人間は高品質の暗号化キーを安全に保存することができず、暗号化操作を実行するときに許容できない速度と正確さを持っています。  
これらのデバイスが製造され、配備され続けていることは驚くべきことです。  
 – KAUFMANN、PERLMANおよびSPECINER [1025]アマチュアのみがマシンを攻撃します。専門家は人々を対象としています。  
  
–トーマス・マコーレイ  
  
実際の攻撃の多くは、少なくともテクノロジーと同じくらい心理学を利用しています。  
フィッシングのようなオンライン詐欺は、多くのオンライン保護メカニズムが実際の同等のものほど使いやすく、偽造するのが難しいため、類似の現実世界の詐欺よりも実行が簡単で、阻止するのが困難です。  
私たちは何百万年もの間、対面での欺瞞に対処するために社会的および心理的なツールを進化させてきましたが、何かをするように求めるメールを受け取った場合、これらはあまり効果的ではありません。  
現実の世界には多くの例があります。ジャガイモの皮をむくにはナイフよりもジャガイモの皮をむくほうが簡単ですが、殺人をする場合ははるかに難しくなります。  
私たちが日常業務で信頼している善悪の非対称性の多くは、簡単に自動化できる正式なやり取りだけに依存するのではなく、物理的なオブジェクトの組み合わせ、人の判断、およびサポートするソーシャルプロトコルに依存しています。  
さまざまな種類の詐欺が、オンラインセキュリティを打ち負かすために使用される主要なメカニズムになりました。  
デマや詐欺は常に発生していますが、インターネットによってそれらの一部がより簡単になり、他の人が私たちの既存の制御をバイパスする可能性のある方法で再パッケージ化できるようになります（個人的な直感、会社の手順、法律さえも）  
ソーシャルエンジニアリングに基づく攻撃の急増のもう1つの要因は、人々がテクノロジーをよりよく使用していることです。  
したがって、セキュリティエンジニアは、基本的な心理学を絶対に理解する必要があります。これは、パスワードからCAPTCHAまで、およびフィッシングからソーシャルエンジニアリング全般まで、あらゆるものに適切に対処するための前提条件です。怒っているオンライン暴徒の根底にあるメカニズムと、テロリズムからパンデミック病への緊急事態への社会的対応を理解するために、リスクの誤解と恐怖の実際的な理解も必要です。  
この章の残りの部分では、まず心理学の関連する調査を調査し、次に、パスワード認証メカニズムを攻撃に対してより堅牢にするための原則をどのように適用するか、より一般的にセキュリティのユーザビリティに、そしてそれを超えて優れた設計に取り組む。  
3.2心理学研究からの洞察  
コンピュータサイエンスよりもずっと長い間研究されてきましたが、私たちの心の理解は完全ではありません。脳は非常に複雑です。  
私たちは「心は脳がすること」であることを知っていますが、私たちの自己と個人の歴史の感覚の根底にあるメカニズムは不明瞭なままです。  
以下では、私たちの貿易に非常に関連のある心理学研究の3つのテーマのヘリコプターツアーのみを提供できます。認知心理学は、私たちがどのように記憶し、どのような間違いを犯したかなどのトピックを研究します。社会心理学は、グループ内の他の人々や権威とどのように関係しているかを扱います。また、行動経済学は、測定可能で搾取可能な方法で一貫して非合理的な決定を下すように導くヒューリスティックとバイアスを研究します。  
3.2.1認知心理学  
それは、私たちがどのように考え、記憶し、決定を下し、さらには空想するかを扱います。  
多くの有名な結果があります。  
これらの洞察の多くはマーケティング担当者や詐欺師が使用しますが、ほとんどのシステム開発者は誤解している、または無視しています。  
 同時選択[1317]とその結果、多くの設計者はメニューの選択を約5つに制限しています。  
人々は最初にどこを見ればよいかを思い出して情報を検索し、次にスキャンします。関連するメニューが見つかったら、10個のアイテムをスキャンするのは、5つスキャンするの2倍の困難です。  
