ネット通販詐欺に遭った場合の対応

（茨城県警察本部サイバー犯罪対策課からのメールより抜粋　2021.1.23）

オレオレ詐欺等の事件（インターネット通販サイト詐欺事件を含む）に利用された口座を凍結した時の残高が 1,000 円以上ある場合は、振込先の金融機関が、振り込んでしまった方々からの被害申請を受け、その被害金額の割合により、残高を基本として返還金を算出し、後日（被害申請から半年程度)、被害者の方々に、ある程度の被害金（全額ではなく凍結時の残高が基本）を返還するという振り込め詐欺救済法という法律があります。

上記救済法が該当するか否かについて、当該金融機関に連絡してご確認してください。

次に、当該通販サイトに個人情報を入力していることから、今後、注意すべきことについて説明します。
まず、知られてしまった個人情報を取り戻すことはできないと考えてください。

１．メールアドレスを登録している場合

・今後、フィッシングメール、架空請求メール、悪質な出会い系サイトへ誘導するメール等の迷惑メールが来る可能性があります。
・「迷惑メール振り分けサービス」などを利用して、なるべく迷惑メールを排除するようにしてください。
・ウイルス対策ソフトがインストールされてない場合は、インストールされることを推奨します。
・送信元メールアドレスのドメイン（@の右側）を常に確認することが大切です。通常、スマートフォンは、送信元メールアドレスを表示せず送信元名称のみを表示しています。「詳細」等のボタンをタップして送信元メールアドレスを表示させ確認する癖をつけてください。
・送信元メールアドレスを確認したところドメインが正規なドメインであったとしても、100%信用できない場合があります。悪意ある者が送信するメールは、送信元メールアドレスが詐称されていることがあるのです。
・そして、身に覚えのないメールに対しては
　見ないで削除
　返信しない
　本文に記載されている電話番号には電話をかけない
　本文に記載されているリンクをクリックしない
　添付資料を削除する
　こと（毅然と無視して削除）が大切です。

２．電話番号を登録している場合

・架空請求の電話がかかってくる可能性があります。
・しばらくの間、登録してある電話番号（家族や友人等）以外の電話番号からの電話には応答しないことが賢明です。

・登録以外の電話番号を応答してしまったところ架空請求の電話だった等の場合は、すぐ切るようにしてください。

３．住所、氏名、電話番号をセットで入力している場合

・悪意を持った者が、今後作成する別の詐欺通販サイトの会社概要欄に、勝手に個人情報を掲示してしまう可能性があります。
・その場合、その詐欺通販サイトの被害者から「送金したのに商品が届かない。」等の電話がかかってくることが想定されます。
・その際は、その方に「詐欺と思われるので地元の警察に相談すること。」を説明すると同時に、貴方の個人情報が掲載されてしまった通販サイトの URL を聞いてください。
警察では、詐欺通販サイト等に「このサイトは危険です。」等の警告画面を表示するよう、警察庁を通じてウイルス対策ソフト関連会社に依頼することが可能です。
・通販サイトに勝手に貴方の個人情報を掲載している場合でも、依頼することが可能です。
・そのサイトの URL が判明した場合は、改めて警察へのご相談をお願いします。

４．住所、氏名をセットで入力している場合

・粗悪な商品を高額な代引郵便として郵送されてくる可能性があります。また、頼んでもいない商品が、勝手に郵送・配送されてくる可能性があります。
・このような商品が送られてきた場合は、受取拒否することを強く推奨します。
・ご家族にも今回のトラブル内容を説明してください。
・身に覚えのない代引郵便物が配達されて来た場合、頼んでもいない商品が配送されてきた場合は、ご家族のどなたが対応しても受取拒否できるようにしてください。

５．悪意ある者が住所地に来てトラブルを起こす危険性

・当該通販サイトは詐欺サイトであり、自分の姿を隠して他人からお金を騙し取る手口であることから、住所地に不審者が来てトラブルになる可能性はないと考えられます。
・しかし、住所、氏名等の個人情報は、闇で売買されています。住所、氏名、電話番号、利用しているメールアドレスの情報を購入した者が、悪意を持っている者の可能性も考えられます。
・家を出る時や帰宅時には、周囲に注意を払う等防犯意識を少し高める必要はあると思われます。
・仮に、自宅周囲に不審者がいる等の場合は 110 番通報してください。

以上