

パスワード

強固なパスワードを使用、維持して自分のオンライン情報の安全を確保する方法について学びます。また、強固なパスワード設計の原則やパスワードの共有によって発生しうる問題についても学びます。さらに、自分のパスワードの安全を確保し、アカウントへの不正アクセスを防ぐ方法についても学習します。

素材

パスワードに関する学習の配布資料

パスワードの基本

パート1

以下の内容を伝えます。

私たちは普段、ウェブサイト、アプリ、サービスで使用するパスワードについて深く考えることはありません。しかし、パスワードの強さは情報の安全性を決める重要な要素です。

クラスインタラクション

参加者に、次の質問について議論してもらいます。自分が実際に使っているパスワードを演習の中で他の人に教えないよう再度注意してください。

以下の質問を投げかけます。

パスワードをいくつ持っていますか？

メールやソーシャルメディアのアカウントごとに別のパスワードを使用していますか？

それぞれまったく違うパスワードですか？それとも1つのパスワードのバリエーションですか？

複数のパスワードを持っている場合、どのアカウントにどのパスワードを使用しているかをどのように記憶していますか？

以下の質問を投げかけます。

どのくらいの頻度で大切なパスワードを忘れますか？

パスワードを忘れたときに何をしましたか？

パスワードを覚えやすくするためにどのような方法をとっていますか？

毎日使用するパスワードはありますか？

知らないうちに、他人にパスワードを知られたらどうなりますか？

その人が誰かによって状況は変わりますか？

誰かがパスワードを使用してあなたのアカウントにログインした場合、その人はあ

なたについてどのような情報を得ることができますか？

パート2

クラスインタラクション

参加者を2人ずつのペアにします。

以下の内容を伝えます。

いつも使用しているソーシャルメディアプラットフォームのパスワードを悪意のある人に知られたらどうなるか、パートナーと話し合ってください。

クラスインタラクション

参加者に話し合う時間を5分間与えます。その後、各グループに内容を発表してもらいます。

以下の内容を伝えます。

次に、親や保護者のオンライン銀行口座のパスワードをハッカーに盗まれたらどうなるか、パートナーと話し合ってください。

クラスインタラクション

参加者に話し合う時間を5分間与えます。その後、各グループに話し合った内容を発表してもらいます。

パート3

以下の内容を伝えます。

ハッカーが非公開のパスワードをどうやって知るのが疑問に思うかもしれません。方法はいくつかありますが、その1つはソーシャルエンジニアリングです。これは人をだましてパスワードを聞き出す手口です。ハッカーは、その人がアカウントを持っているプラットフォームやウェブサイトから公式に送られてきたように見えるメールを送信します。メールの文面に従って記載されたリンクをクリックし、ユーザー名とパスワードを入力してログインするように促します。ログインすると、ログイン情報はハッカーの手に渡ってしまいます。

ハッカーは、「password123」や「test」などの一般的なフレーズや、あなたの名字や名前などを使ってパスワードを推測することもあります。

ハッカーが非公開のパスワードを盗むために使用するもう1つの方法は「総当たり」攻撃です。総当たり攻撃とは、ハッカーがさまざまなパスワードを繰り返し試してアカウントにログインしようとすることです。「総当たり」攻撃は手動で行うこと

もできますが、多くの場合、あらゆるパスワードの組み合わせを高速かつ自動的に試すコンピュータープログラムによって実行します。例えば、よくあるパスワードのリストや異なる文字や数字の組み合わせからなるパスワードのセットを、正しいパスワードを見つけるまで試します。

もちろんもっと複雑な「総当たり」攻撃もあります。パスワードが「fido123」や「password」など、よくあるパスワードのリストに載っている場合、プログラムによっては、これらのパスワードをあまりないパスワードやランダムなパスワードよりも先に試すため、より速く推測できます。ハッカーがあなたに関する情報を知っている場合、攻撃の精度は高まります。例えば、ペットの名前がトビーだと知っていれば、ハッカーは「トビー」の後ろにさまざまな数字の組み合わせを付けたパスワードを試すことができます(「Toby629」や「Toby3020」など)。

