犯罪情勢（宅配を装った偽通知にご注意ください）
【メールマガジン 2021 年 10 月号から抜粋】

豪州消費者庁による当地における最新の詐欺手口などを紹介するウェブサイト「Scamwatch（https://www.scamwatch.gov.au/）」によると、8 月以降、多くの市民の携帯電話のテキストメッセージに宅配を装ったテキストメッセージが配信され、メッセージに従いリンク先で ID やパスワードを入力したり、アプリをダウンロードしたりした結果、個人情報を盗まれたり、携帯電話を乗っ取られたりしたという被害報告が急増しているとのことです。当館では、在留邦人が同様の被害に遭ったケースも把握しており、以下でこの詐欺の手口等について紹介しますので、ご参考にしていただければ幸いです。

〇どのようなテキストメッセージが送られてくるのか

代表的な例として

・Your order will be delivered soon, visit （リンク）
・Your parcel is out for delivery today, track your parcel here （リンク）
・You have 2 pending packages, last chance to pick up the package （リンク）

などのメッセージとともにリンクが送られてくるケースがほとんどです。

〇リンクをクリックするとどうなるのか

住所氏名、電話番号からクレジットカードの番号など個人情報の入力を求められる画面に遷移するケースや、指定のアプリをダウンロードするよう求めるものもあります。アプリをダウンロードさせるケースの場合、携帯電話のセキュリティを無力化するよう、操作者に対し、ブロックされた場合の手順を説明する場合もあります。

これに従い、アプリをダウンロードすると、携帯電話の乗っ取りが可能となり、乗っ取った携帯電話を踏み台とした新たな詐欺行為が行われます。

〇被害に遭わないための方策は

・テキストメッセージ内のリンクをクリックせずに、メッセージを削除すること

メッセージを残しておいたことで、後日誤ってクリックし被害に遭ったケースもあります。

・テキストに直接返信したり、テキスト内の連絡先に電話したりしないこと

実際の宅配の可能性がある場合は、宅配業者の正式な連絡先を調べて確認を行ってください。

〇被害に遭った場合は

・直ちに携帯電話の使用をやめ、携帯電話のサポートセンターに対応を問い合わせてください。
・パスワードなどの個人情報はすぐに変更を行ってください。この際、被害に遭った携帯電話での操作は行わないでください。
・被害に遭った携帯電話を踏み台として詐欺メールが送信されている可能性があることから、携帯電話の登録先の友人等に、被害に遭ったことを知らせてください。
・銀行やクレジット会社に実害の有無を確認するとともに、警察に被害を届けてください。