平成 29 年 2 月

サイバーニュース

アカウント情報や支払い情報などを入力しないでください!!

フィッシング対策協議会によると、これまでに確認されていたAmazon、LINE、セゾンNetアンサー、Appleを騙ったフィッシングメールに加え、新たに**マイクロソフト**を騙ったフィッシングメールが出回っていることが確認されました。

このフィッシングメールの件名は「ご注意！！OFFICEのプロダクトキーが不正にコピーされています。」となっており、本文には「検証作業をしていただけない場合、日本マイクロソフトはお使いのオフィスソフトのプロダクトキーの授権状態を終了させていただきますので、ご了承ください。」などと記載され、このままではオフィスソフトが使用できなくなるように装い、フィッシングサイトに誘導する内容となっています。

本当に信用のできるサイト以外では、

- ○ アカウント情報（メール、電話番号、パスワードなど）
- ○ お客様情報（氏名、生年月日、住所、電話番号など）
- ○ 支払い情報（カード番号、名義、有効期限、セキュリティコードなど）

などの情報を絶対に入力しないでください。

これらの情報をフィッシングサイトなどの不正なサイトで入力してしまうと、LINEなどのアカウントが乗っ取られたり、クレジットカードを不正に使用されてしまいます。

対策の一つとして、フィッシングサイトなどの不正なサイトでは、通信が暗号化されていないことが多いので、URLに記載された通信方法が「保護された通信」であること（「http://」ではなく「https://」になっていること）を確認してください（ただし、「https://」になっていても、全てが信用できる通信ではないことにご注意ください。）。

※ 「Google Chrome」の例

また、今後も有名な会社などを騙ったフィッシングメールが出回ると思われますが、

- ○ フィッシング対策機能を備えたウイルス対策ソフトを導入し、常に最新の状態にする
- ○ メールの内容は不安感をあおるものとなっていたりするが、慌てずに対応する
- ○ 利用中のサイトで自ら登録などの申込をした場合以外、アカウント情報や支払い情報を入力させるような依頼が突然メールで来ることはないので、実在する会社名であっても信用せず、必ず電話やホームページで確認する
- ○ メールに記載されたURL（ハイパーリンク）から直接アクセスせず、検索サイトで調べるなどして正規のURLからアクセスする

などを心掛けて被害に遭わないようにしてください。

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は･･･
石川県警察本部生活環境課サイバー犯罪対策室
076−225−0110
cyber@police.pref.ishikawa.lg.jp