パスワード設計の原則

パート1

以下の質問を投げかけます。

「強固な」または「非常に強固な」パスワードを設定するとはどういうことでしょうか？なぜそうしたほうがよいのでしょうか？

以下の内容を伝えます。

強いパスワードは、個人情報の保護に役立ちます。強固なパスワードを設定しても、アカウントは絶対に不正アクセスされない保証はありませんが、パスワードが弱い場合、他人があなたの情報にアクセスしやすくなります。

パスワードに関する演習

以下の質問を投げかけます。

脆弱なパスワードの例にはどのようなものがありますか？

1. 例えば次のようなものです。Password、12345、Hello!、生年月日、ニックネーム。

これらのパスワードが脆弱な理由は何だと思えますか？

1. 他人や「総当たり」攻撃を実行するコンピューターが簡単に推測できるからです。

パスワードをより強固にするにはどのような方法がありますか？

1. 数字、大文字と小文字、記号を追加する、パスワードを長くする、一般的なフレーズや単語を単体で使わない、など。

クラスインタラクション

参加者が回答した後、黒板やホワイトボードに次の指示を書いてください。

少なくとも1つの数字を含める。

少なくとも1つの記号を含める。

少なくとも1つの大文字と1つの小文字を含める。

パスワードは最低7文字にする。

覚えやすいパスワードにする(パスワードマネージャを利用しない場合)。

パスワードマネージャとは、パスワードを保存、管理するためのウェブサイトやアプリのことです。

一般的な単語のみや個人情報(生年月日、親の名前など)をパスワードにしない。

パスワードを複数のウェブサイトで共有しない。

以下の内容を伝えます。

強固なパスワードを作成するには、2つの方法があります。1つ目は、先ほど黒板やホワイトボードに書いたような「パスワードのレシピ」に従う方法です。このようなレシピに従うことで、文字や数字のパスワードに推測しにくい要素を含めることになり、パスワード自体が推測しにくいものになります。この方法のデメリットは、パスワードが覚えにくくなることです。

強固なパスワード

以下の内容を伝えます。

強固なパスワードを作成するもう1つの方法は、パスワードの長さに関連しています。パスワードの強さはその長さに比例するため、関連のない単語を4つ以上並べることで、他人や「総当たり」攻撃によって推測される可能性が、はるかに低くなります。また、その方法で作成したパスワードはレシピに従う方法によるパスワードよりも覚えやすいというメリットもあります。

さらに、この2つの方法を組み合わせて、関連のない単語を4つ以上並べたうえに記号や数字を含めるという方法もあります。

これらの方法の目的は、いずれも他人が推測しにくい固有のパスワードを作成することです。

以下の内容を伝えます。

参加者を2人ずつのペアにします。

ペアごとに、先ほど黒板やホワイトボードに書いた指示に従って強固なパスワードを作成してみます。コンピューターがランダムに推測しにくいパスワードでも、人間や一般的な長いパスワードのリストを持っているコンピューターにとっては簡単に推測できる場合もあります。パスワードを書いた紙は、アクティビティの最後に回収しません。グループのメンバーはそのパスワードを知っているため、自分のアカウントで実際に使用しないようにしてください。

参加者に5分間の作業時間を与えます。5分経過したら部屋を回り、最も強固なパスワードだと思うものはどれか聞きます。また、書いた紙を見ずに、作成したパスワードを思い出せるかどうか尋ねます。

これらの条件のいくつか(またはすべて)を満たしているパスワードを要求するウェブサイトもありますが、このような制限を設けていないウェブサイトもあります。一般的な単語をランダムに並べたパスワードを作成することもできます。

