令和２年９月８日

地　域　安　全　情　報

（ 犯罪の起きにくい社会づくりのために ）

発信者：宮崎県警察本部サイバー犯罪対策課
（代）0985-31-0110

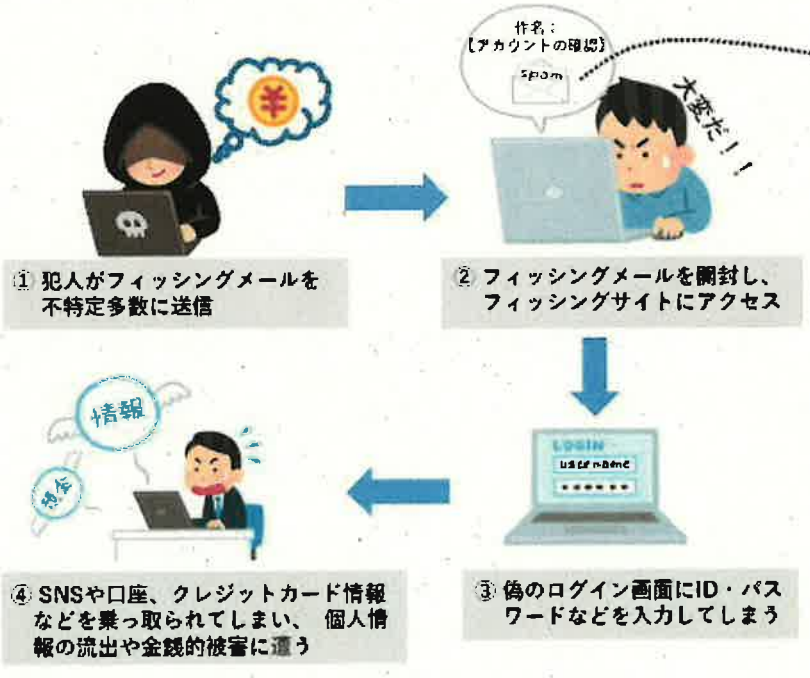
特集：フィッシング対策①

県内において、フィッシングに関する相談が非常に多く寄せられています。
そこで、フィッシング対策について特集を組み、数回に分けて解説していきます。

フィッシングとは

フィッシング(Phishing)とは、「魚を釣る(Fishing)」フィッシングのことではなく、人を騙して情報を盗み、金銭的な利益を得ようとする不正行為のことを意味します。
フィッシング被害に遭うと、インターネットバンクやショッピングサイトの登録情報が盗まれ、勝手にお金を引き出されたり、物品を購入されたりする恐れがあります。

典型的な手口



① 犯人がフィッシングメールを不特定多数に送信

② フィッシングメールを開封し、フィッシングサイトにアクセス

③ 偽のログイン画面にID・パスワードなどを入力してしまう

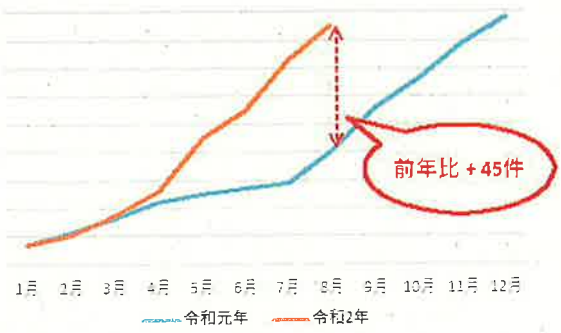
④ SNSや口座、クレジットカード情報などを乗っ取られてしまい、個人情報の流出や金銭的被害に遭う

Amazonを騙ったフィッシングメールの例

フィッシング詐欺多発中!!

