Case study

アメリカ、テキサス州のダラス・フォートワース大都市圏に位置するガーランド市 が 職員のトレーニングによりビジネスメール詐欺攻撃を阻止！

“Wombatのセキュリティ・アウェアネス/トレーニング・プログラムは テキサス市が電信送金詐欺攻撃を回避するのに貢献しました！“

ケーススタディのハイライト

完璧なセキュリティ・アウェアネス・トレーニング・プログラム

・簡潔なティーチャブル・モーメントと組み合わせた月1回のシミュレートされたフィッシング攻撃
・フィッシングおよびその他のサイバーセキュリティのトピックについての継続的なインタラクティブ（対話型）・トレーニング
・エンドユーザが疑わしいメールを容易にレポートすることを可能にする、ワンクリックのレポートツール
・ガーランド市 からの指針に基づいてFuture Comによって管理・提供されるWombat製品

ますます積極的に関与する従業員基盤

・1年目から2年目で平均クリック率が80%低減
・レポートツール導入後の2ヵ月間で、200以上の疑わしいメッセージがエンドユーザによってレポートされた
・サイバーセキュリティ・アウェアネスを新人職員研修プログラムに統合
・電話ベース/メールベースのBEC攻撃の回避
＊BEC (business email compromise) ビジネスメール詐欺攻撃

● ガーランド市(テキサス州のダラス・フォートワース大都市圏の一部）が最初に職員向けのセキュリティ・アウェアネス/トレーニングを実施することを検討していた時、それは最優先事項と見なされていませんでした。それが完全に変わったのは、ガーランド市のITサポートサービスマネージャであるシャノン・メヒア(Shannon Mejia)氏がTAGITM(Texas Association of Governmental Information Technology Managers)主催のイベントに参加した時でした。

このイベントで、メヒア氏は、Future ComのCTOであるクリス・ボイキン(Chris Boykin)氏の話を聞きました。
ボイキン氏が行った「Securing Layer 8…The Human Security Factor」と題したプレゼンテーションは、リスク管理を見直して人間の行動を考慮することのメリットを強調したものでした。

Wombat Security Technologiesのパートナーとして、Future Com（コンサルティング会社）は、組織がサイバーセキュリティに対する全体的なアプローチ、即ち、技術的な予防対策と従業員のアウェアネス/トレーニングの取り組みを融合させるアプローチを取る必要性を認識しています。

このプレゼンテーションは、メヒア氏がガーランド市職員向けの新しいサイバーセキュリティ教育プログラムを支持するのに拍車をかけました。メヒア氏の粘り強さとFuture Comのアプローチがガーランド市に適したアプローチであるという信念はすぐに報われましたが、メヒア氏は当時、その決定がいかに重要なものとなるかには気付いていませんでした。

● プログラムについて

エンドユーザに対してプログラムを正式に開始する前に、メヒア氏はFuture Comと連携して、シミュレートされたフィッシング・キャンペーンをガーランド市職員に送信しました。ボイキン氏は、その結果をタウンホール形式のミーティングでガーランド市の部長(Manager)、役員(Director) 、その他の職員に提示しました。

フィッシングテスト(1,300人以上のユーザに送信されたデータ入力のシミュレートされた攻撃)によって生じた31%の失敗率は、セキュリティ・アウェアネス・トレーニングの必要性を明確に示すものであり、ボイキン氏の有益な プレゼンテーションは、プログラム開始への道を開くのに貢献しました。

Future Comは、メヒア氏の仕様に合わせてプログラムを実行するマネージドサービスとして、ガーランド市と連携しています。
ガーランド市は、以下のサイバーセキュリティ・アウェアネス/トレーニングのツールを使用して、メールを利用するガーランド市職員全員、ならびにガーランド市を拠点とする地元のエネルギー会社の約200人のエンドユーザを判定・教育しています。この公益企業は、ガーランド市職員によって実現された改善について聞いた後、2年目のプログラムの期間中に当該プログラムに含めて欲しいと依頼しました。