クラスインタラクション

同じペアで、単語を並べて新しいパスワードを作ってもらいます。パスワードに4つ以上の単語を使うと強固で覚えやすくなると伝えます。参加者に5分間の作業時間を与えます。5分経過したら部屋を回り、どのようなパスワードを作ったか聞きます。ここでも、アクティビティ終了後に用紙を回収しないこと、また、作成したパスワードを自分のアカウントで使用しないことを伝えます。

以下の内容を伝えます。

ウェブサイトによっては、多要素認証(または二段階認証)を使用して利用者を認証します。このようなウェブサイトでは、SMS、アプリ、メールから送信されるワンタイムコードをパスワードと共に入力する必要があります。

この方法では、セキュリティを強化して認証の精度を高めることで、アカウントをより確実に保護できます。例えば、アカウントにログインするには、パスワードだけでなくアカウントに登録されたアプリやデバイス、メールアドレスにアクセスする必要があります。

パスワードの安全を確保する

パート1

以下の内容を伝えます。

コンピューターや人間にとって解読が難しいパスワードを作成しても、パスワードが脆弱になってしまう場合があります。

以下の質問を投げかけます。

パスワードが脆弱になるのはどのような場合でしょうか？

1. 例えば、複数のアカウントでパスワードを使い回す、個人情報を含んだパスワードを使用する、同じパスワードを何年も使い続ける、パスワードを忘れた場合などです。

パスワードはどれくらいの頻度で変更する必要があると思いますか？

以下の内容を伝えます。

良いパスワードでも他人に知られたり盗まれたりする可能性があります。そのようなときも自分を守る方法があります。アカウントを持っているウェブサイトでデータの漏えいがあった場合、そのウェブサイト及び似たパスワードを使用している他のウェブサイトのパスワードを必ず変更するようにします。

長く複雑なパスワードをいくつも覚えておくのは難しいことです。

以下の質問を投げかけます。

パスワードを紙やコンピューターのドキュメントファイルに書いておくのは良い考えだと思いますか？それはなぜですか？

クラスインタラクション

パスワードを書いた紙やコンピューターのファイルを誰かが見つけたりする可能性について言及します。パスワードを保存、管理するアプリであるパスワードマネージャを利用するのも1つの手段であることを説明します。

パート2

以下の内容を伝えます。

私たちは毎日、さまざまなウェブサイトでたくさんのアカウントを使用しています。すべてのウェブサイトで毎回ログイン、ログアウトするのは面倒になりがちです。

。

以下の質問を投げかけます。

ブラウザの「パスワードの保存」機能を使用して、ウェブサイトのパスワードを保存したことはありますか？それはなぜですか？

ウェブサイトがどのように利用者を覚えているか理解していますか？

1. 参加者に説明を求めます。その後、ウェブサイトはCookieを保存することで利用者がログインしたことを記憶していると説明します。Cookieはコンピューターに保存される小さなファイルで、これによりウェブサイトは利用者やコンピューターを認識できるため、次に訪問した際に再度ログインする必要がなくなります。ただし、Cookieは利用者のウェブサイト間の移動を追跡するためにも使用され、これにより広告配信のターゲットに含められることもあります。

自分のコンピューターであればパスワードを保存してもよいと思いますか？

以下の質問を投げかけます。

コンピューターにログインパスワードを設定していますか？

コンピューターを他人と共有する場合はどうですか？

1. その場合、パスワードフィールドで黒い点やアスタリスクで隠されていても、そのコンピューターを使用する他人にパスワードがわかってしまう可能性があります。画面上で見ることができなくとも、どこかに保存されていないとは限りません。

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と思う場合はありますか？それはどのような場合ですか？なぜそう思いますか？

