



サイバーセキュリティの置き薬

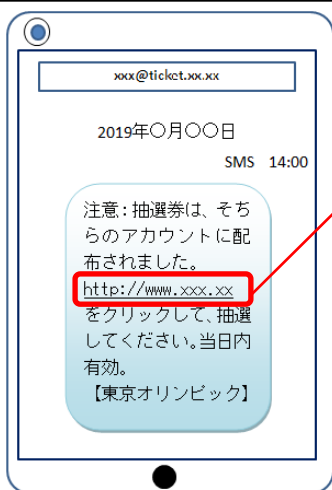
2019年
第8号

突如スマホに届いた東京五輪のSMS、それって本物？

東京五輪のチケット抽選に関係があると見せかけた偽のSMSが、スマートフォンに送られる事例が全国で確認されています。これは、個人の情報を盗む「フィッシング詐欺」の手口と判明しており、今後、東京五輪に関わる様々な手口が出回る可能性もありますので、十分に注意してください。

偽のSMSの画面（例）

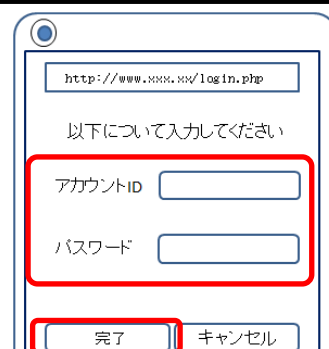
SMSを送りつけて開封させ、URLから偽のサイトにアクセスさせる。



正規サイトを装う偽サイトを表示させ、抽選に関する入力ページに誘導する。



フィッシングサイトに誘導され、表示画面にIDやパスワード等を入力させる。



入力して完了をクリックしてしまうと、情報（ID、パスワード）が盗まれてしまいます。

Check! 公式サイトのドメインは「tokyo2020.org」と「tokyo2020.jp」の2つになっていますが、「2020」の部分が「2o2o」のような偽物も出回っています。

Check! 大会組織委員会は抽選結果のメールについて、**詐欺防止**のため

- 本文にURLを記載しない
- はがきやSMSは使用しない

としているので、注意してください。

【ワンポイントアドバイス】



- ☆ 抽選に関する情報は、**大会組織委員会に対して確認する！**
- ☆ 不審なメールは**開かない！ URLはクリックしない！**
- ☆ パスワード・暗証番号等の個人情報を**安易に入力しない！**