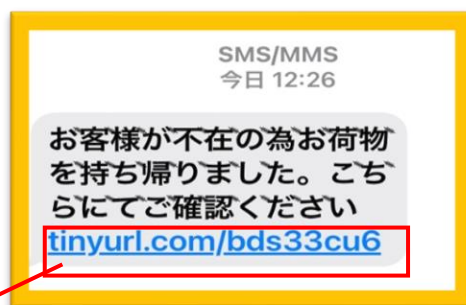


宅配便の不在通知をかたる通知は偽物ですので注意を



上記のような「お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください。」

URL」の短いメッセージがスマホの SNS (メッセージ) に送信され、通知表示されます。

この URL はタップ (開かない) しないで削除します。

記載された「**URL**」をタップすると、「AppStore アカウントは安全異常があるので、再度ログインしてください。閉じる」とログインを求める通知になり、通知を「閉じる」と「ID とパスワードの入力を求めるホームページが開き、Apple の ID とパスワード等の入力画面」の表示になります。

この画面が、情報をだましとるための偽のサイト (フィッシングサイト) です。SMS を通じたフィッシングの被害ですので、これを「スミッシング」と呼ばれています。

本物のホームページと同じ文言や問合せ先が記載され、デザインも似せており、本物と思いつまみせ、これに ID とパスワードなどの個人情報を入力すると「ID とパスワード等」が犯罪グループにだまし取られます。

だまし取られた情報は、アカウントへの不正アクセスや決済サービスの不正利用等とさらなる犯罪に使われる恐れがあります。

このようなスミッシングの被害は増加傾向にあります。これまでは、実在の企業名を名乗る宅配便の不在通知が多かったですが、最近は上記のような会社名を入れず不在通知を装うものが多くなっていますので注意が必要です。

騙されないために、どのような内容であれ、「SMS に記載された URL を開かないで削除する」が必要です。

文書の内容に不安を感じた時はいったん SMS を閉じ、普段使っている公式のアプリやホームページからログインして通知を確認することが大切です。

怪しい SNS が届いたら、まず自分で調べることです。その心がけが自分の身を守ることに繋がります。