GARLAND TEXAS MADE HERE　Future Com

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

● フィッシング判定: シミュレートされた攻撃が現実世界の脆弱性を明らかに

Future Comは、WombatのThreatSim®フィッシングシミュレーションを使用して、月に1回または半月に1回のペースでフィッシングテストをエンドユーザに送信しています。又、マネージドサービスチームは、このツールから(キャンペーンパフォーマンス統計、個々のクリック率などを含む)データを収集し、経時的に進捗を追跡しています。

メヒア氏は、Future Comのチームに主題とスタイルの両方が異なるキャンペーンを作成する専門知識を活用するよう依頼しています。Future Comはデータエントリのキャンペーン、リンクベースのキャンペーン、添付ファイルベースのキャンペーンを組み合わせたものや、企業スタイルのメッセージ、ITおよびソフトウェアをテーマにしたメール、消費者志向の模擬攻撃を含む様々なトピックをカバーするテンプレートを使用しています。このアプローチは、受信者が最も影響を受けやすい攻撃のタイプをFuture Comとメヒア氏が特定するのに役立っており、このことは、ガーランド市のサイバーセキュリティ脆弱性に関する幅広い理解を得るのに役立っています。

「私は、(重要なのは)仕事だけではないということをユーザに知らせています。私は、私たちと一緒に学習するスキルが有用且つ移動型であることをユーザに印象付けようとしています。」 シャノン・メヒア氏、ガーランド市

フィッシングテストは、判定ツールであるだけでなく、アウェアネス・ツールでもあります。それぞれのシミュレートされた攻撃は、カスタマイズ可能なティーチャブル・モーメントと組み合わせることができ、これらのジャストインタイムのティーチング・メッセージは、模擬フィッシュに引っ掛かった全てのエンドユーザに対して表示されます。

ティーチャブル・モーメントは、フィッシングテストの目的を説明し、今後のミスを防止するのに役立ち得る簡潔ですぐに利用可能なヒントを提供することによって、コンテキストを従業員に提供します。また、ティーチャブル・モーメントは、プログラムの一部であるガーランド市全体のトレーニングの割り当ての段階を設定するのにも役立ちます。

● インタラクティブ(対話型)・トレーニング・モジュール

職員には、1年を通してずらして配置されている複数のWombatトレーニング・モジュールが割り当てられます。
メヒア氏がWombatのトピック・ライブラリからモジュールを選択し、Future Comが割り当ての配信を管理し、トレーニングの修了、最も間違えられた質問、その他のエンドユーザのやりとりに関するメトリックを追跡しています。

全てのユーザが同じトレーニングの割り当てを受け取り、修了は任意です。
ガーランド市は、メールセキュリティ及びURLトレーニングに重点を置いたアンチフィッシング・モジュールからプログラムを開始しましたが、ソーシャルエンジニアリング詐欺、パスワードのベストプラクティス、インターネットの安全性についての教育も提供しました。ガーランド市は、1年を通して定期的にトレーニングを提供する柔軟性があることや、Wombatのモジュールがオンデマンドで利用可能であり、トピックに応じて修了まで5～15分しかかからないことを考慮すると、アプローチが非常に管理し易いものであることを高く評価しています。

メヒア氏は、ユーザが迅速でインタラクティブなフォーマットに対する高い評価を口にしていることに言及しています。
「職員は、トレーニングセッションに1時間かける必要がないという事実を高く評価している、と言っていました」とメヒア氏は述べています。

「職員はその速さを気に入っており、トレーニングを受けるのが楽しいとまで言っていました。職員は、私たちが職員に教えようとしている内容を学習することは難しくないと感じており、ユーザが有意義な体験をしていることはプラスであることが分かっています」

● メールレポート

ガーランド市の職員は、長い間、疑わしいメールを監視対象の受信トレイにレポートするよう勧められていましたが、最近Future ComがWombatのPhishAlarm®メールレポートツールを展開したところ、このプロセスは、ユーザにとってもITチームにとっても、より容易になりました。

このメールクライアント・アドインにより、ユーザは、マウスを1回クリックするだけで、疑わしいフィッシングメールをガーランド市の情報セキュリティ(infosec)対応チームに転送することができます。

