

11月の防犯対策



令和3年11月1日発行
（公社）滋賀県防犯協会



「フィッシング」によるクレジットカードの不正利用に注意！

日本クレジット協会の調査によると、2020年のクレジットカード不正利用被害額は、251億円に達し、そのうちの89%を占める223億円がクレジット番号盗用によるものです。

番号盗用とは、クレジットカード番号等の情報だけで不正に決済された金額です。

主に、インターネットショッピング等で非対面でカード会員になりすまして不正利用されています。

フィッシングにより、クレジット番号、有効期限、セキュリティコードを盗み取られて不正な買い物をされるパターンが多いと考えられますので、特にフィッシングメール等に騙されないように注意してください。

※「フィッシング」とは、送信者を詐称したメールやSMSを送りつけ、偽のホームページに接続させるなどの方法で、クレジットカード番号、アカウント情報（ユーザID、パスワードなど）といった重要な個人情報を盗み出す行為のことを言います。

○ フィッシングの特徴

【メールやSMSで良く使われる文言】
対応を急がせるものや不安を煽るような内容が使われています。

次のような文言のメールやSMSは、フィッシングの可能性が高いので、絶対にカード番号等を入力しないでください。

- ・不正利用防止のため、お客様のクレジットカード番号、有効期限、セキュリティコードを登録してください。
- ・第三者による不正アクセスを確認しましたので、お客様のクレジット番号等を再登録してください。
- ・お客様のアカウントが停止されました。確認のため、クレジットカード番号等を入力してください。」



○ フィッシング対策

クレジットカード会社が、個人情報やクレジットカード番号をメールで聞くことはありません。

・個人情報やクレジットカード番号等の入力を促すメールやSMSはフィッシングを疑ってください。

・宅配サービス、金融機関、通信事業者を装ったSMSが多数確認されていますので、これら事業者のメール本文中のURLは、フィッシングサイトである可能性がありますので、アクセスしないでください。

・クレジットカード情報を入力する場合は、必ず公式サイトであることを確認してください。
※ 迷ったときは県警本部サイバー犯罪対策課までお問い合わせください

二七電話詐欺の被害！手口を知って対策を！

○ 被害の発生

新聞記事によると、「10月15日、草津市内の女性宅に警察官を名乗る男が電話で『詐欺の犯人を逮捕した。被害者なので返金される』などと告げた後、女性宅を訪ねた。女性がカード3枚を渡し、暗証番号を伝えたところ、後に計450万円が引き出された。高額の引き出しがあり、銀行が女性に連絡して被害が発覚した。」というものです。

○ 連日かかる詐欺電話

10月21日は守山市内で、翌22日は米原市内において、市役所職員をかたって「介護保険料の還付金があります。近くの銀行かATMに行ってください。」などといった不審電話がかかってきています。これは、全国的にも多発している還付金詐欺の同一手口で、ATMで犯人が操作方法を電話で指示してお金をだまし取るものです。

対策は、『直接犯人と話をしないこと』

犯人グループはだましのプロです。知識を持っている人でも電話で直接話をすると冷静さを失いだまされている現状にあります。重要なのは「直接犯人と話をしないこと」です。犯人は声を録音されるのを嫌がり多くは電話を切りますので固定電話は常時、留守番電話設定にしましょう。

『優良防犯電話』で詐欺撃退！

最も有効な対策は、迷惑電話防止機能がついた優良防犯電話を設置することです。
防犯協会では電器商業組合と共同で、今なら「購入補助キャンペーン」を行っております。（2000台限定で残り110台）

お問い合わせは、防犯協会の電話「077-525-0909」へ