群馬県警察 Gunma Prefectural Police

サイバーポリスニュース

注意！ 不正送金被害が広がっています！

銀行等の金融機関を装ったショートメッセージ(SMS)等をきっかけとしたインターネットバンキング不正送金事案が全国的に広がっており、県内でも被害が発生しています。ユーザＩＤやパスワードをだまし取られないように、SMSやメールのリンクを安易に開かないようにしましょう。

インターネットバンキング不正送金被害の主な手口

①金融機関等を装って、「不正利用のおそれ」などの文言が入ったSMS等が届く
②SMS等に記載されているリンクを開くと、偽の金融機関のインターネットバンキングログイン画面が表示される
（リンクの文字列は、正規サイトに似せたものが使われることが多いほか、偽のログイン画面も本物そっくりに作られている）
③ユーザIDやパスワードの入力を求められるほか、ワンタイムパスワードの入力を求められることもある

偽画面にユーザID等を入力してしまうと・・・

①入力したユーザＩＤ等が犯罪者の手に渡ってしまう
②インターネットバンキングに不正ログインされ、多額の送金をされてしまう

金融機関を装った偽SMSの一例

【○○銀行】お客様がご利用の口座が不正利用されている可能性があります。口座一時利用停止、再開手続はこちら。
https://○○○○-bank.com

【重要】：お客様の【○○銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定してください。https://×××××.com

対策

○手続を促すSMSを受信した際は、金融機関の問合せ窓口へ確認するなどして、SMSの真偽を確認しましょう
○金融機関が推奨するウイルス対策ソフトウェア等を導入しましょう
○多額の不正送金を防ぐため、一日の送金限度額は可能な範囲で低くしましょう
○手口が巧妙化しているため、多段階認証を過信することなく、公式サイトであるかどうかを常に確認しましょう
○金融機関の偽サイトにユーザID等を入力してしまったら、気付いた時点で早急に金融機関に連絡して、送金停止や一時利用停止を申し出ましょう

被害に関する相談は「サイバー犯罪情報・被害相談専用電話」又は最寄りの警察署へ

▼サイバー犯罪情報・被害相談専用電話▼
０８０－２３５０－０００１（平日午前８時30分から午後５時15分まで）

群馬県警察本部生活安全部サイバー犯罪対策課