安全かつ責任を持ってオンラインで参加する

26 分

この学習パスでは、インターネットの使用中に直面する安全リスクについて説明します。あなたは、オンライン詐欺とそれらを回避する方法について学びます.また、オンラインで情報を共有するためのベスト プラクティスについても学習します。また、あなたはサイバーいじめに導入されます。

# オンラインの安全性とプライバシー

17 分 |8ユニット

このモジュールでは、インターネットを使用する際に影響を与える可能性のある安全上のリスクのいくつかと、安全を保ち、情報をオンラインに保つためのヒントについて説明します。

## フィッシングから身を守る

3 分

### フィッシングから身を守る

オンラインでできることはたくさんありますが、常に安全上のリスクに注意する必要があります。オンライン捕食者がオンラインで人々の情報にアクセスするために使用する多くの詐欺があります。

あなたはそれらを避けるために最善を尽くすことができるように、これらの詐欺に注意する必要があります。.**フィッシング**は、注意が必要な一般的なオンライン詐欺です。

**フィッシングの詳細と、このオンライン詐欺から身を守る方法については、次のビデオをご覧ください。**

### ビデオ: フィッシングから身を守る

インターネットは私たちに多くの可能性をもたらします。他の人と会話オンラインで買い物、および個人的なビジネスなど1箇所で行うことができます。しかし、これらのオンラインインタラクションは必ずしも安全ではありません。知っておく必要があり、頻繁に発生しているオンライン詐欺について説明します。魚を捕まえる一般的な方法は、釣り針に餌をつけ、食いついた魚を捕まえる方法です。魚が食べ物に食いつくと、捕まってしまいます。インターネットのフィッシング詐欺も同様に機能します。あなたの情報を盗みたい人は漁師のようなものです。彼らは、ソーシャルメディア サイトやオンライン ゲーム経由であなたに電子メールやインスタント メッセージを送信します。彼らはしばしば、他人になりすまし、あなたの個人情報や、ハイパーリンクをクリックし、重要な作業を完了するよう求めることがあります。情報を与えたり、ハイパーリンクをクリックすると、ハッキングされてしまいます。しかし、ご心配は不要です。これから説明する 4 つの習慣は、フィッシング詐欺からあなた自身を守るのに役立ちます。習慣 1、不審なメッセージに注意する。詐欺師は、彼らのメッセージを公式で見慣れたメッセージに見せようとします。不審なメッセージを受け取ったときはもう一度考え、メッセージまたは電子メールを介して個人情報を共有しないようにしてください。これには自宅の住所、銀行の口座に関する情報、パスワードなどが含まれます。送信者を信頼できない場合は、リンクをクリックしたり、ファイルをダウンロードしないでください。習慣その 2、ウェブページが安全であることを示すサインを探す。クレジット カード情報を提供したり、パスワードやその他の個人情報を提供する際には、信頼できるセキュリティで保護された Web サイトを確認します。ほとんどの安全な Web サイトには、ブラウザーのアドレスバーの先頭にプレフィックス httpsが付いています。さらに、正しい Web ページを開いていることを確認してください。詐欺師はしばしば、公式に見える Web ページに導いたり、社名に間違ったスペルを使用してあなたをだまそうとします。www.microsoft.net は、Microsoft の公式 Web サイトであるwww.microsoft.com とは異なります。常に URL を確認して、正しい Web ページを開いていることを確認してください。習慣その 3、Web ブラウザとオペレーティングシステムを最新の状態に保つ。自動更新を有効にして、コンピューターに常に最新のソフトウェアリリースがインストールされるようにできます。デバイスソフトウェアを最新の状態に保つことで、コンピューターの保護に役立つ、最新のセキュリティ更新プログラムを受け取ることができます。習慣その4、デバイスには認証済みのマルウェア対策ソフトウェアをインストールする。これは、コンピューターを有害なソフトウェアやハッカーから保護するために作られた特別なソフトウェアです。次の餌に引っかからないようにしてください。インターネットを利用する際には、クリックやダウンロード、共有する前に、オンラインでのフィッシング詐欺から身を守るのを忘れないでください。

