

【重要】インターネットバンキングを狙う新たなマルウェアについて

先般、マスコミにて報道されておりますように、インターネットバンキングを狙う新たなマルウェア (DreamBot) が猛威を振るっています。このマルウェアに感染した端末を使用していると、ID、パスワード等の認証情報を窃取され、不正送金が行われてしまう恐れがあります。

インターネットバンキングサービスをご利用のお客様におかれましては、下記の対策を実施のうえご注意くださいようお願い申し上げます。

なお、一般財団法人日本サイバー犯罪対策センターより「[DreamBot・Gozi 感染チェックサイト](#) (試験運用)」が提供されておりますので、ご参照ください。

記

1. 不審なメールに注意

今回のマルウェア (DreamBot) は、感染経路として「電子メール」が利用されています。「写真」や「注文書」等のファイルが添付された心当たりのないメールは開かないようご注意ください。

2. パソコンおよびウイルス対策ソフトのアップデート

パソコンには必ずセキュリティソフトを導入し、ウイルス定義ファイル等を最新版へアップデートしていただくとともに、ウイルスに感染していないことを定期的にご確認してください。

また、パソコンの基本ソフト (OS) やブラウザ、その他のソフトウェアについても常に最新の状態に更新してください。

3. パスワードの定期的な変更

パスワードは必ず定期的に変更してください。

4. セキュリティ機能のご利用

(1) 個人向けサービス

ワンタイムパスワード機能もしくはメール通知パスワード機能

※サービス画面より随時ご利用開始が可能です。

(2) 法人向けサービス

電子証明書方式ログイン機能およびワンタイムパスワード機能

※ご利用の際は、書面によるお申込が必要です。

(3) 個人向け法人向け共通

「PhishWall (フィッシュウォール) プレミアム」 (不正送金、フィッシング対策ソフト)

※当組合ホームページよりインストールしていただき、無料でご利用いただけます。

【ご連絡先】

・覚えのない取引をご確認された場合

大分県信用組合業務支援部 (信組 ATM センター) : 097-536-6118

0:00~24:00 (但し、平日夜間及び土日祝日は「信組 ATM センター」に繋がります。)

・その他サービス全般に関するお問い合わせ

けんしん ITバンキングサービスサポートセンター : 0120-373-883

平日 9:00~24:00 / 土日祝 9:00~17:00 (但し 12/31、1/1~1/3 を除きます。)