proofpoint.

HUMAN FACTOR 2017

不正なメールはコードではなく、人の弱点を 利用します。

サイバー犯罪者は様々な手口でユーザーを騙し、不正なメールやソーシャルメディアの投稿を開かせようとします。2016年に顕著だった傾向をまとめました。



ビジネスメール詐欺 (BEC) 攻撃が急増

2015年に1%だったBECのメッセージ量は **2016年の終わりには42%**に増加しています。



ソーシャルメディアを 利用したフィッシング詐欺

2016年はソーシャルメディアアカウントによるフィッシング詐欺が**150%増加**しました。



曜日によってマルウェア の種類が異なる ランサムウェアは**火曜日から木曜日の間**に

出現する傾向があります。



時は金なり

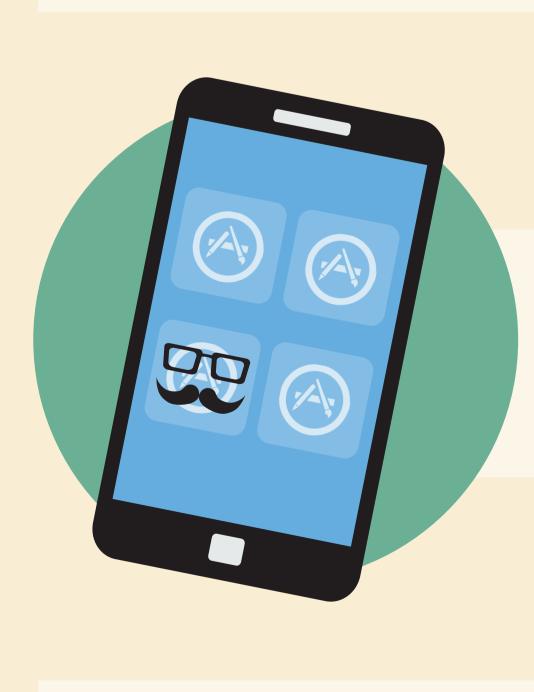
不正なURLのクリックの87%は 最初の24時間以内行われています。





攻撃のピークは日中 仕事が始まってから**4~5時間後がクリックの**

ピーク。ちょうど昼休みが危ない時間帯です。



偽のモバイルアプリ

不正なアプリは、**ブランドを装い、紛らわしい 名前を使って**ユーザーにマルウェアを
ダウンロードさせようとします。

スマートフォンの増加で リスクも増大 不正なURLのクリックの42%は

モバイルデバイスで発生しています。 **昨年の20%から倍増**しています。



レポートの完全版をダウンロード proofpoint.com/jp/resources/human-factor-report-2017-form