## オンラインで安全にコミュニケーションをとる

2 分

### オンラインで安全にコミュニケーションをとる

インターネットは、私たちが新しい方法で他の人と通信することを可能にします。ただし、オンラインで他のユーザーと通信することは必ずしも安全ではありません。インターネット上で誰と話しているのかが必ずしも分からないので、安全を保つように気をつけなければなりません。

**オンラインで安全に通信する方法については、次のビデオをご覧ください。**

### ビデオ: オンラインで安全に通信する

インターネットを使用することで、私たちは世界中の人々と新しい方法でコミュニケーションを取ることができます。これには多くの利点がありますが、いくつかの危険もあります。オンラインの捕食者は毎日、インターネットを使用しています。これらの捕食者は、多くの場合、別の人物を装います。そのため、オンラインで話している相手が誰かを知るのは難しいかもしれません。ここでは、オンラインでコミュニケーションを取る際に、オンラインの捕食者から身を守るためにできる3 つのヒントについて説明します。ヒントその 1、直観に従う。誰かがあなたを不安にさせたり、不快に感じさせた場合、彼らとのコミュニケーションを止め、信頼できる人物にすぐ伝えてください。多くの Web サイトやソーシャルメディアサイトには、疑わしいアクティビティを報告するためのツールが用意されています。ヒントその 2、共有する情報を制限する。オンライン捕食者は、多くの場合、電子メールやメッセージを通じてあなたの個人情報を共有させようとします。オンラインで見知らぬ人に個人情報を共有しないでください。ヒントその3、距離を保つ。オンラインでしか会話したことのない人物と合う際には、改めて考え直してください。オンライン捕食者は、多くの場合、ソーシャルメディアを使用し、他人の写真を使用してプロファイルを設定することで、他人になりすまします。優しそうに見える相手でも、あなたがオンラインで話をしている相手が誰かを知ることは困難です。オンラインで知らない人が会いたいと言ってきた場合は、親か誰か信頼できる人に伝え、危険な状況を避けてください。多くのオンライン捕食者は、スマートな戦略を使用して、あなたを危険な状況に誘い込もうとします。しかし、あなたは彼らよりも賢くなることができます。これらのリスクとヒントを念頭に置くことで、オンラインで人と話をする際に、身を守ることができます。

