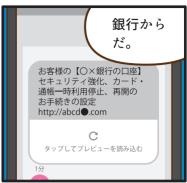
マンガでわかる サイバーセキュリティ

フィッシングサイトには注意しよう

















詐欺流行ってるなぁ。 引っかからないように 注意しないといな~。



. フィッシングとは、金融機関を装ったメール などで、個人情報を盗む詐欺のことです。 スマホの普及に伴いEメールだけでなくSMS での被害も増えています。

例えば こういった銀行を 装うSMSメール が届き…







本物そっくりの偽サイトに 誘導後、銀行口座や暗証番号、 ワンタイムパスワードなどの 情報を入力してしまうと…



不正送金の被害 に遭う可能性が あります。







暗証番号・ワンタイムパスワード を偽サイトに入力すると、預金全 額が不正送金の被害に遭う可能性 があります。 ワンタイムパスワード と暗証番号あれば全部 手に入るぞ

全部ルのものない。

実際に、平成30年では フィッシング詐欺等に より全国で4億円以上 の不正送金被害が発生 しています 平成30年 総被害額4億円

フィッシングB カード ケーム モバイル

また、短期間で複数の企業を装うフィッシングサイト が立ち上がり、一か月で数百人・合計数億円の被害が 発生した事例もあります。 え… そんなに被害が 出てるんだ…



銀行はSMSで暗証番号を 聞き出すことは絶対に ありません! 不審なSMSやメールを受信 した際は、リンクをクリック したり個人情報を入力しない

フィッシングA

銀行

れた!



本物とそっくり なサイトだと 気付けなかった なぁ…





他の事例

- 銀行やクレジットカード会社、ショッピングサイト等を装う、様々なフィッシングサイトが立ち上がった事例がある
- フィッシングサイトを閲覧したユーザの端末に情報を盗取する機能を持ったウイルスをダウンロードさせる事例もある
- 個人だけでなく、法人もフィッシングの被害にあった事例がある(※1)
- フィッシング SMS には、次のような例もある:【●●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、再開手続き:https://●●.com

ここがポイン

- SMS やメールを受信した際は、リンクがフィッシングサイトの URL に偽装されている場合あるので、安易にクリックしないことが重要 (※2)
- 受信したSMSやメールが怪しいと感じた場合、同様のフィッシングメールがないか確認することが有効 (※3) また、公式サイトをブックマークに登録することも有効
- フィッシングサイトを検知・ブロックできる場合もあるので、ウイルス対策ソフトをインストールすることが有効
- 万が一不正送金等の被害に遭ってしまった場合は、速やかに電話受付窓口等に連絡することが重要
- (※1) 警察庁広報資料によると、平成30年では個人で合計約3億6400万円、法人で合計約4,000万円の被害が発生しています。
- (※2)銀行等の一部の企業は、電子メールに電子署名を付与してメールを送っています。メールに正規の電子署名が付いてれば、正規のメールであることが確認できます。
- (※3) フィッシング対策協議会の Web サイトでは、実際に確認されているフィッシングメールの一部が公開されています。