サイバーセキュリティ、フィッシング、スパム

参加者は、セキュリティの脆弱性を利用して利用者から情報を取得しようとする悪意のあるオンライン利用者について学びます。オンライン接続のリスクを説明する、より安全な行動を取るための対策を立てる、スパムメッセージを特定する、パスワードを尋ねる相手としてふさわしい人を見分ける、などができるようになります。

素材

- スパムの配布資料

オンラインのリスク

パート1

以下の内容を伝えます。

インターネットを利用している際にウェブページへのアクセス、オンラインでのコミュニケーション、データのダウンロードを行うだけで、リスクにさらされる可能性があります。アクセスしているウェブサイト、同じネットワークを利用している人、サードパーティなどが、あなたが閲覧しているときに位置情報やその他の個人情報を特定できる場合があります。

以下の質問を投げかけます。

オンラインセキュリティの脆弱性を利用して個人情報を見る可能性があるのは誰ですか？

1. 悪意のあるハッカーや行政調査などが考えられます。

以下の内容を伝えます。

ウェブを閲覧する際、悪意のあるハッカーは、インターネットプロバイダーが行うのと同じように利用者に関するデータを取得できます。このリスクを低減するために、アクセスしようとしているウェブサイトと利用者間のセキュアな接続を使用する必要があります。接続にかかわらず、多くのウェブサイトでは複数のプラットフォームにおける利用者の利用パターンをトラッキングしようとします。そのようなサイトは、ブラウザー、位置情報、その他の利用パターンを見て、利用者を特定しようとします。

以下の質問を投げかけます。

悪意のあるハッカーがオンラインで個人情報にアクセスしようとするのはなぜでしょうか？どのような情報を探しているのでしょうか？あなたがログインしていないウェブサイトが、あなたが誰であるかをトラッキングする理由は何でしょうか？

1. 個人を特定できる情報や、販売したり、金銭を得るために利用したりすることができる情報はありますか？

マルウェアとは何か知っている人はいますか？マルウェアは何ができますか？

以下の内容を伝えます。

マルウェアはあなたのコンピューターでひそかに実行される有害なコードです。マルウェアによっては、ハードドライブからブラウザーデータに至るまで、ローカル

コンピューターのどこにあるデータでも取得できます。また、マルウェアを使用すると、ハッカーが利用者のコンピューターをコントロールしたり、ハッカーが望むあらゆる方法に利用したりすることができます。ただし、大半のマルウェアは、銀行のような安全なポータルを模倣するウェブサイトや、利用者のブラウザーに広告を掲載して収入を得る拡張機能のように、シンプルなものです。

以下の質問を投げかけます。

マルウェア、スパイ行為、トラッキングから自分を守るにはどうすればよいでしょうか？

以下の内容を伝えます。

リンク、広告、ソーシャルメディア投稿をクリックする際は注意が必要です。URLは予想と一致していますか。もう一度そのURLを自分で入力したり、そのウェブサイトを検索したりすると、同じページにたどり着きますか。一般的に、SSLやTLSは重要なアカウント(Google、Facebook、Twitter、銀行口座など)のログインページを保護します。SSLやTLSを使用すると、あなたが正しいURLを入力した場合に、同じネットワークを利用しているハッカーがあなたに偽のサイトを表示することが非常に困難になります。SSLやTLSを使用しないと、とても簡単にできる可能性があります。

ウェブサイトによっては、このようなプラットフォームにコーディングミスがある場合に、利用者の個人情報やオンラインアカウントにアクセスするコードを実行できます。その後、利用者のアカウントを利用して他の人にスパムを送信できます。

信頼できるソースからのソフトウェアのみをダウンロードしたりインストールしたりするようにします。(.exe、.pkg、.sh、.dll、.dmgの拡張子の付いた)実行可能ファイルをダウンロードする際は特に注意するようにします。実行可能ファイルとはアクションを実行するファイルのことです。よくないアクションを実行する場合も考えられます。例えば、他人のハードドライブを消去したり、偽のブラウザーをインストールしたりするよう実行可能テキストを書くことができます。こうした理由から、信頼できるソースからのコンテンツのみをインストールするようにしてください。

ウイルス対策ソフトウェアを使用してマルウェアの実行を回避することもできます。コンピューターに付属しているウイルス対策ソフトウェアもあります(Microsoft Security Essentials for Windowsなど)。また、Appleコンピューターなどの一部のオペレーティングシステムには、信頼されていないソースからのソフトウェアがインストールされないようにする設定があります。このような設定を変更する場合は、事前に十分検討してください。

ブラウザーの拡張機能も利用できます。例えば、プラグインをブロックして、ウェブサイトが簡単に利用者を特定したりトラッキングしたりすることができないようにするものがあります。ただし、同じプラグインを使用することで、動画の視聴などウェブサイトの一部の機能を使用できなくなることがあります。ブラウザーの拡張機能をインストールすることを決めるかどうかは、利用者の好みや、オンライン

