキングを狙ったフィッシング詐欺が多発しております。銀行を騙った不審なメール・電話にご注意くださいますようお願いいたします。なお、「三井住友信託ビジネスダイレクト」などの法人のお客さま向けインターネットバンキングのご利用にあたり、当社からお客さまあてにお電話でメールアドレスなどをお尋ねすることはございません。

- 銀行担当者を騙った人物から不審な電話があった際は、受電内容(部署名・氏名など)を控えたうえで、当社お取引店・担当店部あてにご連絡ください。なお、当社連絡先がご不明な場合は当社ホームページなどでご確認いただくなど、慎重にご対応いただけますようお願い申し上げます。
- 不審な受信メールなどに記載されているリンクをクリックしたり、QR コードを読み取ったりすることで、フィッシングサイトに誘導されるおそれがございますので十分にご注意ください。
- 万一、身に覚えのないお取引が発生してしまったときは最寄りの警察署、お振込み先の口座がある銀行にご連絡ください。あわせて、当社のお取引店・ご担当店部(平日(祝日などを除く)9:00～17:00)または三井住友信託ビジネスダイレクトヘルプデスク(電話 0120-050-791 同 9:00～19:00)にもご相談ください。

＜ご参考:発生事例＞

銀行担当者を騙る人物から一般企業に電話連絡があった後、フィッシングメールが送られてくる事例

① 一般企業(以下、「企業」という)に銀行担当者を騙る人物(以下「犯人」という)から電話がかかってきた(先立って銀行名を騙った自動音声の電話がかかってくる場合もあり)。
② 犯人から「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。これからメールで URL を送信するので、メールアドレスを教えてほしい。」と言われたので、企業の担当者は犯人にメールアドレスを教えた。
③ その後、企業の担当者宛てにリンクが書かれたメール(フィッシングメール)が届いた(犯人との通話は継続している状態)。
④ 企業の担当者がそのメールに書かれたリンクをクリックすると、正規のインターネットバンキングの画面ではない、ID やパスワードを入力する画面(フィッシングサイト)が表示された。
⑤ 犯人の電話指示に従い、企業の担当者が契約者番号・ID・パスワードを入力すると、次に取引実行パスワードやワンタイムパスワードを入力する画面が表示された。
⑥ さらに犯人の電話指示に従い、企業の担当者がワンタイムパスワードを入力すると、犯人から「手続きは終了した。」と言われ、通話を終えた。
⑦ その後、企業の担当者が企業の口座残高を確認すると、企業と全く無関係の法人口座へ資金が不正送金されていることが判明した。