県内におけるフィッシングなどによるクレジットカード犯罪に係る今年の相談受理件数は、８月末時点で前年同期に比べ、45件も増加しています。
まずは、フィッシングについて理解し、フィッシングメールに騙されないように注意して下さい。

フィッシングなどによるクレジットカード犯罪



令和２年９月15日

地　域　安　全　情　報

（ 犯罪の起きにくい社会づくりのために ）

発信者：宮崎県警察本部サイバー犯罪対策課
（代）0985-31-0110

特集：フィッシング対策②

フィッシング対策において最も重要な事は、届いたメールがフィッシングだと気づく事です。
特集第二弾では、フィッシングメール を見極めるポイントについて解説します。

フィッシングメール編

Amazonが使用する差出人メールアドレスのドメイン
（令和２年９月１４日時点、Amazon公式ページより引用）

amazon.co.jp	marketplace.amazon.co.jp
amazon.jp	m.marketplace.amazon.co.jp
amazon.com	gc.email.amazon.co.jp
amazonbusiness.jp	gc.amazon.co.jp
email.amazon.com	payments.amazon.co.jp

ポイント1　～ 基本的な情報を確認する ～

- 件名や本文に不自然な日本語が書かれていませんか？
- 差出人に、利用した覚えの無いサービスや企業の名前が書かれていませんか？
- 登録変更等を促す内容のメールの場合、あなたの氏名等が記載されていますか？

ポイント2　～ 差出人情報の偽装を見破る ～

差出人名部分をタップして送信元アドレスを確認してみましょう。
表示された送信元アドレスのドメインが、差出人名と無関係ではありませんか？

ポイント3　～ 宛先が複数の場合は注意 ～

フィッシングメールは不特定多数の人から個人情報等を盗み取る目的で送信されます。
個人情報を問い合わせるメールは、原則、本人のみに宛てられるようになっており、複数のメールアドレスが宛先となっているメールが届いた場合はフィッシングの可能性が高いです。

ポイント4　～ 公式サイトを確認しましょう ～

メールの見た目だけで判断できない場合、本文中のリンクは開かず、メール送信元企業の公式サイトをお気に入りや直接入力で開き、詐欺に関する情報の掲載がないか確認しましょう。