## 強力なパスワードを作成する

2 分

### 強力なパスワードを作成する

安全を保ち、情報をオンラインで非公開にしておく大きな部分は、強力なパスワードを使用して情報、アカウント、コンピュータを保護することです。

**情報を保護できる強力で効果的なパスワードを作成する方法については、次のビデオをご覧ください。**

### ビデオ: 強力なパスワードを作成する

パスワードは、個人情報とアカウントを、他のユーザーから守るのに役立ちます。パスワードは、玄関の鍵のように重要なものです。あなたはこじ開けにくく、危険な人々が入ってくるのを防げるような強力な鍵を求めます。また、他人が鍵を見つけられないようにしたいと思います。強力なパスワードは、アカウントの強力な鍵のようなものです。他人が推測しにくく、安全で、他人が見つけにくい鍵にしたいと思うでしょう。これから示すヒントに従って強力なパスワードを作成し、それらを安全に保ちます。1 つ目のヒントは、パスワードに、文字と数字、記号の組み合わせを使用します。大文字と小文字、記号の組み合わせを使用し、数字を追加すると、パスワードの強度を上げることができます。ヒントその 2、パスワードに一般的な単語を使用しないでください。これには、「password」や「website」などの一般的な単語や語句、誕生日、名前、出身地などの個人的なキーワードが含まれます。ハッカーはパスワードでこれらの語句を容易に推測することができます。文字と数字の一意の組み合わせを使用することで、より強力なパスワードを作成できます。ヒントその 3、別のアカウントには別のパスワードを使用してください。誰かがあなたの電子メールパスワードを推測した場合、同じパスワードを銀行口座に使用していたら、あなたの安全とプライバシーが脅かされる可能性があります。代わりに、オンラインアカウントごとに異なるパスワードを使用してください。ヒントその 4、パスワードはあなただけのものです。たとえ友人や家族であっても、他の人と共有した場合、誰か別の人がそれを使用したり、安全を保証できない可能性が高くなります。パスワードは他の人に教えないでください。アカウントにログインする際には、完了したら必ずログアウトし、公共のコンピューターにログイン情報を保存しないでください。また、公共のコンピューターや 公共ネットワークで 個人的な作業を 行うと、ハッカーが あなたの情報にアクセスしやすくなってしまうので 行なわないようにしてください。強力なパスワードを使用し、それらを安全に保管することは、お客様のオンラインでの安全とプライバシーにとって重要です。新しいパスワードを作成する際は、これらのヒントに注意してください。

## オンラインで情報を共有するためのベスト プラクティスの説明

2 分

### 共有するときにスマートになる

オンラインに入ると、多くのことを考えずに安全を脅かす多くのことを行うことができます。オンラインで共有する内容をもう一度考え、安全を念頭に置いておく必要があります。

**オンラインでの過剰共有のリスクの詳細については、次のビデオをご覧ください。**

### ビデオ: オンラインでのオーバーシェアリング

インターネットとウェブを使用すると、世界中にいる友人や家族とつながることができます。私たちは、ソーシャルメディアや他のプラットフォームを使用して、友人の生活に何が起こっているかを見たり、個人的なニュースを共有し、他の人と連絡を取り合うことができますが、オンラインで物事を共有する際には、常に安全とは言えません。次のシナリオを考えてみましょう。ハロルドは新しい車を取得し、友人に見せたいと思います。そこで、彼はソーシャルメディアにその写真を投稿します。これは問題ないように思われますが、写真には、ハロルドについての多くの個人情報が含まれています。誰もが1枚の写真から彼のナンバープレート番号を見ることができ、どのような車を運転しているか、さらに どこに住んでいるかが わかります。友人が見るのであれば問題ないかもしれませんが、しかし、間違った人が見つけ、悪いことに使用した場合は非常に危険です。オンラインで何かを共有したいときには、安全性とプライバシーを念頭に置くことが重要です。ソーシャルメディアのウェブサイトでプロフィールを設定する際には、アカウントのプライバシー設定を必ず確認してください。アカウントが [公開] に設定されている場合は、誰でもあなたの情報や、共有した内容を見ることができます。代わりに、アカウントのプライベート設定を使用して、あなたの個人的なつながりがある人物だけが共有内容を表示できるようにしてください。また、ソーシャルメディアで招待を受け、誰かとつながる際には、慎重になる必要があります。ほとんどのソーシャルメディアプラットフォームは、リクエストを承認または拒否し、誰かがあなたの友人となったり、サイトのフォロワーとなる手段を提供しています。あなたが誰かを受け入れたら、その人物はあなたのプロフィールや共有している情報に直接アクセスできるようになります。リクエストを受けた際には、この点に留意し、知っている人物や信頼できる相手とのみやり取りするようにしてください。あなたのプロファイルやアカウントにアクセスできるユーザーは制御できても、他の人があなたの情報をどう使うかを制御することはできません。オンラインで共有した内容を消去することはできません。見知らぬ人に見られたり、公開されたくないことをオンラインで共有しないでください。共有する前にもう一度考えることを忘れないでください。何かをオンラインで共有する際には、安全を念頭に置き、賢い選択を行ってください。

