

サイバーセキュリティ関連情報（8月号）

鳥取県警察本部サイバー犯罪対策課

○ クレジットカードの利用確認を装うフィッシングに注意！！

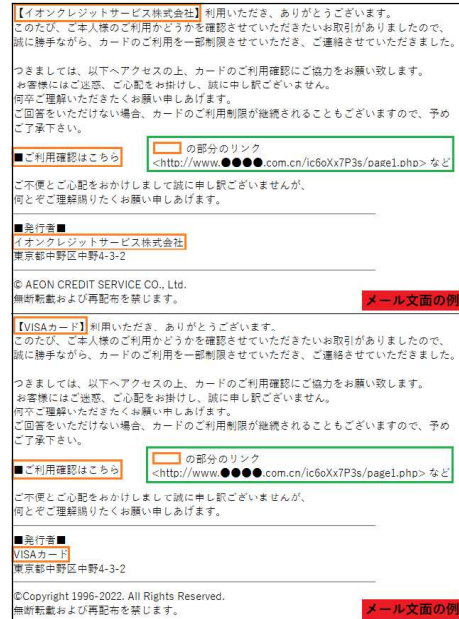
フィッシング対策協議会は、クレジットカード会社やキャッシュレス決済事業者等をかたり、クレジットカードの利用確認に関する通知を装うフィッシングメールの報告が増えているとして、注意を呼び掛けています。

確認されているメールは、「カード年会費のお支払い方法に問題があります」「本人確認のお知らせ」等の件名で送信されるものであり、メール本文内において、利用確認と称して、URLのリンクを踏ませ、フィッシングサイトに誘導します。

このようなフィッシングサイトにおいて、カード番号、有効期限、カード確認番号、カード名義人、生年月日、電話番号、住所、郵便番号、WebユーザーID、Eメール、パスワード等の情報を入力してしまうと、クレジットカードやキャッシュレス決済の不正利用に繋がりますので、絶対に入力しないようお願いいたします。

また、フィッシングサイトは、本物のサイトの画面をコピーして作成することが多く、見分けることが非常に困難です。

日頃から、サービスへログインする際は、メールやSMS内のリンクからではなく、公式サイトからアクセスするよう心がけてください。



引用：【フィッシング対策協議会】 https://www.antiphishing.jp/news/alert/creditcard_20220624.html

○ ワンクリック詐欺の手口に注意！！

独立行政法人情報処理推進機構（IPA）は、アダルト系や出会い系のサイトで動画や写真を見ようとしたときに、高額な代金やキャンセル代を請求する画面が表示される、いわゆる「ワンクリック詐欺」に関する相談が引き続き寄せられているとして、注意を呼び掛けています。

ワンクリック詐欺は、サイトを訪問してきた利用者に対し、

- ・ 契約内容を明確に説明しようとせず、利用者に契約に同意する意思がないにも関わらず「有料会員契約が成立（登録）した」、もしくはアプリをインストールしてないにも関わらず「有料アプリのインストールが完了した」などと表示して、代金の支払いを要求する。
- ・ あたかも利用者個人を特定しているように「利用端末の情報、IPアドレス」などの情報を表示する。
- ・ 「契約は法的に有効」と主張し、法的措置や遅延料金請求など強い表現で早期の代金支払いを求める。

などの方法で行われ、以前より、形を変えながら続いている手口です。

ワンクリック詐欺では、あたかも利用者进行を特定できる個人情報取得したかのような情報が表示され、不安をあおってきますが、これはインターネット上の通信を行うために必要な情報として伝わっているだけで、これらの情報で個人を特定することはできません。

仮にそのような画面が表示されても、「身元を知られた」などと不安に陥ることなく、くれぐれも画面に表示された連絡先に電話やメールをしたり、相手の請求に応じ、代金を支払わないよう注意してください。

お客様情報詳細	
お客様ID番号	307484505
ご契約日時	2022-05-11 12:14
お支払期日	2022年5月11日 23:59
お支払金額	450,000円 (特別価格:350,000円)
ご契約端末情報	Mozilla/5.0 (Linux; Android 12; SC-01M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Mobile Safari/537.36

【「あたかも個人情報を取得したかのように表示される」画面の例】

引用：【独立行政法人情報処理推進機構（IPA）】 <https://www.ipa.go.jp/security/anshin/mgdayori20220706.html>