令和２年12月18日

地　域　安　全　情　報

（ No. ５３ ）

（ 犯罪の起きにくい社会づくりのために ）

発信者：宮崎県警察本部サイバー犯罪対策課
（代）0985-31-0110

特集：フィッシング対策③

依然として、フィッシング被害に関する相談が非常に多く寄せられています。
少しでも被害を無くす為に「フィッシング１１０番」への情報提供をお願い致します！

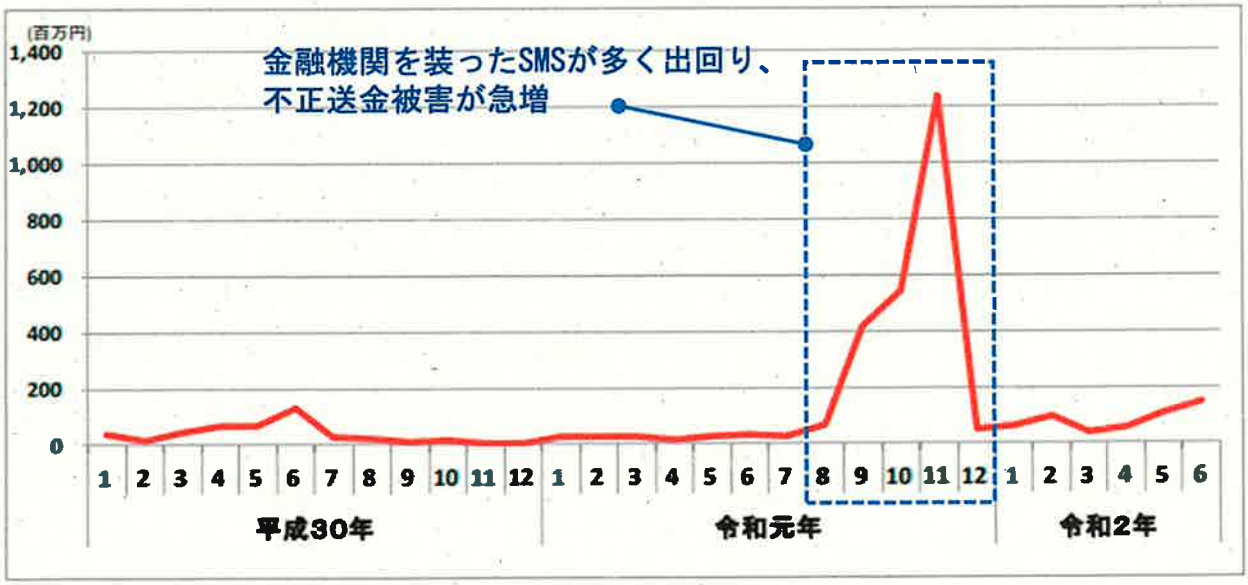
巧妙化するフィッシングの手口

フィッシングの手口は、近年どんどん巧妙化しています。

- 送信元情報を実在する企業や金融機関の実在するメールアドレスに偽装する。
- フィッシングサイトの見た目やＵＲＬを本物そっくりに偽装する。
- ＳＭＳ（ショートメッセージサービス）を送りつけて、フィッシングサイトに誘導する。

止まらないフィッシング被害

以下のグラフは不正送金事犯の被害額の推移を表したものです。
被害が急増した前年下半期と比べて、本年上半期は被害額が減少していますが、前年同期と比べると大幅に増加しており、その要因は、ＳＭＳやメールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられます。



引用：警察庁ＨＰ（ https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf ）

フィッシング110番(0985-31-0110)への情報提供をお願いします!

- フィッシングメール、フィッシングＳＭＳが届いたら．．．．
  → メールの内容、送信元情報、本文記載のＵＲＬ等を教えて下さい。
- フィッシングサイトを見つけたら．．．．
  → フィッシングサイトのＵＲＬ、見つけた時の検索キーワード等を教えて下さい。
- フィッシング被害に遭ってしまった．．．．
  → 宮崎県警察本部又は最寄りの警察署にご相談下さい。

令和２年12月18日

地　域　安　全　情　報

（ No. ５４ ）

（ 犯罪の起きにくい社会づくりのために ）

発信者：宮崎県警察本部サイバー犯罪対策課
（代）0985-31-0110

特集：フィッシング対策④

今回の特集では、これまでに把握しているスミッシングの実例を紹介します。
以下のようなメッセージは詐欺の可能性が非常に高いので、騙されないで下さい！

スミッシングとは

スミッシングとは、携帯電話やスマートフォンに標準搭載されているＳＭＳ（ショートメッセージサービス）機能を悪用したフィッシング詐欺のことを言います。
本県でもスミッシングのメッセージが届いたという相談が非常に多く寄せられています。

こんなSMSが送られてきたら危険です!!

