産学官連携ニュース No.9

H29.12.15

不正送金被害につながるウイルス感染に注意

H29.10 ころから、実在企業やサービスを騙ったメール  が大量配信されており、添付ファイルの開封や、本文中に記載のリンクをクリックすることで、コンピュータウイルス「DreamBot」に感染させられます。

「DreamBot(ドリームボット)」に感染するとどうなるの？

DreamBot は、利用者が入力した ID やパスワード等を窃取する機能、またコンピュータを遠隔操作する機能を持っています。

金融機関のインターネットバンキング用認証情報やクレジットカード情報等を窃取され、犯人にコンピュータを乗っ取られ、遠隔操作により、銀行口座から預金が不正送金されてしまうおそれがあります。

対　策

○パソコンのＯＳ、アプリケーションを更新
○ウイルス対策ソフトを導入、更新
○メールの添付ファイルを不用意に開かない
○メール本文中のリンク先を不用意にクリックしない
○ワンタイムパスワードや二経路認証を活用する

金融機関が推奨するセキュリティ対策を参考にしましょう

JC3(日本サイバー犯罪対策センター)で感染をチェックできます

「DreamBot・Gozi 感染チェックサイト」(試験運用)
https://www.jc3.or.jp/info/dgcheck.html

年明けは、処理を急ぐあまり、たまったメールを不用意に開いてしまいがちです。ＯＳやウイルス対策ソフト等を更新した上で、開封・閲覧には細心の注意を払って感染しないようにしましょう！！

参考：警察庁、JC3

本件問い合わせ先：岐阜県警察本部生活環境課サイバー犯罪対策室　058-271-2424（内線 3051,3237）