1. 例えば、親が子どものパスワードを知りたい場合や、Netflixのようなサービスで共同アカウントや家族アカウントを持っている場合が考えられます。

あなたは自分のパスワードを他人に教えていますか？教えている場合は誰にですか？それはなぜですか？

仲良しの友達に「僕/私のことを大切に思ってるなら教えて」と言われたら、パスワードを教えますか？それはなぜですか？

以下の内容を伝えます。

大切な人にはパスワードを教えてもよいと思うかもしれませんが、大切な人だからといって必ずしも自分のオンラインアカウントに自由にアクセスできるようにする必要はありません。

パスワードを教える前に、その人との関係について、今後その関係が変わる可能性も含めてよく考えてください。例えば、両親や保護者にパスワードを教えることと、親友に教えることはまったく違います。

以下の質問を投げかけます。

他人にパスワードを教えたら、自分にどのようなことが起こる可能性がありますか？

1. 誰かがあなたの銀行口座に不正アクセスする、オンラインであなたになりすます、秘密を知ってしまう、などが考えられます。

あるアカウントのパスワードを他人に教えた場合、そのアカウントの使い方を変えますか？

以下の質問を投げかけます。

誰かに見られる可能性がある場合、Netflixで見ないようにするコンテンツやメールに書かないようにする内容がありますか？

クラスインタラクション

参加者に、共有アカウントを使用する際の自分の行動を振り返ってもらいます。アカウントを共有している人に自分のオンライン行動を見られていることを意識する必要があることを伝えます。

以下の質問を投げかけます。

自分のアカウントが、ソーシャルメディアプロフィールのように自分をバーチャルに表すものだとすれば、他人にアカウントを使用させてもよいと思いますか？

クラスインタラクション

誰かが自分になりすまして、自分の友達にメッセージを送る可能性について話し合ってください。

以下の質問を投げかけます。

使用しているデバイスがパスワードを保存することを許可していますか？それはなぜですか？個人用の携帯電話やコンピューターにパスワードを保存するのは安全だと考えますか？友達に電話やコンピューターを貸した場合はどうなりますか？

家族や友達と共有しているデバイスがありますか？そのデバイスでアカウントを共有していますか？それとも各自が別々のアカウントを持っていますか？

図書館や学校などにある「公共」デバイスを使用することはありますか？そのデバイスで他のデバイスと同じような使い方をしますか？

パート3

クラスインタラクション

参加者を2人ずつのペアにします。

以下の内容を伝えます。

ペアごとに、学校や図書館などの公共の場でコンピューターにログインした際に、前に使用した人がソーシャルメディアやメールのアカウントにログインしたままになっていたことがあるか話し合います。そのような場合に、そのアカウントを覗いたり、アカウントで何かしたりするか考えてもらいます。

クラスインタラクション

5分間話し合った後に、内容を発表してもらいます。そのような不正使用についてグループ全体で話し合います。

アカウントへの不正アクセス

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: パスワードの基本」と重複しています。
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。

以下の内容を伝えます。

パスワードをすでに知っている場合やランダムな推測に成功した場合以外にも、他人があなたのアカウントにアクセスすることは可能です。例えば、あなたの個人情報がある程度知っていれば、それに基づいてパスワードを推測したり、ある会社の人を説得してあなたの情報を引き出したりすることができます。このように技術的な手段を使わずアカウントに侵入する攻撃は、ソーシャルハッキングまたはソーシャルエンジニアリングと呼ばれます。

以下の質問を投げかけます。

ウェブサイトのパスワードを忘れたことがある人は手を挙げてください。

「パスワードを忘れた場合」をクリックするとどうなりますか？

1. 通常、セキュリティのための質問の答えを求められるか、自分の電話番号やメールアドレスに連絡が来ます。

ウェブサイトに聞かれるセキュリティのための質問にはどのようなものがありますか？

1. 友達や知り合いが答えを知っている、または推測できる質問にはどのようなものがありますか？例: ペットの名前、生まれた場所、母親の旧姓、好きな先生の名前、親友の名前、好きなスポーツチームなど。

