

新型コロナウイルス関連詐欺（その2）（メールマガジン2020年5月号から抜粋）

当地における詐欺の最新手口を紹介する「スキヤム・ウォッチ（www.scamwatch）」によると、最初の認知以来、1,000件を超える新型コロナウイルス関連詐欺の報告がなされており、その一般的なものとして「個人情報のフィッシング」「オンラインショッピング詐欺」「年金詐欺」を挙げております。そこで今月号では先月号に続き、これら詐欺について、その具体的事例及び対策をご紹介します。

【政府機関を騙るフィッシング詐欺】

携帯電話のテキストメッセージやパソコンの電子メールを用い、政府機関によるコロナウイルスに関する情報提供と称して、個人情報を盗み取るケースが多く報告されています。特にテキストメッセージの場合、送信者名には政府機関を表す「GOV」や「myGov」などの表示がされることから、受信者が正当なメールであると誤信し、メッセージに含まれるリンクをクリックして個人情報を入力し、被害に遭うケースが増えています。

これら詐欺の対処法は以下のとおりです。

- 政府機関からのメールに見える場合であっても、本文中のリンクをクリックしないこと。
- 政府機関のサイトにアクセスする場合、ブラウザーに直接「my.gov.au」と入力するなどし、直接当該機関のウェブサイトアクセスすること。
- 政府機関からの連絡やメールであると謳っている場合でも、個人情報や財務情報を要求するものには決して回答しないこと。

【有名企業を騙るフィッシング詐欺】

フィッシング詐欺には、銀行やスーパーマーケット、保険会社、通信会社などの実在する有名企業を騙り、コロナウイルス・セールなどと称し、添付ファイルやリンクにアクセスさせて、個人情報の窃取や購入していない商品の支払いを求めるなどの詐欺行為も報告されています。

これら詐欺の対処法は以下のとおりです。

- 一見信頼できる有名企業からのものであっても、テキストメッセージや電子メールのリンクをクリックしないこと。
- 個人情報や財務情報を要求する電話には応答しないこと。
- TelstraやNBNなどの通信会社と称するものであっても、自身のコンピュータへのリモートアクセスを提供しないこと。
- メッセージに関する真偽の確認において、メッセージ中の連絡先を使用せず、電話帳や過去の請求書などの独立したソースを活用すること。

【オンラインショッピング詐欺】

先月号でも紹介しましたが、現在、コロナウイルスの治療薬や予防接種などと称する偽の製品を販売するオンラインストアや、フェイスマスクなどの製品を販売していると称する偽のオンラインストアが多数報告されており、これら詐欺の対処法は以下のとおりです。

- 購入する前に購入者のレビューを検索すること。
- 現在、コロナウイルスに対するワクチンや治療法は存在しないことを認識すること。
- 電信送金や国際送金、電子通貨など、なじみのない支払方法を要求する場合は特に注意すること。

【年金詐欺】

現在の各種規制により財政難にある人々から退職年金を盗もうとしたり、不要なサービスを提供したり、料金を請求したりする詐欺が多数報告されております。これらの詐欺は、退職年金または金融サービスの関連機関を装い、「退職年金の一時利用を可能にする」「新ルールが制定され、今後年金を受け取るために情報の更新が必要である」などと騙って、退職年金口座に関する情報を要求するものが大部分です。

これら詐欺の対処法は以下のとおりです。

- 相手が誰であろうと、自身の退職年金に関する情報を提供しないこと。
- 電話の場合、一旦通話を切り、関連機関に直接電話して真偽を確認すること（この場合、相手から提供された連絡先にアクセスせず、オンライン検索などの独立したソースから得た連絡先を利用すること）。