サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和3年
2月22日
Vol.57

その当選メッセージ！本物ですか？
～うまい話・儲け話に要注意～

手口例

- **正規企業を装った「メールやSMS（ショートメッセージサービス）」や「SNSの偽アカウントからのDM（ダイレクトメッセージ）」**
- **WEBサイトを閲覧中に突然表示される「ポップアップ形式のメッセージ」**

などに記載された、

『ご当選おめでとうございます』『○○○をプレゼントします』

等のうまい話や儲け話で気持ちを引き付けられ、リンク先の偽サイトや詐欺サイト等へ誘導される手口が確認されています。

画面の指示に従って操作を進めてしまうと、「手続きに必要」などと**クレジットカード情報・個人情報の入力や電子マネーの購入等を迫られる**可能性があります。

メッセージ例

＜◎（企業のアカウント名）📷！

要注意

おめでとう！！！！

今日はとてもラッキーです。

あなたは勝者としてランダムに選ばれます
賞品を受け取るには、以下の手順に従ってください。
1　https://www.○○○.com（リンクをクリック）
2　自分で登録します（登録には２分もかかりません）
3　ここに戻って「完了」メッセージを送信します。完了したら、スクリーンショットの証拠を送ってください。証拠を見せて！
　ランダムに選ばれるので、この機会を無駄にしないでください！

幸運を！！

その他にも…「最新の携帯電話」「高額宝くじ●●億円」「●●●万円の高級車」「スポーツブランドのTシャツやスニーカー」などの**当選通知**や「月収+10万円が可能」「見知らぬ人がお金をくれる」などの**儲け話**等、多種多様のメッセージが確認されている。

対策ポイント

県内企業を装う事例も確認されています！

- **とにかく慌てない！**
　「そもそも応募していなければ、当選することはない」「そんなうまい話はあるわけがない」等、**疑いの目を持つ。**
- **差出人やURLなどをよく確認！**
　アドレスやアカウントが正規のものか確認を。確認の際は受信メール等のリンクを利用するのではなく、**WEBブラウザで検索するなどの別の方法で実施。**
- **安易にリンクのクリックや個人情報の入力をしない！**
　個人の日々の癖付け、**セキュリティに関する意識の向上が重要。**
- **情報収集を行う！**
　「対象企業が実際にキャンペーンなどをしているのか」「注意情報を出していないか」等、**自ら検索するなどしてよく確認を。**

参照元：JC3(日本サイバー犯罪対策センター)
https://www.jc3.or.jp/topics/support_iphone_fraud.html

相談窓口

愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)