「私達は、職員が起こり得ることをより意識するようになるのを実際に見てきました。間違いなく、従業員はメールをクリックする前にもう一度よく考えており、確信がないときは私たちに連絡してきます。」 シャノン・メヒア氏、ガーランド市

● 新規雇用者の新人研修で重視されるサイバーセキュリティ

ガーランド市のセキュリティ・アウェアネス・トレーニングの重視は、新規職員に第一印象を与える方法としての新規雇用者のオリエンテーションプロセスにまで拡大されています。新人研修プロセスの一部として、メヒア氏は、新規従業員にボイキン氏のタウンホール・プレゼンテーションのビデオを見せ、サイバーセキュリティ・トレーニングについての議論を促進しています。

メヒア氏は、主な目的の1つは、アウェアネス及び教育のメリットがガーランド市での毎日の仕事を超えて拡大するものであることを職員に理解させることであると述べています。「新規雇用者のトレーニング中に私が強調することの1つは、サイバーセキュリティプログラムは私生活でも間違いなく職員の役に立つことができるということです」とメヒア氏は述べています。

「私は、(重要なのは)仕事だけではないということ、個人メールアカウントでもフィッシングに引っ掛かる可能性がある(過去に引っ掛かった可能性がある)ということをユーザに知らせています。私は、私達と一緒に学習するスキルが有用且つ移動型であることをユーザに印象付けようとしています。」

コーネットソリューションズ株式会社
Cornet Solutions (TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

● 経時的に測定可能な改善

クリック率の大幅な低減

ガーランド市のユーザは、31%のベースライン失敗率から大きな前進を遂げました。プログラムの1年目に、Future Comは、17%をわずかに上回る(ベースライン判定を含む、すべてのキャンペーンにおける)平均失敗率を記録しました。プログラムの2年目の途中の第3四半期では、全てのキャンペーンにおけるガーランド市の平均失敗率はわずか3.4%まで下がりました。

「職員からの肯定的な結果が明確に見られました。数字がそのことを示しています」とメヒア氏は述べています。「フィッシングテストに失敗しているユーザ、リンクをクリックして個人データを入力しているユーザの数は、大幅に減少しました。」

● レポートされるメールの増加

「私達は、職員が起こり得ることをより意識するようになるのを実際に見てきました」とメヒア氏は述べています。
「以前は、ユーザはあまり質問しないように見えました。しかし今では、ユーザはより意識しており、定期的に質問しています。間違いなく、職員はメールをクリックする前にもう一度よく考えており、確信がないときは私達に連絡してきます。」

PhishAlarmツールにより、ガーランド市は、メールをレポートしている職員の数や職員が提出しているメッセージのタイプに対する可視性をより容易に得られるようになりました。ツール導入後の数ヶ月で、Future Comは、PhishAlarmボタンを使用して200以上のメールがレポートされたことに気付きました。これらのメールのうちの3分の2以上は、潜在的なフィッシングメールとして分類され、残りの3分の1は、シミュレートされたフィッシング攻撃でした。

「Wombatの簡単に理解できるインタラクティブ・トレーニングは、詐欺を発見するための実用的な方法をユーザに教えながら、ユーザの注意を引き続けるように設計されています。シミュレートされたフィッシング及びティーチャブル・モーメントと組み合わされたトレーニングは、セキュリティ・アウェアネスにとどまらず、セキュリティに関して実際に人間の行動を変えるためのメカニズムを提供します。」
クリス・ボイキン氏、Future Com

● 阻止されたBEC攻撃

このプログラムは、クリック率の低下とレポートされるメールの増加においてだけではなく、現実の脅威に対する対応においても測定可能な結果を示しています。実際、注意を怠らない職員が、ガーランド市に対して多大な損害をもたらすビジネスメール詐欺(BEC: business email compromise)攻撃になる可能性があったものを特定し、止めることができました。

