個人情報を狙った偽の入力画面に注意

この秋以降、新たな手口でインターネットバンキングでの送金に必要な暗証番号等の個人情報を盗み取り、不正に送金する犯罪の被害が増えています。

■手口

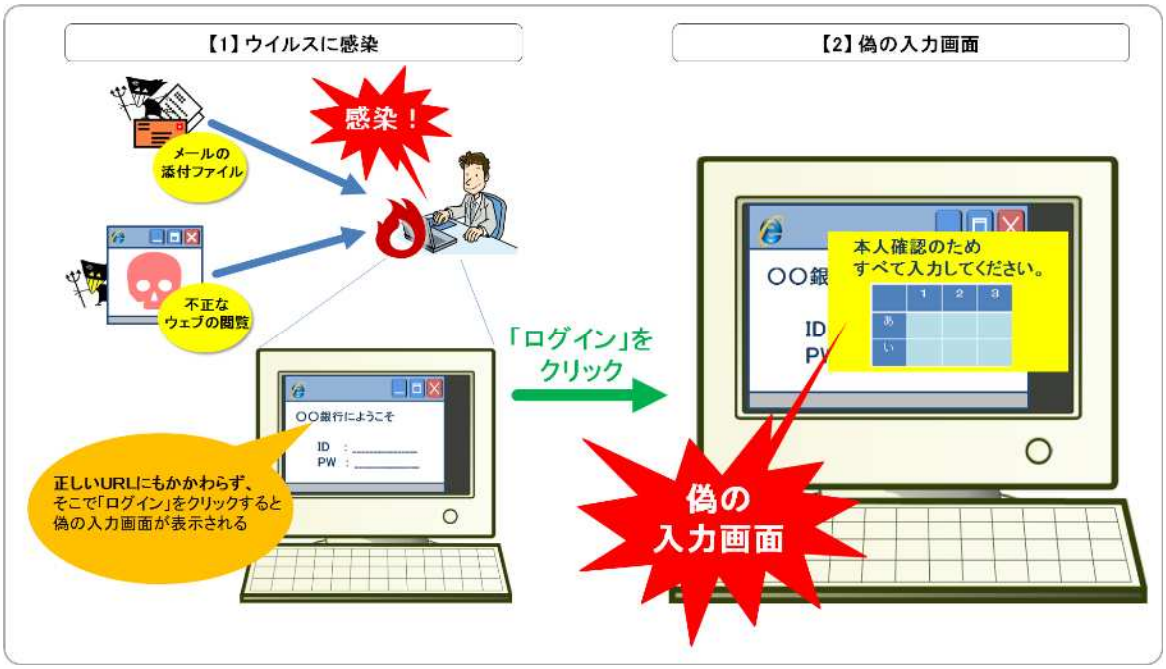
これまで、インターネットバンキング利用者のIDやパスワードをだまし取る手口として、銀行やクレジット会社などの企業を装ったホームページや電子メールを利用して、個人のIDやパスワードを聞き出そうとするフィッシング行為が多く行われていました。

しかし、最近、利用者が金融機関の本物のホームページからログインすると、第2暗証・質問、合言葉・インターネット用暗証番号などの入力を求める偽の入力画面が表れ、個人情報を盗み出そうとする新たな手口が発生しています。

■問題点

新しい手口では、本物のサイトを利用中、その画面にかぶさるような形で偽の入力画面が表示されるため、表示されているＵＲＬからは、偽物であることを判別できません。また、本物のサイト画面が表示された後なので、一見すると本物の画面と間違えてしまいます。

このような画面が表示されたパソコンを解析したところ、偽の入力画面を表示すると見られるウイルスが検出されました。



■対策

利用者は日頃から以下の対策をとることが望まれます。

【インターネットバンキング利用時の注意点】

○　不審な入力画面が表示された場合、個人情報は入力せず金融機関等に通報する

○　乱数表や合言葉などを一度に全て入力しない（インターネットバンキングを行う金融機関が個人情報全ての入力を求めることは通常ありません）

【ウイルスに感染しないために】

○　身に覚えがないメールは開かない

○　不必要なプログラムや信頼のおけないサイトのプログラムをダウンロードしない

○　こまめにＯＳやソフトのアップデートを行う

○　使用しているパソコンにセキュリティソフトウェアを導入し、ウイルスを駆除する

また、インターネットバンキングを行う金融機関では、以下のような対策を通じて犯罪の防止に資することが望まれます。

○　一定の時間に限り有効な「ワンタイムパスワード」の導入

○　自社サイトで正規のログイン手順や過去の犯罪の手口を示して利用者の注意を喚起する

なお、同様の手口は、インターネットバンキング以外の分野でも使われるかもしれません。どのようなサイトでも、不審な入力画面が表示された場合には個人情報を入力しないなど、十分に注意をして下さい。