サイバーセキュリティ通信【第20号】

令和元年10月
大分県警察本部生活安全部
サイバー犯罪対策課

SMBC契約者を狙うフィッシング詐欺が急増中！

本年9月ころから、三井住友銀行を装ったショートメッセージや電子メールを利用したフィッシング詐欺に関する被害が全国的に急増しています！

届いた偽メールの内容に従って、アカウントのIDやパスワードを入力した人は、インターネットバンキングにおいて不正送金を行われる被害も確認されています。

メール内では、正規サイトにアクセスするように見せかけて、実際にアクセスすると偽サイト（フィッシングサイト）にアクセスさせるという手口も用いられており、被害防止対策には十分な注意が必要です。

フィッシングメールの内容は非常に巧妙です！

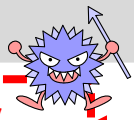
【フィッシングメールを使った犯行手口】

1　アカウントの不正使用の可能性やパスワードの変更を通知する三井住友銀行を装ったメールが届く。
2　メールに記載されたＵＲＬ（三井住友銀行の本物のURLのハイパーリンク）にアクセスすると、正規ログイン画面とそっくりなフィッシングサイトが表示されて、口座番号、暗証番号、本人確認情報の入力を求められる。
3　求められた口座番号等を入力すると、口座番号等が盗み取られ、インターネットバンキングサービスにおいて不正な送金がされる。

振込手数料引き上げに伴うSMBCダイレクトの各種手数料改定について、お客様の三井住友銀行口座のセキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定をしてください。

ご入力いただいた内容で所定の審査をすすめさせていただきます。
ご確認については、こちらから確認ください。
https://www.smbc.co.jp

【不審なメール文の例】



× http://www.uso800.com/ ←― **実際にアクセスするURL**

正しい三井住友銀行のインターネットバンキングサービスのURLは

○ **https://direct.smbc.co.jp/･･･**
○ **https://direct3.smbc.co.jp/･･･**
○ **https://mb.smbc.co.jp/･･･**

のいずれかです。

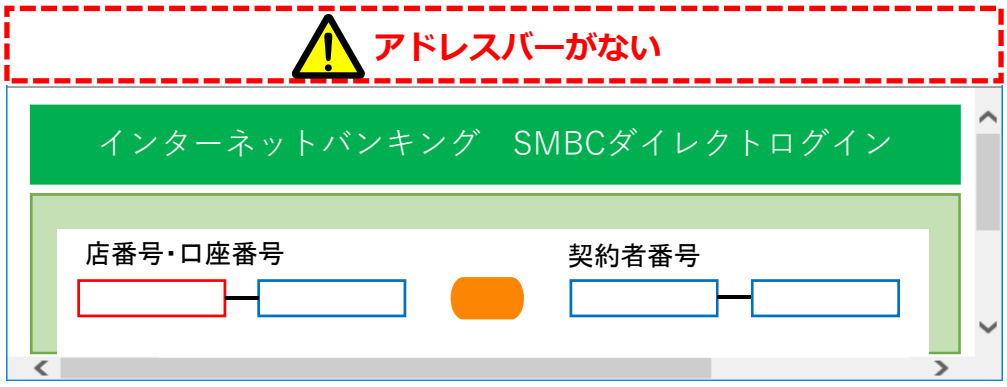
ただ、メール中のURLをクリックして直接アクセスすることなく、正規サイトからアクセスするように心がけて下さい。

フィッシングサイトの特徴

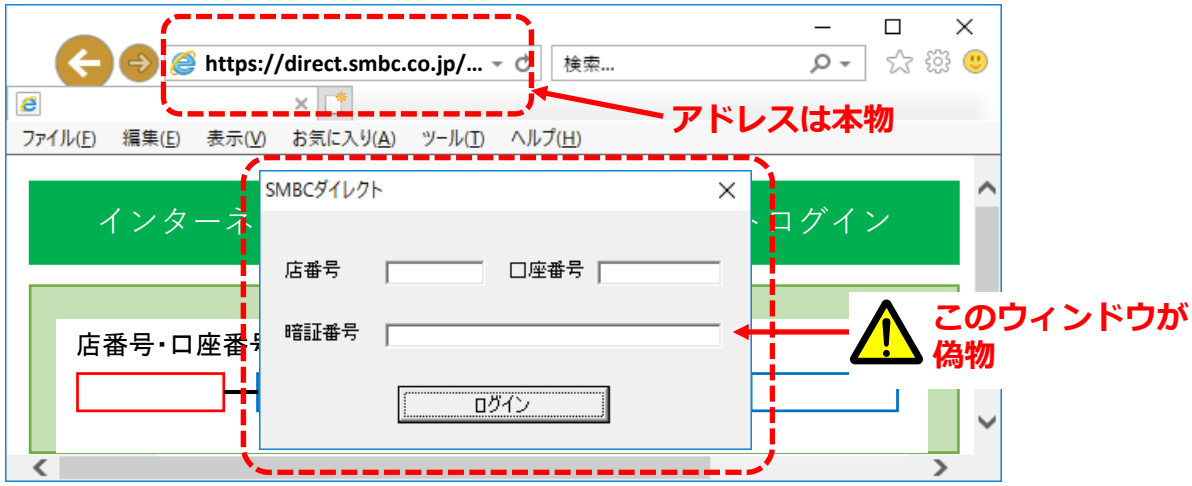
フィッシングサイトの内容には、次のような特徴があります。

①

②



③



これらはあくまでも一例で、見破るには注意力と知識が必要になります。

- インターネットバンキングを使う端末は
  - ○　可能な限りインターネットバンキング専用端末を用意する（メールを閲覧する端末でインターネットバンキングを使用しない）
  - ○　フィッシング対策ソフトやアンチマルウェアソフトを導入する

などの対策を確実にとるようにお願いします。

銀行等各サービス提供者のウェブサイトでは典型的事例や最新事例が紹介されていますので、ウェブサイトを閲覧して犯人の手口を学ぶことも大事です。

あなたの会社や団体で研修の一環として、サイバーセキュリティセミナーを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。
大分県警察本部生活安全部サイバー犯罪対策課
企画・指導・サイバーセキュリティ係　Tel:097－536－2131