ここでも、空間構造の記憶は反響の記憶とは異なるため、ミラーの洞察は誤用されています。  
近年、この分野の重心は、適用された認知心理学から人間とコンピューターの相互作用（HCI）にシフトしていますその結果、HCIの研究者は、知覚、運動制御、記憶、問題解決など、人間のパフォーマンスをモデル化して測定するだけではありません。また、ユーザーのシステムのメンタルモデルがどのように機能するか、開発者のメンタルモデルとどのように異なるか、およびテクニック（タスク分析や認知ウォークスルーなど）についても理解を深めました。  
セキュリティ研究者は、これらのプラウシェアを剣に変える方法を見つける必要があります（悪者はすでにそれに取り組んでいます）  
ぶら下がっている果物がいくつかあります。たとえば、安全研究コミュニティは、機器を操作するときに人々が犯すエラーの研究に多くの努力を注いでいます[1589]。  
スキーマ、つまりメンタルモデルは、コンピュータよりもはるかに優れて人、音、概念を認識できるため、間違ったモデルがアクティブになったときに脆弱になります。  
•実行されるアクションはスキルの問題になることがよくありますが、手動のスキルが失敗した場合（たとえば、間違ったボタンを押すなど）は、スリップする可能性があり、間違ったスキルを使用することもできます。  
。  
したがって、システムを設計するときは、ソフトウェアのインストールなどの危険なアクションが、通常のアクションシーケンスとはまったく異なるアクションシーケンスを必要とすることを確認する必要があります。  
1つの例は、完了後のエラーです。すぐに目標を達成すると、整理整頓のアクションから気が散ってしまいます。  
•ルールに従っている人は、間違ったルールに従うとエラーが発生しやすくなります。  
フィッシャーマンは多くのトリックを使用して、httpsの使用から「安全」のため、人々に間違ったルールを実行させます。  
•3番目のカテゴリの間違いは、認知上の理由で人々が犯したものです。彼らは単に問題を理解していないか、誤解しているふりをして、作業を完了するためのアドバイスを無視します。  
また、ほとんどのプログラマはセキュリティメカニズムも使用できないため、多くのセキュリティバグが発生するという認識が高まっています。  
保護メカニズムがかなり誤った方法で使用されている場合でも、プログラムはしばしば機能しているように見えます。  
彼らはこれが悪いことをよく知っていますが、もっとうまくやる時がありません。  
ジェームズギブソンは、行動の可能性またはアフォーダンスの概念を開発しました。物理的な環境は、動物にとって登ることができるか、脱落可能か、または下がることができ、同様に座席は座ることができます。  
多くの場合、認識はアフォーダンスで構成されます。アフォーダンスは、価値や意味よりも基本的なものです。  
不注意な人のためのトラップを設計することもできます。落とし穴を堅い地面と間違える動物は困っています。  
私たちの目が環境に対して相対的に動くとき、結果として得られる光学的な流れは、画像を解釈し、その中のオブジェクトのサイズ、距離、および動きを理解することを可能にします。  
オプティカルフローにより、両眼視とは関係なく、周囲の物体の形状を理解できます。  
要するに、認知科学は、特定の一連の行動を簡単、困難、または不可能にするために、システムインターフェースを設計する方法に関する有用な洞察を提供します。  
間違いを簡単または困難にすることで、多かれ少なかれ間違いを犯す可能性があります。セクション28.2.2では、医療機器と航空機の両方に関わる重大な事故を引き起こすユーザビリティの失敗の実際の例を示します。  
防御側は攻撃者に何を期待できますか？  
これらを探すには、コードウォークスルーを使用してソフトウェアの脆弱性を検索できるのと同じように、攻撃ポイントを特定するための認知ウォークスルーを試す必要があります。  
したがって、すでに機能している攻撃に注意することが重要です。  
   
