STOP. THINK. CONNECT.

－フィッシング詐欺について－

２０２６年１月２９日　安全対策邦人連絡協議会

自己紹介

- 元ビクトリア警察刑事/事件捜査に15年以上従事
- 緊急通報対応、被害者支援、地域パトロール、事件捜査等、幅広い警察実務に従事
- 刑事資格取得後は、武装犯事案、薬物犯罪、家庭内暴力、サイバー犯罪、特殊詐欺をはじめ、殺人、性犯罪、誘拐等
- 複数の捜査チームを率いて捜査管理や、国境を越えた捜査、日本を含めた外国当局との連携を要する国際性の高い案件にも多数関与
- 重大犯罪捜査官向け研修の講師・コーディネーター

フィッシング詐欺

偽ったメールやSMSで、本物にそっくりな偽サイト等を悪用して、
個人情報を盗み取るサイバー攻撃の手口

- 銀行やクレジットカード会社を装うSMSやメール
- Australia Postやその他宅配業者を装う通知 （不在通知等）
- MyGov / ATOを名乗る連絡
- 携帯会社や公共料金を装う通知や請求
- SNSのアカウントに関するメール（アカウントロック等）

フィッシング詐欺の共通点

- 実在する企業やブランドの偽装

👉 見分けられなくて普通！

- 緊急性を促す内容　（不正アクセス、口座が凍結等）

👉 人は不安になると、**確認行動を急ぐ**

- 期限の強調（本日中に、２４時間以内に等）

👉 **冷静に考える時間を奪う**のが目的

- 個人情報を要求する内容

👉 **ここが被害の入口**

- リンクやQRコードに誘導する
- 発信元が不審、宛名がない

例）example.com vs examp1e.com

狙われている情報

- 氏名、住所、生年月日などの個人情報
- 運転免許所、パスポートなどの画像情報
- ユーザーIDやパスワードのアカウント情報
- カード番号や暗証番号などの銀行・クレジットカード情報

盗まれた情報はどうなる？

- 不正決済・クレジットカード詐欺
- なりすまし口座開設（別詐欺に利用される）
- 不正契約（ローン、携帯電話等）
- 行政サービスの不正利用
- SNS、メールアカウントの乗っ取り、不正利用
- **ダークウェブなどの匿名性の高いサイトで売買**

Operation Cookie Monster

FBIが主導し、AFP、ニューサウスウェールズ州警察、ビクトリア州警察、クイーンズランド州警察、ウェスタンオーストラリア州警察が支援した国際捜査の結果、盗まれたアカウント情報や侵害されたデバイス情報へのアクセスを提供する有名な犯罪マーケットプレイスが閉鎖されました。

AFPとその協力機関は24件の捜索令状を執行し、3つの州で10名が逮捕されました。その中には、オーストラリアで最も多くの侵害情報を購入したと警察が主張するビクトリア州の男性も含まれます。

招待制のウェブサイトでは、ログイン認証情報、閲覧履歴、自動入力フォームデータ、その他侵害されたデバイスから取得された機微なデータが提供されていました。

閉鎖当時、Genesis Marketは150万台以上の侵害されたコンピュータへのアクセスを提供しており、それぞれのコンピュータには数十のアカウントに関する情報が含まれていました。

https://www.afp.gov.au/news-centre/media-release/10-australians-arrested-part-international-illegal-marketplace-takedown

被害にあわないための対策

- **正しいドメイン名かの確認を習慣化する**

- URLを安易にクリックしないで、公式サイトや正規のアプリからアクセスする
- 返信や記載された番号に電話しない
- 自分だけで解決しようとせず、まず相談

被害にあってしまったら？

- 銀行やカード会社に直ちに連絡
- パスワードの変更
- ReportCyberから通報　https://www.cyber.gov.au

今日のまとめ

STOP. THINK. CONNECT.

- **緊急性・短い期限・リンク・情報入力**
  この4点がそろったら詐欺を疑い、迷ったら相談
- **発信元**を確認しましょう
- 銀行の口座やクレジットカード情報、その他個人情報を入力するサイトへは、**メールやSMSで送られてきたURLではなく、公式アプリやサイトからログイン**


Any Questions ?