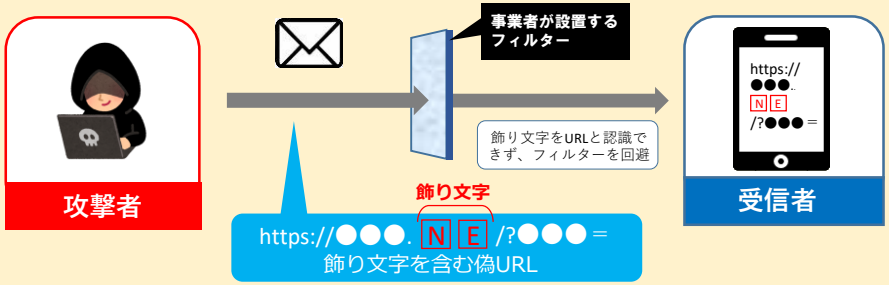
事　例

偽メールを遮断するために、フィルター機能を使っていたのに、企業や金融機関を装った怪しいメールが届いた…

実在する企業や金融機関を装って、偽のメールやSMSを送りつけ、記載したURLから偽サイトに誘導し、個人情報を盗み取るフィッシングの被害が後を絶ちません。

フィッシングの被害防止策として、偽のメールを遮断するフィルター機能が有効ですが、フィルターを回避するための巧妙な手法も確認されています。

ケース１　飾り文字などが含まれた偽URL



※　飾り文字には、上記のとおり、URL中のアルファベットが罫線で囲まれた文字などがあります。

★ URLに飾り文字などが含まれる場合は、フィッシングサイトの可能性がありますので、アクセスしないようにしましょう

ケース２　URLの代わりに「QRコード」を貼り付けて、偽サイトに誘導

QRコードを貼り付けた広告を配布する

QRコードを読み取りサイトにアクセス

カード情報を盗み取る

★ QRコード付きのチラシは、QRコードの接続先URLを確認して、安全か矛盾点がないかなど確認しましょう

SNSでサイバー犯罪の最新手口を随時投稿中です。
ぜひフォローしてチェックしましょう！

詳しくはこちら

公式X（旧ツイッター）　公式インスタグラム

知る！学ぶ！防ぐ！ サイバー犯罪

福岡県田川警察署

相談事例から「知る！学ぶ！防ぐ！」

事　例

SNSで「ひと月で数万円稼げる」などという副業の広告を見つけて始めたが、お金を騙し取られてしまった！！

当県において、SNSでウソの副業を持ちかけれて、金銭を騙し取られるという相談が多発しています。

SNSの副業広告にアクセスして知り合った人物から、「動画を見てスクリーンショットを撮り送信すると、報酬がもらえる。」などと副業を持ちかけられ、最終的には、「業務中のミスで違約金が発生した。」など、何らかの理由付けをして、金銭を騙し取る手口です。

SNSを利用する若い世代にも被害が増えており、特に注意が必要です。

SNSなどで副業の広告にアクセス

・SNSアカウントと繋がり、仕事内容を説明されるため、説明どおりに仕事をこなす
・実際に報酬が支払われる

・「業務中のミスで違約金を支払う必要がある」などと金銭を要求される
・指定口座に金銭を振り込むよう指示される

被害に遭わないために・・・

★『うまい話には必ずウラがある』と思って疑い、鵜呑みにしないようにしましょう
★ 少しでも不審に感じたら、まずは身近な人に相談しましょう