あなたのカード情報 狙われています

クレジットカードの利用拡大により、不正利用被害も年々悪化しています。
不正利用被害の9割以上が「番号盗用」※による手口です。
自分自身のカード情報を守る行動をしましょう!

※「番号盗用」…クレジットカード情報が盗み取られ、不正利用されること

番号盗用の手口

手口❶ フィッシング
（実在する企業を装って、偽サイトに誘導、カードの個人情報を盗む）

スマホに「登録されたクレジットカード情報に誤りがあります。再度登録してください。」というメッセージを受信。カード会社やネットショッピング等の偽サイトでクレジットカード情報を入力し、送信してしまう。

手口❷ 盗み撮り

クレジットカード番号、有効期限、セキュリティコードなどの情報が盗みとられると、インターネットショッピングなどで不正に使われる可能性がある。

手口❸ 紛失・盗難

クレジットカードが入った財布を落とす、外出先で置き忘れる。

手口❹ スキミング
（クレジットカードの磁気ストライプから情報を不正に抜き取り、偽造カードを作成して利用する）

最近では物理的なスキミングのほか、Webスキミング(ECサイト※に不正なプログラムを埋め込み、利用者が入力したクレジットカード情報を盗む)や、非接触型スキミング(非接触型カードから専用の機器を使って情報を盗む)などの手口もある。

※ECサイト…インターネット上で商品やサービスを売買するWebサイト

被害防止のための対策

番号盗用を未然に防ぐ

- 利用するWebサイトの安全性を見極める。
- クレジットカード画像をむやみに送らない。
- 不審なメール・メッセージに注意し、記載のURLは絶対に開かない、カード情報は入力しない。

おかしいなと感じたら

- 利用明細の内容に身に覚えがあるか確認。
- クレジットカードが手元にあるか確認。

不正利用に気づいたら

- クレジットカード会社へすぐに連絡。
- 最寄りの警察署に相談し、カードを再発行。

クレジットカード情報は、
見せない!
渡さない!
フィッシングサイトで入力しない!
自分自身のカード情報を
守る行動を!

警視庁ホームページでは、クレジットカード不正利用の被害防止啓発動画を公開しておりますので、ぜひご覧ください。

悪質訪問業者の 飛び込み営業にご注意ください

悪質訪問業者は、突然訪問して「無料点検」を持ち掛け、
言葉巧みに不安をあおるなどして不要な契約を結ぼうとします。
また、強盗など他の犯罪の下見として訪問している可能性もあります。

悪質訪問の事例

事例❶ 屋根の修理

2人組の男性が一戸建て住宅を訪れ「屋根の木材が腐っている。」「台風が来たら瓦が飛んでいく。人に当たったら大変。」などと不安をあおり一旦は契約。後日、着工前に家人が屋根に上ってみたところ、破損状況がなかったため、クーリングオフ。後の警察の捜査により工事の必要性はなかったことが判明した。

事例❷ ガス給湯器の点検

「○○ガスです。給湯器の点検時期です。」と男性から電話があり、予約を入れた。当日、○○ガスの委託業者を名乗る男性が現れたが、給湯器のカバーを開けたと思いきや、すぐに閉めて「交換ですね。」と急かすので、怪しいと思い対応を拒否した。後で○○ガスに問い合わせたが委託の事実はなかった。

事例❸ 水道の点検

インターホンが鳴り、若い男性が「水道局です。メーター点検です。」と言いつつも、夫の名前を何回も確認したり、水道局員なのにメーターの場所を知らないなど不審だったため、ドアは開けなかった。男性に対して、名前や所属を確認すると立ち去った。水道局に確認したが点検の事実はなかった。

事例❹ 分電盤の点検

オートロックマンションにもかかわらず、玄関のインターホンが鳴り対応すると、男性が「下の階の電気点検をしました。ついでにお宅も点検します。」と言って分電盤を点検した。すると「とても古いので交換した方がいいですよ。」と言われたので、その場で契約してしまった。男性が帰った後、渡された名刺の会社名をインターネットで検索しても出てこなかったため、怪しいと思いすぐに解約手続きを行った。

悪質訪問業者の対策

家のドアを開けずに、身分や用件を確認

- 訪問を受けたときは、インターホン越しで対応し、身分や用件を確認する。

点検させない

- 無料と言われても、その場では点検させない。

即決しない

- その場では契約しない。

困ったときは、警察にご相談ください
● 最寄りの警察署　● 警視庁総合相談センター #9110
※相談内容に応じて、相談窓口等をご案内します。