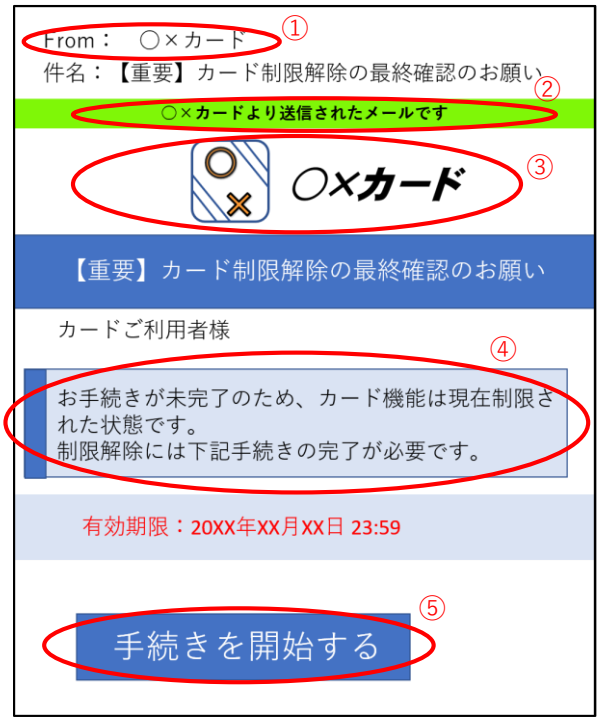
CYBER SECURITY NEWS
栃木県警察
サイバー対策センター
令和８年８月

巧妙化するフィッシングメール

最近のフィッシングメールは、生成AIを活用し精度の高いものが作成されています。
以前は、誤字脱字やおかしな日本語、違和感のある構成などでフィッシングメールと分かりましたが、最近では文面から見破ることが難しくなってきています。

＜クレジットカード会社を装ったフィッシングメールの一例＞



① 送信者の表示名を実在の企業名に偽装

② 送信認証※が正式に行われた風に見せかけるバナーを配置

※メールの送信者を技術的に確認するもの

③ 実在の企業のロゴ、マーク等を使用

④ メール本文は自然な日本語で誤字脱字がない

⑤ バナーをフィッシングサイトにリンクさせ、URLが確認できないように隠す

犯罪者はフィッシングメールと気付かれないようあの手この手で偽装しています。

フィッシング詐欺の被害に遭わないためには…

1　メールやSMSのURLやバナーは絶対押さない！

メール本文のURLは、見た目だけ偽装することもできるため、正規のURLに見えても実際は偽サイトのURLにアクセスしてしまうこともあります。
心当たりのある場合にこそ注意が必要です。
メールやSMS内のURLやバナーから安易にアクセスすることはやめましょう。

2　内容を確認するには、公式サイトやアプリを使用！

内容の確認には、必ず公式サイトや公式アプリを使いましょう。

3　セキュリティ対策ソフトを活用

詐欺サイトにアクセスした際に警告を表示してくれるセキュリティ対策ソフトやアプリを活用しましょう。