

各種詐欺にご注意ください ～身を守るための7か条～

【メールマガジン 2019年12月号から抜粋】

日本では、振り込め詐欺をはじめとした各種詐欺が社会問題化しておりますが、豪州においても同様にさまざまな手口による詐欺被害が深刻化しております。以下は、詐欺から身を守るために留意すべき事項をまとめたものです。常にこれを意識しておきましょう。

(1) 詐欺の可能性を常に意識すること

電話や手紙、メール、対面、ソーシャルネットワーキングサイト如何にかかわらず、知らない人や企業からの連絡を受けた際は、詐欺である可能性を常に考慮してください。特にそれが破格のサービスをうたっているものである場合は、詐欺であると思って間違いありません。

(2) 取引相手を調査すること

オンラインでしか会ったことがない、あるいは相手のビジネスが正当なものであるか不明である場合は、相手について調べてみてください。ほとんどの詐欺は、相手の氏名やその取引先をインターネットで検索するだけでも見抜くことが可能です。

(3) 疑わしいテキストやポップアップウィンドウ、またはメールを開封しないこと

電話帳やオンライン検索などの独立ソースを通じて連絡先の身元を確認してください。その際、送信されたメッセージに記載されている連絡先を使用しないでください。

(4) 個人情報を確実に保管すること

詐欺師は、他人の情報や写真を使用して、身元を偽ったり、詐欺の標的にしたりします。郵便受けは錠錠し、請求書やその他の重要文書は破棄する前に細断してください。パスワードや暗証番号は安全な場所に保管してください。またソーシャルメディアで共有する個人情報の範囲に注意してください。

(5) 異常な決済方法に注意すること

詐欺師は、電信送金、プリペイドカード、さらには Google Play や Steam、iTunes カード、ビットコインで支払いを要求することがあります。このようななじみのない決済方法で支払いを要求する場合、詐欺の可能性が高いことを認識してください。

(6) パソコン（スマートフォン含む）を安全に管理すること

自身のパソコンには常にパスワード保護を使用し、他のユーザーとアクセス共有をしないでください。セキュリティソフトウェアを常に更新し、コンテンツのバックアップを怠らないでください。Wifi ネットワークはパスワード保護されたものを使用し、公共のパソコンや公衆 Wifi を使用してオンラインバンキングにアクセスしたり、個人情報を提供したりしないでください。

(7) パスワードは慎重に選択すること

他人が推測しづらいパスワードを使用するとともに、定期的に更新してください。できる

限り大文字、小文字、数字、記号を混在させた強力なパスワードを使用してください。また全てのアカウントやプロフィールに同じパスワードを使用せず、誰ともパスワードを共有しないでください。

※万一被害に遭われた場合、「1 3 1 - 4 4 4」に電話し、警察に届けてください。

※参考 URL

○スキヤム・ウォッチ（最新手口の紹介）

[www.scamwatch.gov.au](http://www.scamwatch.gov.au)

○オーストラリア・サイバー・セキュリティ・センター（サイバー・スペース上での手口紹介・被害報告）

[www.cyber.gov.au](http://www.cyber.gov.au)