### 自分で試してみる

このビデオから何を学びましたか?個人情報をオンラインで共有する際に留意すべき 1 ~ 3 の事柄を書き留めます。

## デジタルフットプリントの管理の重要性を説明する

3 分

### デジタルフットプリント

ウェブの閲覧からソーシャルメディアでの更新の共有、オンライン購入まで、オンラインでできることはたくさんあります。オンラインで行うすべての操作は、オンライン履歴または**デジタルフットプリント**の一部になることを念頭に置く必要があります。

オンラインで発生する事柄を消去するのが難しいため、情報を共有したりオンラインで行ったりする場合は、デジタルフットプリントについて考える必要があります。

**デジタルフットプリントとその管理方法の詳細については、次のビデオをご覧ください。**

### ビデオ: デジタルフットプリントを管理する

インターネットを使用する場合は、デジタルフットプリントに注意する必要があります。汚れた道に誰かが歩い跡が残る物理的な足跡と同様に、あなたのデジタルフットプリントは、オンラインにおけるあなたのすべての行動の履歴です。あなたが行うソーシャルメディアの投稿、あなたが訪問するすべてのウェブサイト、およびオンラインで共有する情報は、あなたのデジタルフットプリントを構成します。オンラインで何かを投稿したら、削除することはできません。そのため、あなたのデジタルフットプリントは永遠に残る可能性があります。デジタルフットプリントに、オンラインでの肯定的な評判を与えてくれる者が含まれる場合、これはよいことかもしれません。個人ブランドを構築する際に役立つ可能性があります。オンライン履歴は、アプリがあなたについて詳しく知るのにも役立ちます。彼らは、この情報を使用して、あなたの気に入ることや毎日の習慣に合わせ、表示する情報を調整することができます。しかし、この情報が間違った方法で使用されたり、他人と共有される可能性もあります。オンラインに接続する際には、次の点に注意してデジタルフットプリントを管理するようにしてください。ヒントその 1、あなたのフットプリントがあなたについて何を語っているかを把握する。他の人はあなたのデジタルフットプリントを使用して、オンラインでのあなたについての判断を下します。あなたが仕事に応募した際に雇用主が使用したり、アカデミックプログラムに応募した際にリクルーターが使用したりるす場合などです。自分のデジタルフットプリントが、自分について何を語り、自分の個人情報がどのように使用されているかを知ることが重要です。あなたの個人的なブランドをオンラインで確認するには、自分で検索してみることができます。Bing 検索エンジンで自分の名前を検索し、表示される結果を確認します。これらの結果が望まないものである場合は、オンラインで何を共有するか、他の人に表示を許可する情報について考えてください。ヒントその2、プライバシー設定を管理する。自分で使用するほとんどのソーシャルメディアサイトやオンラインアプリケーションでは、プライバシー設定を変更できます。これにより、あなたの情報を見ることができる相手や、誰かがあなたをオンラインで検索したときに、表示される情報を制御するのに役立ちます。ヒントその 3、cookie を管理する。Cookie は、あなたが Web を閲覧する際、Web ブラウザーに提供されるメモです。これらのクッキーは、あなたがアプリを使用している間、アプリが必要な情報を追跡するのに役立ちます。これにより、アプリがユーザーに合わせてうまく動作するのに役立ちますが、このデータは、デジタルフットプリントにも貢献します。ブラウザー設定を使用して、特定の Web サイトでのcookie の使用を制限またはブロックできます。ヒントその4、共有する前に考える。オンラインで何かを一度共有したら、それを元に戻すことはできません。共有する前に、何を公開デジタルフットプリントの一部にしても問題ないかを確認してください。デジタルフットプリントは永遠に残る可能性があります。これらのヒントを念頭に置いて、自分のデジタルフットプリントと、その使用方法に満足できるようにしてください。

ナレッジチェック

3 分

1. セキュリティで保護されたサイトを使用していることを確認するには、Web ページの URL で次のどのコンポーネントを探す必要がありますか。

* http
* 安全
* **https - 正しい!"https" は、Web ページがセキュリティで保護されていることを意味します。**
* Ssh

1. これらのパスワードの中で最も強いパスワードはどれですか?

