埼玉サイバーセキュリティ推進会議（事務局：埼玉県警察本部生活安全部サイバー犯罪対策課）
S．C．S．C通信
H30．6．28
NO．49

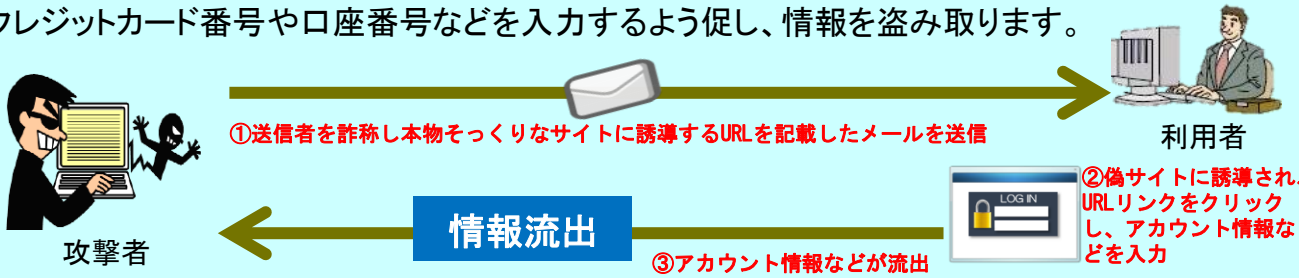
教育機関等を対象としたフィッシングメール事案に対する注意喚起

本年５月、某教育機関において、メールの転送被害による個人情報等の漏えいが判明致しました。教職員宛てにフィッシングメール（クラウドサービスなどの名前を騙り、本物と酷似したメールでID、パスワードを盗むもの）が届き、本物と誤信した教職員が、メールに記載されたURLのリンク先において電子メールのID、パスワードを入力したところそれらの情報が盗まれてしまいました。その結果、教職員のメールが不正に外部に転送されるように設定変更が行われ、学生の個人情報等の漏えいにつながったのです。

フィッシングメールとは

フィッシングメールはフィッシング詐欺とも言われ、送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、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）といった個人情報を盗み出す行為のことを言います。

典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物とそっくりな偽サイトに利用者を誘導し、そこでクレジットカード番号や口座番号などを入力するよう促し、情報を盗み取ります。



被害事例

・Apple IDを狙うフィッシングメールの例

件名：「あなたのアカウントは一時的に無効になっています」

本文：「Apple IDのアカウント情報が不正確などの理由で一時的に無効になっています。
それを解消するために、下記のURLにアクセスして下さい。
http://www.apple.xxxxxx.com 」

このように、受信者の不安をあおるような内容のメールを送り、指定のURLにアクセスするよう巧みに誘導していたものもあります。

被害防止対策

・メール本文に記載されたURLを安易にクリックしない。

・企業を名乗るメールに、@gmail.com、@yahoo.co.jpなどのフリーメールのドメインが使用されている場合は特に注意する。

・受信したメールアドレスのドメインをよく確認する。

（例）正　@saitama.co.jp　　誤　@saiitama.co.jp（iが一つ多い）　　誤　@saitana.co.jp（mがnになる）

例にあげたドメインのように、よく確認しなければ間違いに気付かず誤信する危険があります。

・誘導された接続先が銀行やショッピングサイトなどの場合、そのURLが暗号化通信を示すhttps://wwwから始まっているかを確認する。

※最近は、暗号化している(https)誘導先サイトもあるため過信は厳禁です

STOP 立ち止まる | THINK 考える | CONNECT 楽しむ