テレワーク時の安全確保のカギはコミュニケーション：CrowdStrike CSO から皆様へ

31 March 2020 | Shawn Henry (CrowdStrike)

サイバーセキュリティのプロフェッショナルたちによって、組織の保護機能は日々大きな進歩を遂げています。しかし、世界中のあらゆるテクノロジーをもってしても、ユーザーと資産を完全に保護することはできません。そのためには、個々のユーザーが注意を払い、常に警戒することも必要なのです。このことは現在のコロナウイルス（COVID-19）による危機的状況においても、まったく同じです。これほど多くの企業が、テレワークへの迅速な移行を迫られるなか、注意・警戒・通知は、私たち皆のスローガンとしなければなりません。

CrowdStrike の CSO として、社内のセキュリティ確保のために重要なのは、当社のすべてのチームとの頻繁かつオープンなコミュニケーションを行い、彼らが組織として、また個人として、日々直面する脅威を認識し、それに対する準備を行えるようにすることです。セキュリティリーダーが関係者に連絡を取り、最近の攻撃者グループの活動に伴い増大するリスクに対する警戒を訴えることが特に重要です

詐欺の手口とソーシャルエンジニアリング

攻撃者グループらが、人間の感情の 1 つである「恐れ」を悪用しようとするのは、驚くことではありません。現在、私たちは感情的にも弱くなっています。攻撃者らはそこに目を付けているのです。危機的な状況下において、人は適切な判断ができなくなる傾向にあります。悪質なハッカーや詐欺師らは、そこに付け込もうとします。

最近では、コロナウイルスの世界的大流行に乗じた詐欺の手口が増加しています。CrowdStrike® Intelligence チームは、その多くの例を収集し、周知しています。ソーシャルエンジニアリングは、企業に侵入するための最も有効な方法であるため、多くの攻撃者に採用される手法です。また、攻撃者らはパンデミックを悪用して、個人情報や企業の知的財産を盗もうとしています。攻撃者らは、COVID-19 の最新情報を公開しているように見せかけた悪質な Web サイトやアプリを利用して、マルウェアをユーザーのデバイスに送り込み、ユーザーの情報を盗んだり、デバイスをロックして身代金を要求します。皆が最新のニュースを知りたいと考え、このような戦術に釣られてしまいます。しかし、私たちは恐怖によって判断力を鈍らせるわけにはいきません。私たちが警戒を緩め、このような詐欺に屈すれば、敵の勝ちです。

ソーシャルエンジニアリングでも、最近のテレワークの増加に付け入る隙を狙っています。テレワークする従業員が増えるほど、ソーシャルエンジニアリングのリスクも高まります。同僚と対面することが少なくなった無防備な従業員を騙すのはずっと簡単です。「IT 部門」からというその通話は、本当に IT 部門からのものでしょうか。「Apple」からの E メールは、本物でしょうか。いったん落ち着いて、自問自答しましょう。その電話やメールの相手は、本当に名乗ったとおりの人物なのか。

オンライン上で安全を確保するための推奨事項

私たち皆の安全のために、すべてのユーザーに、以下のような注意喚起を行ってください。すでに皆が知っていることかもしれませんが、今はその記憶を呼び起こすべき時だと思います。

- 知らない相手からの E メール内のリンクは絶対にクリックしないこと。まずは、リンクを観察してみましょう。信ぜよ、されど確認せよ！
- 知らない相手からの E メールの添付ファイルは開かないこと。
- アカウント情報の提供や確認を求める内容の E メールや通話には気を付けること。
- E メールや自動音声電話で、あなたのユーザー名やパスワード、誕生日、マイナンバー、口座情報などの個人情報を聞かれても、決して応じないこと。
- 正当なソースから要求された情報を常に個別に検証すること。
- 正当な Web サイトのアドレスを確認して、ブラウザ内に手動で入力すること。
- リンクアドレスに、スペルミスや不正なドメインがないかよく観察する（たとえば、アドレスの末尾が「.gov」であるはずのところ、「.com」となっているなど）。
- 送金あるいは情報の送信をする前に、電話やテレビ電話で先方に確認をとる。
- 消毒用品や防護具の販売、あるいは COVID-19 の予防、治療、診断、治療のための製品については、偽物に注意すること。

セキュリティ意識の向上は、被害に遭わないための最良の方法です。攻撃の標的となっている兆候を見つけるには、一般的なソーシャルエンジニアリングの手口を知っておくことが重要です。「自分はソーシャルエンジニアリング攻撃の被害に遭っているかもしれない」と従業員が疑った場合には、IT セキュリティ担当者に連絡できるようなプロセスが整備されていることを確認してください。

COVID-19 に関する正確な最新情報を求めている方向けに、CDC（アメリカ疾病予防管理センター）では広範なガイダンスと情報を公開し、内容を頻繁に更新しています。COVID-19 に関する正確な情報ソースとして最適なサイトは、**www.cdc.gov** および **www.coronavirus.gov** です。

CrowdStrike 新型コロナウイルス（COVID-19）とサイバーセキュリティ リソース Web ページでも、御社とテレワーカーのセキュリティ確保に役立つ情報を入手できます。

皆さまの今後の安全をお祈りするとともに、オンラインのご利用および在宅勤務のセキュリティについても十分に注意されることを願っております。これらの困難な時期には、私たちが自分自身の精神面、肉体面、感情面に気を配ることが非常に重要です。CrowdStrike では、私たちのお客様の組織とあらゆる場所で勤務されている従業員の皆様を守るために全力を尽くしています。しかし、この嵐を無事に乗り切るには、すべての人の意識と警戒心が不可欠です。

Shawn Henry（CrowdStrike）

追加のリソース

- CrowdStrike の既存お客様向けの、**新規テレワーカーの安全性確保**を目的とした 2 つの新プログラムについて、是非ご一読ください。
- COVID-19 時代のサイバーセキュリティへの対応に関して、**CrowdStrike の CEO、George Kurtz** がブログで発信しています。
- COVID-19 蔓延時におけるサイバーセキュリティ上の課題や、テレワーカーの安全のための推奨事項に関する詳細については、**CrowdStrike の CTO、Mike Sentonas** および**チーフプロダクト・エンジニアリング・オフィサーの Amol Kulkarni** のブログをご覧ください。