* **John@453 - 正解!このパスワードには、大文字、小文字、特殊文字、および数字が含まれています。**
* ジョン500
* JoHn300
* 125893

1. デジタルフットプリントは次のとおりです。

* オンライン アカウントの情報のサイズ。
* オンラインで接続している人の数。
* **あなたが行い、オンラインで言うすべての記録。- 正しい!デジタルフットプリントを使用すると、オンラインでのアクションを簡単に追跡できます。**
* オンラインユーザー名。
* r 強力なパスワードを使用しています。

## 概要

1 分

おめでとう！

オンラインの安全とプライバシーのモジュールを完了し、次の質問に自分で答えることができます。

1. インターネットやウェブを使用する上でどのような危険性がありますか?
2. オンラインの安全リスクや詐欺の兆候は何ですか?
3. インターネットを使用している間、安全を保つためにどのような手順を実行できますか?
4. デジタルフットプリントを管理するにはどうすればよいですか?

**次のビデオでは、強力で効果的なパスワードを作成する方法を学習します。**

# オンライン礼儀正しさ

9 分 |5 ユニット

このモジュールでは、オンラインで情報を使用するための権利とベスト プラクティスについて詳しく説明します。また、サイバーいじめについても学びます。

導入

1 分

私たちは、インターネットを使用して多くの情報にアクセスし、他の人と通信することができますが、私たちは責任あるデジタル市民として行動していることを確認する必要があります。

このレッスンでは、インターネットと Web を責任を持って使用する方法について説明します。

**このレッスンを終了すると、次の情報が得られる場合があります。**

1. Web 上で共有される情報やコンテンツに対するユーザーの権利について説明する。
2. Web 上の情報を使用するためのベスト プラクティスについて説明する。
3. ウェブ上で他の人を粗く扱うことの意味を説明する。
4. **お客様の情報を保護します。**

## Web 上の情報を使用するためのベスト プラクティスの説明

2 分

### 責任を持って情報を使用する

デジタルの世界では情報へのアクセスは簡単ですが、オンラインで見つけた情報を使用する場合は、いくつかのルールに留意する必要があります。

**次のビデオを視聴して、オンラインで見つけた情報の使用に関するガイドラインの一部を確認してください。**

### ビデオ: 責任を持って情報を使用する

インターネットは私たちに無制限の情報と可能性を与えてくれます。私たちは面白いビデオからお気に入りの曲、または宿題の問題を解決する方法についての情報など、あらゆるものを見つけることができますが、オンラインで見つけた情報には責任を持つ必要があります。次のシナリオを考えてみましょう。ハロルドは料理本を執筆し、オンラインで販売したいと考えています。彼は写真を撮るのが上手ではありません。そこで、彼はオンラインで画像を検索します。彼はさまざまな食べ物の画像をダウンロードして、自分の本にそれらの画像を含めます。これは簡単にできることなので、問題がないように思われるかもしれませんが、オンラインで見つけた情報を使用するのに公正または責任ある方法とは言えません。誰かが自分の作品を、言葉や画像、動画、音楽などと共にオンラインに公開した場合、その人物がコンテンツの所有者になります。所有者として、その人物は特定の権利、通常は著作権や、それらのコンテンツの使用方法に関する権利を持ちます。誰か別の人物の言葉や作品を自分のものとして使用すると、盗作と見なされます。これは原作者にとって公平ではなく、トラブルが発生する可能性があります。他の人物のコンテンツを自分の作品で使用したい場合は、必ず、その人物に作品のクレジットを提供するようにしてください。あなたが販売している製品で誰かの作品を使用している場合は、最初にその作成者から許可をもらう必要があります。また、誰かの作品を使用するためのライセンス料の支払いが必要となることもあります。場合によっては、コンテンツの作者が作品の無料使用を許可していることもあります。Bing などの検索エンジンを使用して、他のユーザーが使用できる画像やメディア、およびその他のタイプのコンテンツを検索できます。インターネットを使用して、オンラインで情報を見つける際には、公平かつ責任を持って使用するようにしてください。