ダイレクトのパスワードが翌日に失効し、[redacted]銀行のメンテナンスサイト [redacted].com により、更新をお願いします。

[redacted]銀行ですが、「犯罪収益移転防止法」に基づき、本人確認提示をお願いします。
[redacted].com

<[redacted]銀行>
お客様の口座は悪用された可能性があります。速やかに安全確認を実施ください。認証はこちら
www.[redacted].com

■ 金融機関（銀行）を装った実例

お荷物のお届けにあがりましたが不在の為持ち帰りました。ご確認ください。
[redacted].duckdns.org

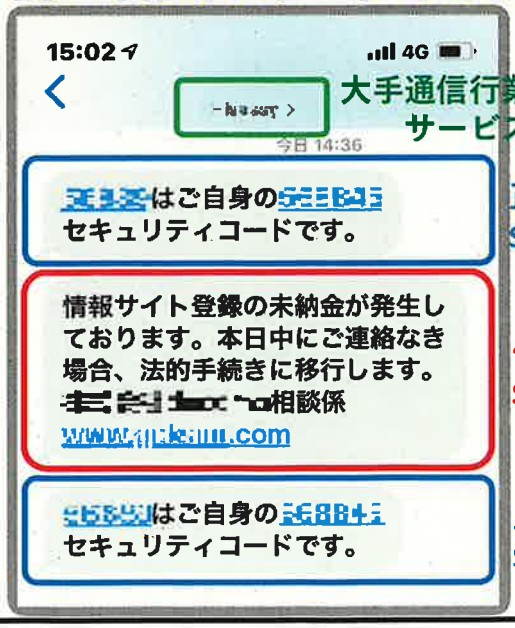
このメッセージが送られてきたという相談が、非常に多く寄せられています！！

■ 宅配業者を装った実例

【警察庁】銀行をご利用のお客様に対し不正防止措置の認証確認を行っております、認証の設定はこちらへ:https//[redacted].com

■ 官公庁（警察）を装った実例

更に巧妙なパターンもあります!!!



大手通信行業のサービス名

正規SMS

偽装SMS

正規SMS

最新の手口では、正規事業者のＳＭＳメッセージ画面に、偽のメッセージを紛れ込ませるという手法が確認されています。

偽装されたメッセージ中に書かれているＵＲＬをタップすると、ＩＤやパスワード、クレジットカード情報といった個人情報の入力を求めるフィッシングページが表示され、個人情報が盗まれたという事例が多数寄せられています。

メッセージ内にＵＲＬや電話番号が記載されたＳＭＳが届いたら、安易にタップせず、事業者のホームページを直接検索する等して、フィッシング詐欺関連の情報が掲載されていないか、確認しましょう。

