回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.60

あさまセキュリティニュースレター

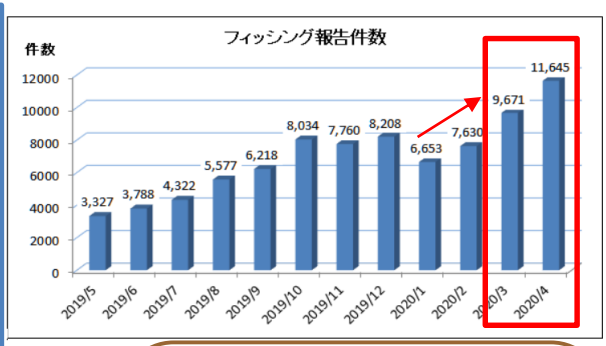
フィッシングメール急増中、細心の注意を！！　（2020年5月13日）

日本データ通信協会　HP抜粋　5月の要注意メール例

- LINEになりすました偽メール「件名：LINEにご登録のアカウント（名前、パスワード、その他個人情報）の確認」（本偽メールは、実在の企業と無関係に送信されたものです）
- Amazonになりすました偽メール「件名：Amazonアカウントを利用制限しています」（本偽メールは、実在の企業と無関係に送信されたものです）
- Appleになりすました偽メール「件名：Apple IDについての重要なお知らせ」（本偽メールは、実在の企業と無関係に送信されたものです）
- PayPayになりすました偽メール「件名：【PayPay】アカウントの異なる端末からのアクセスのお知らせ」（本偽メールは、実在の企業と無関係に送信されたものです）
- Amazonになりすました偽メール「件名：Amazonプライムの自動更新設定を解除いたしました！」（本偽メールは、実在の企業と無関係に送信されたものです）
- 楽天になりすました偽メール「件名：セキュリティ対策のため、楽天アカウントがロックされています」（本偽メールは、実在の企業と無関係に送信されたものです）
- 楽天になりすました偽メール「件名：楽天市場【セキュリティアラート：Google Chrome for Windows(デスクトップ)新しいサインイン】」（本偽メールは、実在の企業と無関係に送信されたものです）

その他、地方銀行やネット銀行、クレジットカードブランド、オンラインショッピング（ヨドバシカメラ等）をかたるフィッシングメールが出回ってます

フィッシング対策協議会　HP抜粋



外出自粛により、家でネットのサービスを利用することが増える一方で、攻撃者はそこを狙ってきています！手口も巧妙化、知らない間に、偽サイトでメールアドレス、パスワードを入力しているかも、、、正規サイトか疑わしいところで入力してしまった場合は、パスワードの変更を！
今後マスクや給付金をかたるメールにもご注意ください！！

攻撃のパターン

- 日常使用する各種サービスからのメールを装い、偽サイトへ誘導、利用している**実際のID・パスワードを入力させる**。ログイン後、個人情報やカード情報を入力させる
- 入力した情報を元に、各サービスへログイン、不正利用

（同じメールアドレス・パスワードの組み合わせ（**パスワードの使いまわし**）の場合、他サービスでも不正ログインされてしまう）

被害

不正アクセス　**登録情報の搾取**　**サービスの不正利用**　**他サービスでも不正アクセス被害**

対策

- よく利用しているサービスは不正メールがあることを知る、**定期的に下記情報源からご確認を！**
- メールのリンクからアクセスせず、正規のURLをお気に入り等に登録、毎回WEBブラウザから開く
- パスワードの使いまわしは避ける、サービスごとにID・パスワードの組み合わせを変える

情報源

フィッシング対策協議会　https://www.antiphishing.jp/report/monthly/202004.html

一般財団法人 日本データ通信協会　https://www.dekyo.or.jp/soudan/index.html　　JC3　https://www.jc3.or.jp/

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414