## ウェブ上で他人を粗く扱うことの意味を説明する

3 分

### いじめ

インターネットは、私たちは世界中からオンラインで他の人と接続することができます。残念ながら、人々は常にオンラインでお互いをうまく扱う必要はありません。

**サイバーいじめ**は、インターネット上で行われるいじめの一種です。意地悪なメッセージを送ったり、他の人に対する否定的な噂を広めたりするのは簡単ですが、標的にされた人にとっては危険です。

**次のビデオを見て、サイバーいじめを防ぎ、デジタル市民になるためのヒントを学びます。**

### ビデオ: 他の人をオンラインで丁重に扱う

* インターネットや私たちを友人、家族や同僚を新しい方法で結び付けます。時には、人々は活用し、他人についての否定的なメッセージを広めるためにサイバーいじめ、またはインターネット上でのいじめは、実際のいじめと同じくらい人々はインターネットを使用して誰かに意地悪なメッセージを送り、偽の噂を広め、または誰かの個人情報を誰かがサイバーいじめを受けると、彼らの感情は傷つき、彼らの評判常にサイバーいじめをインターネットを誰にでも安全な場所にするためのここでは、デジタルにおけるガイドラインをいくつか示します。つまり、あなたが扱われたいように対面であっても否定的なメッセージを他の人を傷つける可能性のある行動に違いを尊重する。私たちは皆、多くの点で異なっています。オンラインで他の人と互いの違いや意見、経験、文化を尊重しましょう。他の人がオンラインで同意できない場合であっても、敬意を持ってインターネットを親しみやすく返信する前に一度立ち止まる。オンラインで何かを共有する前に、常に一時停止し、結果についてあなたのメッセージは他の誰かをそれはあなたの評判をや、誰かの安全や評判をオンラインで共有する前に自分自身と他の人のために立ち上がりましょう。オンラインで安全でないと感じた場合は、その状況から逃れて信頼できる人物にオンラインで残酷な活動や関係者に支援を提供し、信頼できる人物にインシデント私たちは皆、インターネットを過ごしやすい場所にする役割をあなたの役割を果たし、オンラインでの責任あるデジタル

## ナレッジチェック

2 分

1. これらの行為のどれが著作権を侵害していないのですか?

* 許可なく出版した本の中で誰かの画像を使用する。
* **誰かの本から段落を引用し、それらを参照する - 正しい!所有者を引用する際に著作権を遵守します。**
* 自分の名前で他の人の動画を販売する.
* 誰かの本を無免許で売る。

1. サイバーいじめは、次の場合に行うことができます。

* ソーシャルメディアプラットフォームでのみ。
* 電子メールを通じてのみ。
* SMS でのみ使用します。
* **ソーシャルメディアプラットフォームやSMS、および電子メールを介して。- 正しい!サイバーいじめは、あらゆる種類のオンライン通信で行うことができます。**

## 概要

1 分

おめでとう！

オンライン礼儀正しさモジュールを完了し、次の質問に自分で回答できるようになりました。

1. オンラインで見つけた情報を使用する場合は、どのような操作を行う必要がありますか。
2. あなたは、サイバーいじめを防止または終了するために何ができますか?

# 証明書を印刷する

2 分 |2単位

証明書を受け取るには、このコースのすべてのモジュールを完了する必要があります。

## 貸方の受信

1 分

### 完了

安全かつ責任を持ってオンラインで参加を完了しておめでとうございます。[**クレジットの受取]** を選択してコースを完了し、証明書を受け取ります。

### 受領済貸方

安全かつ責任を持ってオンラインで参加を完了しておめでとうございます。

下のボックスに、証明書に表示する名前を入力し、[**証明書の表示**]を選択してください。