セキュリティの観点から見て代償を払ってもよいと考えられるかどうかによります。次のような質問について、じっくり考えてみましょう。トラッキングされることはどの程度都合が悪いですか。自分のプライバシーの価値はどれくらいですか。このコンテンツの一部をどの程度見たいですか(ブラウザー拡張機能によって動画を表示するプラグインがブロックされてもよいかなど)。

セキュリティツール

パート1

クラスインタラクション

注: このアクティビティの内容の一部は「アクティビティ1:
オンラインのリスク」に含まれています。 すでにアクティビティ1を行っている場合は、その部分をもう一度確認するか省略するかの判断はお任せします。

以下の質問を投げかけます。

インターネットを利用する際に自分の安全が確保されているかどうかを把握していますか？

以下の内容を伝えます。

正しい対策を取らなければ、このようなオンラインのリスク(前のセクションで説明したもの)から自分を守ることは、不可能ではないにしても難しくなります。

新たなオンラインのリスクも絶えず発生しているため、警戒しておくことが重要です。

以下の質問を投げかけます。

そのウェブサイトが実際に重要なウェブサイトであると他人があなたを納得させた場合、その人は何を行うでしょうか？

このようなリスクを回避するまたは低減するために使用できるツールがあります。このようなツールを知っている人はいますか？

以下の内容を伝えます。

HTTPSは、ウェブサイトがインターネットを経由するデータを暗号化するために使用する規格です。暗号化することで、利用者の接続からのデータをサードパーティが簡単に見ることができなくなり、セキュリティを強化できます。使用するURLの前に「https://」を追加すると(「https://www.mysite.com」など)、すべてのブラウザーで利用できます。ただし、すべてのウェブサイトでHTTPSをサポートしているとは限りません。

1. 取り扱いに注意を要する情報(パスワード、クレジットカード情報など)は、「HTTPS://」で始まるウェブページでのみ入力するようにしてください。

2. ソフトウェアツールを利用して、できる限り常にHTTPSを使用するようにできます。

3. ほとんどの主要なブラウザーでは、アドレスバーの近くに、HTTPS接続を示す鍵マークのようなセキュリティインジケーターが表示されます。

4. 残念ながら、HTTPSをサポートできる悪質なウェブサイトもあるため、HTTPSの場合でも利用者の安全が保証されるわけではありません。つまり、HTTPSは接続の安全を強化しますが、ウェブサイトに問題がないことを保証するものではありません。

セキュアソケットレイヤー(SSL)やトランスポートレイヤーセキュリティ(TLS)は、HTTPSの安全を確保する技術の名前です。SSLやTLSはデジタル暗号化キーを使用しています。これは実物の鍵のように機能します。例えば、紙に友達への秘密を書いた場合、その紙を見つけた人が秘密を見る可能性があります。一方、鍵のコピーを友達に手渡して、その鍵を使用してロックした箱に秘密をしまったとします。誰かがその箱を奪った場合、鍵がなければ簡単に秘密を見ることはできません。誰かがその箱を似たようなものとすり替えた場合でも、あなたは自分の鍵で開けることができないことに気付くはずです。SSLやTLSも同じように機能しますが、ウェブサイトでのみです。

ブラウザーセキュリティインジケーターは、Extended Validation (EV)証明書の情報もやり取りします。EV証明書は、認証局でウェブサイトの実在性が確認されたウェブサイトに付与されます。ブラウザーでアドレスバーの横にサイト名や登録企業名がEVインジケーターとして表示されることがあります。EV証明書は、認証局でウェブサイトの実在性が確認されたウェブサイトに付与されます。ブラウザーでアドレスバーの横にウェブサイト名や登録企業名がEVインジケーターとして表示されることがあります。特定のウェブサイトのコンテンツを疑わしいと感じた場合、[証明書の表示]をクリックして証明書のURLがブラウザーのURLと一致しているかどうかを確認できます。(プロジェクタースクリーンで [証明書の表示] の見つけ方を見せるのもよいでしょう。 これを表示する方法はブラウザーによって異なります。例えばChromeの場合、[表示]の下で[開発者] >
[デベロッパーツール]の順にクリックします。 [デベロッパーツール]で[Security]タブ > [View Certificate]の順にクリックします。)

信頼できないソースからのソフトウェアを起動しない以外に、ウイルス対策ソフトウェアを使用して信頼できないページにアクセスしたり、マルウェアをダウンロードしたりしないようにすることができます。

「フィッシング」行為は、主に正当な関係者を装ったスパム送信者からのメールを通じて行われます。次にそのような相手からパスワードが尋ねられます。相手はあなたがパスワードをメールで送信するか、偽のウェブサイトに入力することを狙っています。スパムフィルターを利用すると、このようなメールの一部があなたの受信箱に表示されないよう設定できます。スパムフィルターを効果的に設定するために、受信箱に届いた不審なメールをスパムとしてマークしてください。

以下の質問を投げかけます。

自分のコンピューターに誤って有害なファイルをダウンロードすることを避けるた

めに、どのような対策を講じることができますか。

以下の内容を伝えます。

信頼できるウェブサイトのダウンロードファイルにアクセスしていることを常に再確認するようにしてください。心当たりのない添付ファイルを開いたり、ポップアップウィンドウやエラーメッセージをクリックしたりする際は、十分に注意してください。コンピューターに信頼できるマルウェア対策プログラムをインストールすることも検討してください。

