治安・安全情報（インターネット犯罪対策：サポート詐欺と悪質スパム）
【メールマガジン 2020 年９月号から抜粋】

新型コロナウイルスの流行に伴い、インターネット利用者を標的とした犯罪が増加していることについて、これまでも本メルマガでお伝えしてきましたが、今月は最近において被害の急増がみられる「サポート詐欺」と「悪質スパム」についてご紹介します。

（１）サポート詐欺

サポート詐欺とは、画面に突然、偽のセキュリティ警告等の画面（サポート詐欺のサイト）を表示させるなどして、ユーザーの不安を煽り、問題を解決させるためとして、不正なプログラムをインストールさせたり、有償のサービス契約の締結等をさせられたりする手口です。中には認証画面を表示させ、認証情報を盗み取ろうとするものもあります。

【特徴】

〇インターネット閲覧中にポップアップが表示され、指定の番号に電話するように促すメッセージがある。

〇ポップアップ画面は閉じても再度表示される。

〇5 分以内に電話をかけるよう指示する記載があったり、ビープ音が鳴るなど、ユーザーの不安を煽るような仕組みとなっている。

【対応策】

〇警告画面が表示されても慌てずにブラウザを閉じる。ブラウザが閉じない場合は、タスクマネージャーからブラウザを終了させたり、PC の再起動を行う。

〇警告画面のポップアップは、ウェブサイトの広告に仕込まれていることが多いので、これらをむやみにクリックしない。

〇電話の指示等により遠隔操作のソフトウェアをインストールしてしまった場合、パソコン内の情報窃取やマルウェアへの感染等のリスクとなることから、各種アカウントの ID・パスワードの変更や PC のリストアなどの処置を講じる。

（２）悪質スパム

最近、Facebook メッセンジャーに知人・友人のアカウントから動画ようのサムネイルや YouTube ようの URL リンクが送られてきて、これをクリックした結果ウイルスに感染したり、自身の Facebook アカウントを乗っ取られたという被害が急増しています。被害にあったアカウントはつながりのある他のアカウントに同様のスパムをばらまくことで、被害が拡大しています。（「スパム」とは受信者の意向を無視して無差別かつ大量に一括してばらまかれるメッセージのことを指します。）

【特徴】

〇実際の知人・友人のアカウントから送信されるため、無警戒になりやすい。

〇サムネイルやリンクには「このビデオはいつですか？」「あなたはこのビデオに出演して

いると思います」などとしたメッセージが付随する。
〇リンクをクリックすることで、不正プログラムのインストールを促されたり、Facebook のログインページを偽装したウエブページを表示し、ID やパスワードを盗むものも存在する。
【対応策】
〇友人からのメールであっても、不用意にリンクをクリックしない。
〇間違ってクリックした場合でも、その先で示されるインストール作業やログイン作業は行わない。
〇ウイルス対策ソフトを最新バージョンにアップデートしておく。
〇パスワードは定期的に変更するほか、ログイン時の二段階認証設定やログインメールの通知を設定しておく。

※過去のインターネット利用犯罪についてはこちらをご参照ください。(当館ホームページの「犯罪情勢」コーナー)
https://www.sydney.au.emb-japan.go.jp/itpr_ja/life_and_safety_hanzaijousei.html