



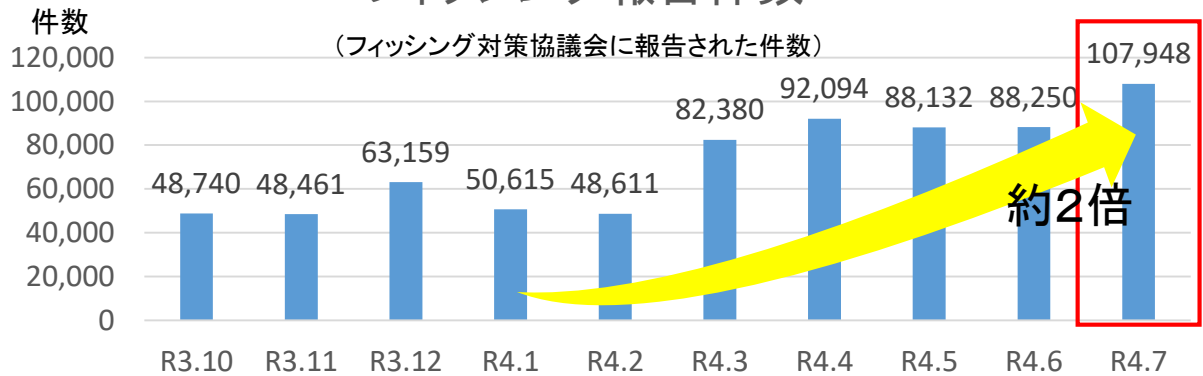
サイバーニュース

R 4 年 第 8 号
奈良県警察本部
サイバー犯罪対策課

減らないフィッシング詐欺！多様化するメールの内容にご注意を！

フィッシング報告件数

(フィッシング対策協議会に報告された件数)



フィッシング対策協議会の発表では、7月中のフィッシング報告件数は、今年1月と比較して約2倍に増加しています。
また「クレジットカードの利用を装うフィッシング」が全体の約47.6%を占めています！



最近のフィッシングメールの例

※実際に認知したフィッシングメールの本文を一部抜粋しています。

【ETC利用照会サービスを騙るSMS】

この度はETCサービスをご利用いただきまして誠にありがとうございます。
ETCアカウントにアカウントリマインダーリスクが検出されましたETC決済方法を再確認ください。

メッセージに記載のURLをクリックするとID・パスワードの入力を求められるログイン画面へ誘導されます。
誤ってID等を入力すると「**支払い方法が無効**」等と表示され、次にクレジットカード情報の入力を求められます。

【クレジットカードの利用確認を騙るSMS】

【●●クレジットサービス】
この度、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただきます。ご連絡させていただきました。
つきましては、下記へアクセスの上、カードのご利用確認にご協力をお願い致します。

メッセージに記載のURLをクリックするとクレジットカード情報の入力サイトへ誘導されます。

【経済産業省を騙るSMS】

【経済産業省】
現在、電力需給ひっ迫注意報が発令されている。
お客様が情報を確認する必要があります。
確認しないと、料金明細がお客様の住所に正しく届かないなどの事態が発生します。

メッセージに記載のURLをクリックすると、経済産業省や全国の電力事業者のロゴが表示されたサイトに誘導され、名前等の個人情報の他、クレジットカード情報の入力が求められます。

最近のフィッシングメールでは「**電力ひっ迫、通信障害の返金**」等と社会情勢に合わせた内容にするなど、あの手この手でみなさんの情報を搾取しようと企てています！
よく見ると、日本語の構成が...

フィッシングの被害に遭わないためには...

- SMSやメールに記載されたURLにはアクセスしない！
- 個人情報及びクレジットカード情報(口座情報)は容易に入力しない！

が鉄則です。

万が一、フィッシングサイトで情報を入力してしまった場合は、すぐに警察やクレジットカード会社、銀行等に連絡してください！