多くの女性は、医療検査と技術が患者を男性であると想定しているため、またはエンジニアが車を設計するときに男性の衝突試験ダミーを使用しているために死亡しています。スポーツウェアからスタブベスト、宇宙服まで、防具はデフォルトで男性用に調整されています[498]。  
 彼らは男性によって設計されており、当時はマニアックな若い男性ですが、ユーザーの半分以上が女性である可能性があります。  
初期の実験は行動の研究から始まりました。実験は女性が周辺視野をより多く使用することを示し、より大きなディスプレイは性別バイアスを減らすことが正式に判明しました。  
しかし、自然はどれくらいで、どれだけ育てるのでしょうか？  
ジェンダーは心理学の研究で物議を醸すトピックとなっています。共感者として（一般に他者の感情や社会的知性を直感するのが得意）  
ほとんどの男性は体系化でより高いスコアを示し、ほとんどの女性は共感でより優れています。  
バロンコーエンの研究は、アスペルガーおよび自閉症スペクトラム障害に関するもので、彼はそれを男性の脳の極端な形と見なしています。  
私たちがそのように生まれていれば、それは間違いではありません。  
これは、なぜ女性よりも男性がコンピューターサイエンスに興味を持っているのか、女性が一貫してアメリカとイギリスのCSの約6分の1を占める理由を説明しているのでしょうか  
ポーランド、ルーマニア、バルト三国の旧共産国では、CSの学生の3分の1を女性が占めていますが、インドの数はほぼ同じです。  
私が1970年代に始めたとき、女性プログラマーは男性と同じくらい多く、開拓者の多くは、産業界、学界、政府のいずれであっても女性でした。  
「男性の脳/女性の脳」の説明に対する議論は、ダフナジョエルや、脳の認識可能な男性と女性の特徴はあるものの、個人の脳には両方のモザイクです[985]。  
私たちの筋肉と同様に、私たちが運動する組織はより大きく成長します。  
他の研究では、性別によるパフォーマンスの違いは新生児には見られず、6歳から7歳頃に見られます。その頃までに、子供たちは性別を区別し、その周りの社会的な手がかりに適応することを長い間学んでいます。青/ピンクの性別玩具とマーケティングの津波。  
 これは、彼らがアイデンティティの一部として内在化する性別ステレオタイプによって、後の小児期および青年期に強化されます。女の子が数学が得意ではない、またはコンピュータに興味がないと思われる文化では、「数学が得意」であることを称賛することで、ステレオタイプの脅威（自分が属するグループについて否定的なステレオタイプを確認する恐れ）を呼び起こすことができます。  
おそらく結果として、男性は個人的な賞賛に対してよりよく反応します（「それは本当にあなたの頭が良かった！」）  
。  
さらに、同様のメカニズムが、非学術的であるとシグマ化されている民族グループの貧弱な学術的パフォーマンスの根底にあるように見えます。  
細胞と回路を含む、遺伝子と培養の間にはいくつかの層があります。  
この調査については、Gina Rippon [1605]を参照してください。  
たとえば、車の方が高速か安全か。  
彼らはカーレースに勝つために男性はより優れたドライバーですか、それとも保険金請求が少ないため女性はより優れたドライバーですか  
米国の調査では、リスクは白人と男性の方が低いと判断されており、より詳細な研究では、白人男性の約30％がリスクを非常に低いと判断しているためです。  
アジアの男性は、自動車などのいくつかの危険に対して同様に低い感度を示します。  
もちろん、私たちのエンジニアは、教育システムや実際に私たちの文化のバイアスが少なかった場合のようにではなく、そのまま世界と連携する必要があります。しかし、コンピューターシステムは自動車や宇宙服のように男性によって男性のために構築されているため、コンピューターシステムが差別化される可能性があることに注意する必要があります。  
ジェンダーとセキュリティの使いやすさについて多くの作業を行った人はいませんので、機会があります。  