令和２年12月24日

地　域　安　全　情　報

（ No. 58 ）

（ 犯罪の起きにくい社会づくりのために ）

発信者：宮崎県警察本部サイバー犯罪対策課
（代）0985-31-0110

特集：フィッシング対策⑤

宅配事業者を装った「不在通知」の偽ＳＭＳに関する相談が非常に多く寄せられています。
よくある相談事例や手口を知り、騙されないように注意しましょう。

宮崎県警察本部生活安全部のｔｗｉｔｔｅｒアカウント（ @MP_seian ）でも関連情報を発信していますので、フォローをお願いします。

相談事例

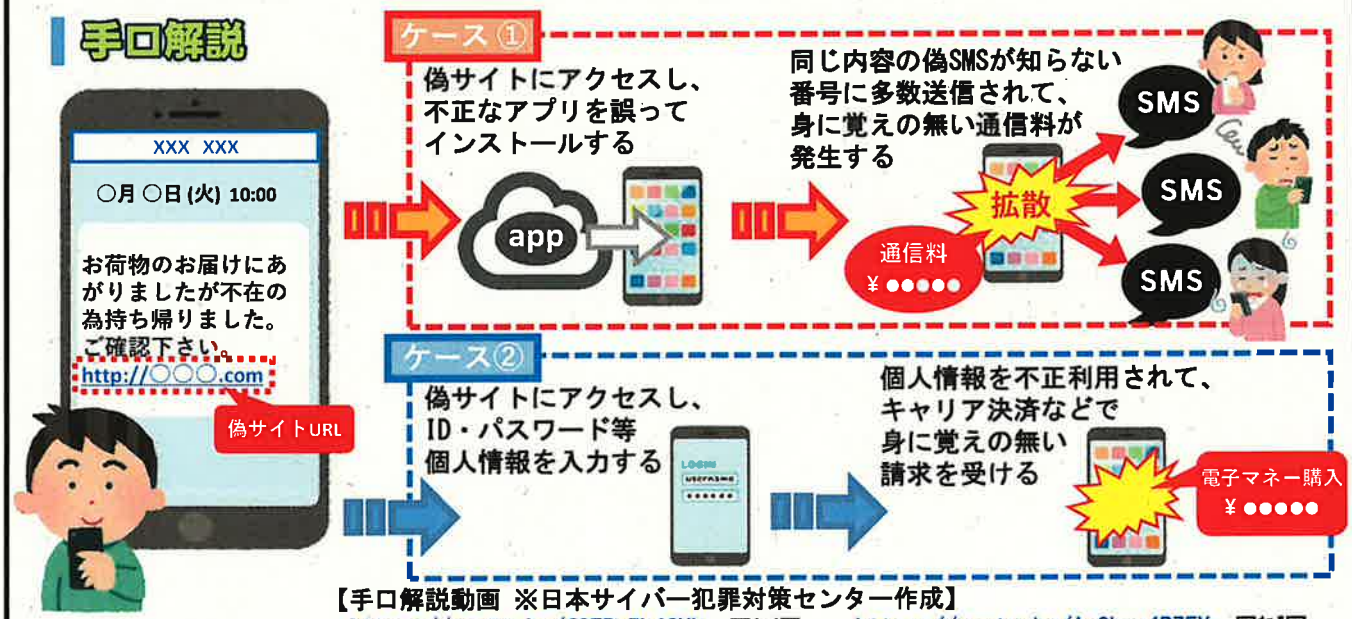
ケース ①

宅配物の不在通知のＳＭＳを受信し、何かダウンロードするような画面になった。
数日後、知らない番号から荷物受取を申し出る着信が何度も来るようになった。
不審に思い、携帯電話ショップに相談に行くと、自分の電話番号からＳＭＳが多数送信されていて、通信料が１万円以上かかっていることが分かった。

ケース ②

宅配物の不在連絡のようなＳＭＳが届いたので、本文記載のＵＲＬにアクセスし、氏名などの個人情報を入力して送信してしまった。
その後、キャリア決済で、数万円分の電子マネーが購入されていることが分かった。

手口解説



【手口解説動画 ※日本サイバー犯罪対策センター作成】

https://youtu.be/f0FPr7b43Vk （Android端末の場合）

https://youtu.be/As2hgq4PZFY （iPhone端末の場合）

予防・対策

- 「不在通知」ＳＭＳの送信元に、折り返しの連絡をしない。
- 「不在通知」メッセージが届いても、記載されているＵＲＬに安易にアクセスしない。
- ＵＲＬにアクセスしてしまっても、提供元不明のアプリをインストールしたり、リンク先のページでＩＤやパスワード、その他の個人情報等を安易に入力しない。
- 誤って不正アプリをインストールしてしまった場合は、直ちにアンインストールする。
- 偽サイトにＩＤやパスワード、クレジットカード情報等を入力してしまった場合は、ＩＤ・パスワードの変更、クレジットカードの停止措置を行う。

こんな手口は「うそ電話詐欺」！

電話からはじまる「うそ電話詐欺」

自治体や金融機関の職員を名乗って・・・

○過払い金がある（医療費等）
○ATMで返還の手続きをする
○ATMに着いたら、機械の操作方法を教えるので電話して

還付金詐欺

対策
○犯人からの電話に出ない対策（裏面参照）
○口座情報を教えない
○ATMで電話を使用しない

子や孫・警察官・弁護士などを名乗って・・・

○風邪をひいて声が変わった
○携帯電話をなくして番号が変わった
○名前を名乗らない

オレオレ詐欺

対策
○犯人からの電話に出ない対策（裏面参照）
○家族の合い言葉を決めておく
○本人や家族に電話して確認する

警察官・金融機関（関係団体）・家電量販店などを名乗って・・・

○詐欺グループを捕まえたら、あなた名義のカードを持っていた
○他人があなたのカードを不正に使用している
○カードを預かるので、職員が自宅に伺います

キャッシュカードを狙った詐欺（預貯金詐欺、キャッシュカード詐欺盗）

対策
○犯人からの電話に出ない対策（裏面参照）
○電話でお金の話は詐欺を疑う
○他人にキャッシュカードを渡さない！暗証番号を教えない！

メールや手紙、インターネットなどからはじまる「うそ電話詐欺」

○未納料金があります
○訴訟最終通告のお知らせ
○パソコンがウイルスに感染した
○高額の当選金が当たった
○アダルトサイトに登録された

架空料金請求詐欺

対策
○相手から指定された電話番号に電話をかけない
○「電子マネーを買って」と言われたら詐欺を疑う
○個人情報を教えない

犯人は、この他にもあの手この手でお金をだまし取ろうとします。
詳しくは、警察庁や警察本部のホームページをご覧ください。