パスワードを他人に教える

パート1

以下の質問を投げかけます。

パスワードを他人に教えてもよいのはどのような場合だと思いますか？

1. 考えられる回答として、共有アカウント(Netflixなど)などがあります。

パスワードを他人に教えることに関連するリスクは何ですか？

1. 悪意のある利用者があなたのパスワードを取得した場合、アカウントが不正アクセスされる可能性があります。パスワードを教えると、他人にアクセスされる可能性が高くなります。他のウェブサイトで同じパスワードを使用する場合も、そのサイトが他人にアクセスされる可能性があります。

以下の内容を伝えます。

ログインにパスワード入力を必要とするアプリケーション以外には、パスワードを教えないようにしてください。前述のように、フィッシングは人をだましてパスワードを聞き出す行為です。

ただし、あなたのアカウントにアクセスしたり、アカウントが危険な状態にあると主張したりするために、パスワードを明示的に尋ねる人もいます。このような人の中には、あなたを困惑させている原因をアカウントで調べる手助けをしたいと思っている友達のように善意を持っている人もいますが、パスワードを他人に教えることは賢明ではありません。そのパスワードを複数のアカウントで使用している場合はなおさらです。パスワードを他人に教える予定がある場合、そのパスワードが他の場所では使用されていないことを確認し、パスワードマネージャを使用してアクセスを共有するようにしてください。

親、先生、雇用主のように、あなたが信頼できる大人からパスワードを尋ねられる場合もあります。このような信頼できる大人の場合でも、パスワードを尋ねる理由やパスワードの処理方法について話し合うことが、通常はすべての人(あなたと相手の大人の両者)にとってプラスに働きます。特に家族以外の大人の場合、その相手があなたのパスワードを取得する必要があると考える根拠となる法律や他のタイプの規則があるかどうかを直接相手に確認してみるとよいでしょう。

法執行機関の担当者など、あなたが個人的に知らない家族以外の大人からパスワードを求められた場合は、法律や規則について丁寧かつ明確に尋ねることが特に重要になります。警察官や他の政府職員からソーシャルメディアパスワードを尋ねられた場合は、落ち着いて礼儀正しく対応するようにします。パスワードを求める理由や、相手がこの情報をあなたから取得する権利があると考える根拠となる法律や規

則を尋ねましょう。

親や保護者、先生、雇用主、法執行機関の担当者、政府職員、その他の大人による要求の状況によって、パスワードの提供が必要になることがあります。パスワードの提供が必要となる状況には、パスワードの提供を必要とする法律や規則がある場合や、パスワードを教えるリスクよりパスワードを提供してサポートを得るほうがメリットがあると自分で判断した場合などがあります。

大人からパスワードを求められたものの、その要求を不快に思う場合は、親や保護者、その他の信頼できる大人をすぐに探してください。できれば要求に応じる必要がある前に探しましょう。

以下の質問を投げかけます。

パスワードをオンラインで教えるべきなのはどのような状況の場合ですか。

1. アクセスしようとしているウェブサイトで自分のパスワードを入力するよう求められた場合のみです。他の場所では決してパスワードを教えないでください。これには、通常は暗号化されていないまたは安全ではないメールでのやり取りも含まれます。

課題

配布資料

課題

参加者を2、3人のグループに分けます。参加者にスパムの資料を配布します。その後、スパムを特定できると思われる方法や、特定の個人やグループと特定の情報を共有すべきかどうかについて示すフローチャートを、参加者に作ってもらいます。

以下の内容を伝えます。

それぞれのシナリオを読んでそれぞれのメッセージがスパムであるかどうか、そのシナリオで個人やグループと情報を共有すべきかどうかについて話し合います。

クラスインタラクション

参加者に10分間の作業時間を与えます。その後、各グループに回答を発表してもらいます。

以下の質問を投げかけます。

パスワードをメールで他人に教える必要があるのはどのようなときですか？

以下の内容を伝えます。

ウェブサイトや企業では、絶対にパスワードをメールで尋ねないことが一般的です。正当なソースのように見える場合でも、このような方法でパスワードを送信しないようにしてください。メールが安全であることはほとんどありません。

パート2

課題

参加者にグループから戻って各自で次の演習を行ってもらいます。

フローチャートを作成する時間を15分取ります。

以下の内容を伝えます。

スパムを特定できると思われる方法や、特定の情報を他人と共有すべきかどうかについて示すフローチャートを、各自で作成して紙に書きます。特定のシナリオを使用してフローチャートを作成すると便利です。配布資料に表示されているいずれかのシナリオを使用したり(この場合はフローチャートの上部分にシナリオの番号を書いてください)、ゼロから独自のシナリオを考えたりすることもできます。独自のシナリオを考える場合は、フローチャートの上部分でそのシナリオについて短い文章

で説明してください。

フローチャートを作成する時間を15分取ります。