多くのシステムは、白人またはアジア人であり、直接遭遇しないさまざまな形の偏見や障害について、まったくまたはまったく考えていない若いフィットストレートの賢い男性によって設計され続けます。  
開発チームのトークンオタクの​​女の子が新製品をテストするだけでは十分ではありません。虐待関係にある高齢者、子供、女性など、教育が少なく脆弱なことについても考える必要があります（これについては後で詳しく説明します）。  
スタック全体について考える必要があります。  
開発者の不均衡を修正できない場合は、別の場所で補うことをお勧めします。  
グループの行動に関連する要素の多くは社会的起源のものなので、次に社会心理学に目を向けます。  
3.2.3社会心理学  
性別、部族、チーム、職業、さらには宗教に関係なく、人々がグループに所属することから派生するアイデンティティから、自分と他の人を比較することで得られる自尊心を通じて、多くの側面があります。彼らのすぐ後には、犯罪と治安にも非常に関連する傍観者効果に関する研究が行われた。  
3.2.3.1権限とその乱用  
被験者は、実際には実験者のバカである他のグループメンバーから間違った意見を聞いて、線の長さを判断しました。  
スタンレーミルグラムは、ナチス戦争犯罪者アドルフアイヒマンの1961年の裁判に触発され、実験者の要請により「学習者」の役割を演じる俳優に激しい電気ショックを与える準備ができた実験対象の数を調査しました。 「教師」の役割–「学習者」がひどい痛みを感じて被験者に止めるように頼んだときでさえ  
ほとんどがそうでした–ミルグラムは、彼らに言われたら一貫して被験者の60％以上が実に不道徳なことをすることを発見しました[1312]。  
3つ目はスタンフォード囚人実験でした。これは、通常の人々が命令がなくても邪悪な行動をとることができることを示しています。  
実験の目的は、看守（そしておそらく囚人）が刑務所での虐待を起こしたかどうかを発見することでした。  
しかし、ワードの役を演じる学生は急速にサディスティックな権威主義者となり、実験は倫理的な理由から6日後に中止された[2073]。  
しかし、ビジネスの運用上のセキュリティ対策を設計している場合は、権限の乱用は、現実のものであろうと表面的なものであろうと、真の問題です。  
 若い従業員を盗難の疑いで拘束し、ストリップサーチする。  
元刑務所の警備員が警察官になりすまして起訴されたが無罪となった。  
マクドナルドは、いたずら電話のパターンが確立されてから数年後でも、店長を適切に訓練しなかったとして訴えられました。そして2007年10月、陪審員は彼女が18歳の従業員であったときにストリップ調査された犠牲者の1人に$ 610万ドルを支払うように彼らに命じました。  
ボーイフレンドは5年になり、マネージャーは彼女を違法に拘留した罪を認めた。  
ケンタッキー州の陪審員はこれを購入せず、マクドナルドに支払いを命じました。  
そのため、米国の雇用主は、権限の乱用に抵抗するようにスタッフを訓練することに失敗した場合、大きな損害を被る危険性があります。  
3.2.3.2傍観者効果  
報道によると、38人の目撃者が警察に通報することもできず、襲撃は30分近く続いたとのことです。  
John DarleyとBibb Latan´eは、1968年に、てんかん発作を起こしているように見える誰かを助ける傍観者の確率を調整する要因についての実験を報告しました。  
別の傍観者が男性であるか、女性であるか、または医学的に資格があるかどうかでさえ、本質的に違いはありませんでした[513]。  
何かをやりたい場合は、3人ではなく1人にメールで質問します。  
ただし、危険にさらされている場合、本当の問題は、傍観者の少なくとも1人が助けになるかどうかであり、ここでの最近の研究ははるかに肯定的です。  
したがって、傍観者が一般に反対側を通り過ぎると仮定するのは誤りです。したがって、傍観者効果の名前はかなり誤解を招きやすいものです。  
3.2.4詐欺の社会的脳理論  
