ゆうちょ銀行をかたるフィッシングメール

　ゆうちょ銀行をかたるフィッシングメールの本文に記載されたリンク先から偽のゆうちょ銀行のウェブサイトへアクセスさせ、「ゆうちょダイレクト」のIDとパスワードを入力させて、インターネットバンキング口座から預貯金を別口座へ不正送金する手口の犯罪が流行しています。

ゆうちょ銀行をかたるフィッシングメールの特徴

差出人: 【ゆうちょ銀行】<information@jp-bank.japanpost.jp>
送信日時: 2020年6月5日金曜日 [redacted]
宛先: [redacted]@[redacted].co.jp
件名: 「通帳アプリ」の公開再開について

新型コロナウイルス感染症に罹患された皆さま、また、感染拡大によりご不安な日常生活を過ごされている皆さまに、謹んでお見舞い申し上げます。

最近、ゆうちょ銀行はお客様の口座資金のセキュリティを高めるために、全面的にシステムのバージョンアップを行いました。すぐに口座の更新をお願いします。

こちらの URL をクリックしてください
https://www.jp-bank.japanpost.jp/opakojin/uchsokin/chopa

■ゆうちょダイレクトのセキュリティに関するお願い
ゆうちょダイレクトをより安全にご利用いただくため、
以下のセキュリティ対策の実施をお願いいたします。
●トークン（ワンタイムパスワード生成機）のご利用（無料）
●ＯＳやインストールしているソフト等は常に最新の状態で使用
●メーカーのサポート期限が経過したＯＳやソフト等は使用しない
●ウイルス対策ソフトの導入および最新の状態への更新
●不正送金対策ソフト「ＰｈｉｓｈＷａｌｌプレミアム」のご利用（無料）
■========================■

※このメールにお心当たりのない方は、至急ご連絡をお願いいたします。
ゆうちょダイレクトサポートデスク
※　現在、受付時間を短縮しております。
電話：０１２０－９９２５０４（通話料無料）
お取扱時間：平日　８時３０分２１時
土日休日　９時１７時
（１２月３１日１月３日は、９時１７時）
　ゆうちょ銀行

新型コロナに便乗
新型コロナウイルス関連のことを記載することで本物のゆうちょ銀行と思わせる手口です。

クリックしちゃ 絶対ダメ！

別リンクを埋め込み
リンク先のURLは、実在する本物のゆうちょ銀行のサイトのURLが表示されていますが、実際には別のフィッシングサイトのURLが埋め込まれています。クリックすると、本物そっくりの偽のサイトが表示され、IDやパスワードの入力を求められます。

実在する電話番号
実在するゆうちょダイレクトサポートデスクの電話番号を記載して安心させる手口です。

実在するゆうちょ銀行のメールアドレス
送信元を偽装しているため、差出人は、【ゆうちょ銀行】と表示され、実在するゆうちょ銀行のメールアドレスから送信されたように表示されます。

ゆうちょ銀行のお知らせを引用した件名
過去、ゆうちょ銀行がWebサイトで公開したお知らせ等を引用した件名となっています。

↑ゆうちょ銀行のホームページ
※今回の場合、「ゆうちょ通帳アプリ」の公開再開についてというお知らせを引用した件名

中国語フォントを使用・日本語の誤表記など
メール本文内には、日本語のメールとしては違和感のある中国語フォントが使用されています。

実施：実施　経過：経過　および：および

※特に「経」「縮」「絡」などの「糸へん」の表記に注目して下さい。
日本語の誤表記や誤字、脱字などがあれば要注意です。
8時30分21時 → 8時30分から21時 、9時17時 → 9時～17時

★フィッシングメールを見抜くポイント★

差出人が実在する組織名や個人の氏名、実在するメールアドレスだったとしても、これらは偽装することが可能です。
また、メールに記載されているリンク先が正しいURL表記だとしても別サイトに誘導するURLを埋め込むことが可能です。
本文のフォントや日本語の誤表記などで違和感を感じたらフィッシングメールと疑い、リンク先をクリックしないで下さい。
万一、リンク先をクリックしてしまっても、ID、パスワード等の個人情報は絶対に入力しないで下さい。
不審なメールが届いて困った時、また、判断に迷った時は、直ぐ警察にご相談ください。

2020年6月8日 発行

最新セキュリティ情報はこちらから

鳥取県警察本部
総合相談電話　☎　＃9110
サイバー犯罪対策課　警部補　福井 貴
☎　0857-23-0110　（内線　3424）
URL　https://www.pref.tottori.lg.jp/police/