このような情報を知っている可能性のある人は他に誰がいますか？

パスワードを忘れた場合、ウェブサイトからどのような方法で連絡が来ますか？

あなたの連絡先を入手できる可能性のある人は他に誰がいますか？

以下の質問を投げかけます。

知らない人が、セキュリティのための質問の答えに関連するあなたの個人情報を手

に入れるにはどのような方法がありますか？

1. ソーシャルメディア投稿を閲覧する、公開情報をオンライン検索する、何度も推測する、あなたの友達に連絡する、など。

個人情報が含まれたソーシャルメディア投稿の例をいくつか挙げてください。

1. キャプションにその名前が書かれたペットの猫のInstagram写真、位置情報がタグ付けされた写真、公開の誕生日投稿など。

Googleを使用して他人の情報を検索し、パスワードに不正アクセスする方法にはどのようなものがありますか？

1. 検索エンジンで、ある人が中学校3年生のときのクラス写真が学校新聞に掲載されているのをオンラインで見つけた場合、当時の担任の先生の名前がわかります。

パート2

以下の内容を伝えます。

セキュリティのための質問の答えを含んだ情報を投稿するのは非常に危険です。セキュリティのための質問は、自分だけが答えを知っているものを選ぶようにします。セキュリティのための質問に嘘の答えを設定することもできますが、その場合は答えをパスワードマネージャに保存するか、覚えやすいものにします。

アカウントに登録されている電話番号やメールアドレスにウェブサイトから連絡が来ることがあります。パスワードを忘れた場合、多くのウェブサイトは一時的なパスワードを発行するか、パスワードを再設定するためのハイパーリンクを利用者に送信します。

以下の質問を投げかけます。

これは、新しいパスワードをリクエストしている人が利用者本人であることを安全に確認できる方法ですか？

アカウントに登録しているメールアドレスを共有している場合はどうですか？

1. パスワード再設定リンクを送信する方法は基本的には安全ですが、アカウントやパスワードを他人と共有している場合はリスクが生じます。

以下の内容を伝えます。

ソーシャルハッキングは、直接人に連絡し、その人をだまして情報を盗み出そうとすることです。誰か(友達、家族、銀行員など)のふりをしてメールを送り、本人確認のためと言って生年月日などの大切な情報を聞き出そうとする場合もあります。あなたの友達のソーシャルメディアアカウントに不正アクセスし、あなた(やあなた以外のたくさんの人)に誕生日や育った場所を尋ねるメッセージを送ってくるといった、より巧妙な手口もあります。友達から送られてきたメッセージが変だと思ったら、まずその友達に(ソーシャルメディアプラットフォーム以外で)連絡して、送り主が本当にその友達かを確認します。

本物に見えるメールやウェブサイトを使用した攻撃はフィッシングと呼ばれ、個人情報の盗難やなりすまし犯罪につながる可能性があります。例えば、誰かが個人情報を盗んであなたになりすまし、あなたの名前でクレジットカードを作成、使用した場合、あなたが大人になったときにクレジットカードを作りにくくなる可能性があります。

また、フィッシングの犯人はあなたになりすましてより多くの情報にアクセスし、メールを盗み見たり、あなたのふりをして友達にメッセージを送ったり、あなたのお金を盗んだりする可能性もあります。また、新しいパスワードを勝手に作成して、あなたをアカウントからブロックすることもできます。

課題

配布資料

課題

参加者に、次の質問に答えてもらいます。回答は「パスワードに関する学習」の配布資料に文章や図で書き込みます。

1. 今回の講座で学んだ中で、次回パスワードを作成する際に活かそうと思う点を3つ挙げてください。
2. 他人にパスワードを教えてもよいと思える場合を1つ挙げてください。
3. パスワードを他の人と安全に共有するための方法を3つ挙げてください。
4. パスワードが間違っただ人の手に渡った場合に起こりうる悪いことを3つ挙げてください。