欺瞞はどのように機能し、それをどのように検出および測定でき、どのように阻止できますか？  
それまで、人類学者は、より良いツールを作るために私たちはより大きな脳を進化させると考えていました。  
旧石器時代全体を通して、私たちの脳はチンパンジーのサイズから人間のサイズに進化しましたが、同じシンプルな石の軸を使用しました。  
では、ニックハンフリーに尋ねた理由は、大きな脳がまだ必要ないのに進化させたのでしょうか。  
私たちの祖先は、より優れたツールを作るために大きな頭脳を進化させませんでしたが、ツールとして他の霊長類をよりよく使用しました[934]。  
それまで社会心理学は貧しい国のいとこであり、厳格とは見なされていませんでした。それ以来、人々はそれがおそらく認知進化の原動力であることに気づきました。  
（タコは例外ですが、捕食者と獲物がどのように反応するかを理解する必要があります。）  
共感などの社会化の肯定的な側面も重要であるため、誰もがこの特徴付けに完全に同意するわけではありません。  
私たちの目標は、真実ではなく説得です。レトリックが最初に来て、ロジックが2番目に来る。  
この実験、サリー-アンテストでは、子供がアンと子供が見ている間、サリーがカップの下に隠したお菓子を見ます。アンはそれから戻ってきて、子供はアンが甘いと思うところを尋ねられます。  
サイモンバロンコーエン、アランレスリー、ウタフリスは、アスペルガース/自閉症スペクトラムの子供たちがこの能力をかなり後に獲得することを示しました[177]。  
これにはあらゆる意味があります！私たちは政治、上級幹部の間、およびマーケティングにおいて過小評価されています。  
オタクは内部告発者である可能性も高くなります。私たちは、他人を喜ばせるためだけに不快な真実について沈黙を守ることはあまりありません。  
スペクトラムに参加している有名なオンライン犯罪者の何人かは、何よりも不幸でした。ゲーリー・マッキノンは、国防総省をハッキングして、飛行中の受け皿に関する真実を発見したと主張し、FBIの対応の過酷さを予想していませんでした。  
気質の共感の欠陥を持つ他の人々には、他人の感情を無視するが十分に理解してそれらを操作する精神病者が含まれます。彼らは人種差別主義者でなければならないので、彼らの対戦相手は人間よりも少ないか、または道徳的に死に値するものであると考える兵士およびテロリストにとって。  
3番目のスレッドは自己欺瞞です。  
不便な真実を忘れ、信じたいことを合理化します。  
しかし、それは議論の余地があり、多くのレベルでです。  
 誠意をどのように定義しますか？  
 そして、彼らがあなたにうそをつくことができないと予想したならば、あなたは国家指導者を選ぶことさえしますか？  
Russell Golman、David Hagman、George Loewensteinは、情報が無料で、より良い意思決定につながる可能性がある場合でも、人々がどのように情報を回避するかに関する調査を調査しています。投資家は、市場がダウンしているときはポートフォリオをあまり見ません[781]。  
また、ソーシャルメディアへのフィルターバブルの影響とも関連しています。  
人々は自分を正直であると考え、逸脱から生じる倫理的不協和音を避けようとします[172]。犯罪学者は、中和という用語を使用して、ルールブレーカーが自分の行動について感じる罪悪感を最小限に抑えるために使用する戦略を説明します（フィルター効果と自己欺瞞の両方に重複があります）。  
もう1つのリンクは、ヒューゴメルシエとダンスパーバーの議論の機械としての脳に関する研究です。  
敵意の検出は、私たちの祖先の進化的環境では大きな問題でした。州の前の社会では、恐らく男性と少年の4分の1が殺人で亡くなり、さらに後世の多くは動物の捕食者によって殺されました。  
その結果、私たちは今、テロなどの敵意を伴う脅威に対する防御に費やしすぎており、さらに多くの人々を殺す疫病やさらに多くを殺す可能性のある気候変動に対する防御に十分ではありません。  