「それは、私たちがベンダのうちの一社と考えていた会社からの電話で始まりました」とメヒア氏は述べています。「電話口の人は、会社の銀行ルーティング情報が変更になったと言いました。その人は、新しい情報を経理部にメールすると述べ、適切なメールアドレスを尋ねました。」電話口の人物はガーランド市が頻繁に取引しているベンダの社員と名乗ったので、電話に出た職員は、電話をしてきた人に快くメールアドレスを教えました。メールが受信されると、そのメールは、そのベンダとの関係を管理するガーランド市の施設部に転送されました。

「幸いなことに、そのメールを開いた職員は、銀行の情報のような機密のトピックを含むメッセージについてもう一度よく考えることをトレーニングから知っていました。そのことがこの職員に警鐘を鳴らしたので、この職員はさらに詳細に調査しました」とメヒア氏は述べています。「この職員が、送信者のメールアドレスが以前のメールアドレスとはわずかに異なることに気付いたのはその時でした。
今回は、以前のメールアドレスにはなかったハイフンがドメイン名にあったのです。」

この職員は、**セキュリティ・アウェアネス・トレーニング**中に学習したベストプラクティスに従い、既知のコンタクトチャネルを介してフォローアップすることにしました。その後の電話で、ベンダは銀行ルーティング情報を変更していないことを確認しました。

行動する前にもう一歩踏み込んで確認することによって、この職員はガーランド市をBEC攻撃から守りました。

「次の週に、テキサス州の別の市で全く同じタイプの攻撃が起こったことを聞きました」とメヒア氏は述べています。
「残念ながら、その市の職員は詐欺だと分からず、だまされて詐欺口座に送金したため、数十万ドルを失いました。」

「私達の取り組みが大いに報われるのを見ることは驚くべきことでした。率直に言えば、これはサイバーセキュリティ教育の取り組みを続ける大きな動機になりました。私達は、職員に様々なものを見て、何かおかしいと思われる要求に注意することを教えてきました。職員は実際に私たちの期待に応えてくれました。私は、トレーニングを提供していなければ同じ結果を得られたとは思わない、と抵抗なく言えます。」

GARTNER'S MAGIC QUADRANT

Wombat Security Technologies社のセキュリティ・アウェアネス(認識)及びトレーニングソリューションは、3年連続して Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors のリーダーとなっています。

コーネットソリューションズ株式会社
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

変化をもたらし続けるパートナーシップ

Future Comは、ガーランド市系列のその他の部署と連携していますが、メヒア氏との関係は、厳密に言えば、TAGITMイベントでのボイキン氏の洞察に満ちたプレゼンテーションによって始まったものでした。「クリスに会った瞬間から、クリスとFuture Comは自分たちが何について話しているか分かっていること、Future Comであれば**セキュリティ・アウェアネス・トレーニング**において正しい方法で私たちを導くのを任せられることが分かりました」とメヒア氏は述べています。

一方、Future Comは、Wombat Securityとパートナーになり、同社の業界トップの判定・教育・強化・レポートツールを使用して効果的なセキュリティ・アウェアネス/トレーニングのサービスをクライアントに提供することを嬉しく思っています。「ガーランド市は、特に『人間のセキュリティ要因(human security factor)』に関してセキュリティ体制を改善しようとしていた時、Future Comに連絡してきました。

Wombatはフィッシュやその他の人間をベースとした攻撃に引っ掛かることに関して人間の行動を改善することに安定した実績があるので、Future ComはWombatとパートナーになることを決めました」とボイキン氏は述べています。

「Wombatの簡単に理解できるインタラクティブ・トレーニングは、詐欺を発見するための実用的な方法をユーザに教えながら、ユーザの注意を引き続けるように設計されています」とボイキン氏は付け加えています。

「シミュレートされたフィッシング及びティーチャブル・モーメントと組み合わされたトレーニングは、セキュリティ・アウェアネスにとどまらず、セキュリティに関して実際に人間の行動を変えるためのメカニズムを提供します。私達は、ガーランド市ならびにその他のクライアントで実施されたベースラインのテストからその後の月1回のテストまでの著しい改善を見てきました。」

コーネットソリューションズ株式会社
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp