ESETとは、
ウイルスからあなたのコンピューターを守る
セキュリティソフトです

電子メールがハッキングされたかどうかを知るには？

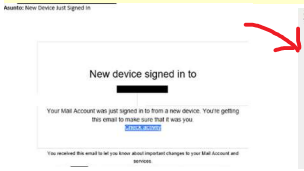
なぜ電子メールをハッキングしようとするのか？

全世界におけるサイバー犯罪の被害額は、年間で数百兆円に及ぶ。
これらの被害額で大きな割合を占めているのは盗難データの売買。この中に電子メールアカウントに保存されているデータが含まれている。
銀行取引明細書を会計士に送ったり、連絡先を含んだ賃貸契約書、あるいは機密情報を弁護士に送ったりしているのではないだろうか。

- クレデンシャルスタッフィング攻撃を実行する。ほかのアカウントでも同じログイン情報を使っていると推測し、自動化されたソフトウェアを介して、アカウントへの侵入
- ほかのアカウントをリセット→その電子メールにアクセスし、パスワードを変更
- すべての連絡先に、スパムやフィッシングといった悪意のあるメールを送信する。

電子メールアカウントがハッキングされたことを確認する方法

①受信箱や送信済みアイテムに見覚えのないメールがある。
②パスワードが変更され、アカウントからロックされた。
③自身のメールアドレスから友人へ、スパムメールが送られている。
④異なるWebサイトやアプリからパスワード変更依頼が複数届く。
⑤見知らぬIPアドレスや位置からのログイン試行が、メールプロバイダーから通知される。



送信先：xxx

件名：新しいデバイスからのログイン

新しいデバイスからxxxにログインがありました。
電子メールアカウントへ新しいデバイスからログインがありました。
あなたからのログインであることを確認するために電子メールを送信しました。
アクティビティを確認する。

再び電子メールアカウントがハッキングされるのを防ぐには？

①ほかのWebサイトで使い回しているパスワードや設定を変更する。
②多要素認証（MFA）を設定し、パスワードの盗用リスクを軽減する。
③マルウェアがないことを確認するよう、コンピューター全体をスキャンする。
④電子メールやテキストメッセージ、ソーシャルメディアなどで、見知らぬ送信元から要求されても、個人情報やログイン情報を入力しない。
⑤公共Wi-Fiや共有コンピューターで電子メールアカウントにログインしない。

※深刻な被害に遭ったら、ソーシャルメディアやBCCで主要な連絡先に知らせる