暗号化では、信念のロジックを使用して認証プロトコルのセキュリティを分析し、「アリスはボブがチャーリーがキーKを制御していると信じている」などのステートメントを処理します。これについては、次の章で説明します。  
ダン・デネットは哲学の意図的なスタンスを導き出し、推論するときに使用する命題の態度-信念、欲望、および認識-は、人や動物の意図に帰着すると主張しました。  
ワソンテストでは、片側に文字の等級があり、もう一方に数字のコードがあるカードを検査する必要があることを被験者に伝え、「カードの前面に生徒がD級を持っている場合、その後、背面にはコード3”のマークを付ける必要があります。  
 D、F、3、7の質問に対して、「どのカードを裏返して、すべてのカードが正しくマークされていることを確認する必要がありますか？  
しかし、進化心理学者のレダコスミデスとジョントゥービーは、ルールが「ビールを飲んでいる場合、彼は20歳でなければならない」に変更され、個人がビールを飲む人、コーラを飲む人、25歳と16歳。  
CosmidesとToobyは、論理とおそらく算術を実行する私たちの能力は、社会的交流を規制する手段として進化したと主張しています。私はナイジェリアの詐欺師が、詐欺に陥る白人はアフリカ人は愚かであるに違いないと考えているので、それに値するものだと述べました。詐欺師が外国の標的を公正なゲームと見なしている例はもっとたくさんあります。  
人々は雇用主が彼らに十分に支払っていないので、費用を処理することは正当化できる、または彼らが税金をだますとき、福祉のためにお金を浪費していると感じるかもしれません。  
DDoS-for-hireサービスを運営している子供たちは、「ウェブストレッサー」サービスの提供は合法であるとお互いに安心させ、そのサービスは合法的な目的にのみ使用できるとウェブサイトで述べました。  
英国国家犯罪庁は、Googleの広告を購入して、ウェブストレッサーサービスを検索しているすべての人に、DDoSが犯罪であるという公式の警告が表示されるようにしました。  
最後に、社会的文脈の喪失は、オンラインの脱抑制の要因です。  
恥ずかしがり屋の人々はパートナーを見つけることができますが、私たちは悪質な炎の戦争も見ます。  
これがすべての主導権を握るのは、オンライン詐欺の性質と規模は、適切な相互作用設計によって調整できるということです。  
彼らは、WhatsAppがサポートするグループなど、パフォーマンスを刺激する有名人もトローリングを促進する匿名性も提供していないクローズドグループを警戒しています。  
  
2000年代半ば以降、セキュリティ研究者によって適用されてきた心理学の1つの分野は意思決定科学であり、心理学と経済学の境界に位置し、人々が使用するヒューリスティックと、意思決定の際に彼らに影響を与えるバイアスを研究しています。 。  
初期の先駆者は、初期のコンピューター科学者でありノーベル賞を受賞したエコノミストであるハーブサイモンでした。彼は、古典的な合理性は、計算の選択がどれほど難しいかに関係なく、期待される有用性を最大化することを行うことを意味すると述べました。  
 以来、人間の合理性に対する真の限界が広く探求されており、ダニエル・カーネマンは、この分野への彼の主要な貢献により（後期のアモス・トベルスキーとともに）2002年にノーベル経済学賞を受賞しました。  
  
カーネマンとトヴェルスキーは、人々が不確実性に直面して意思決定をどのように行ったかについて広範な実験的作業を行いました。  
損失を回避するようにアクションを構成すると、人々はそれを実行する可能性が高くなります。フィッシング詐欺師は、「PayPalアカウントが凍結されているため、ここをクリックしてロックを解除する必要があります。」などのメッセージを送信して人々を引っ掛けます。また、確率の計算が苦手であり、あらゆるヒューリスティックを使用して意思決定を支援します。最初の推測または比較に基づいて判断し、必要に応じて調整します。アンカー効果。 •私たちは、例を頭に浮かびやすくすることに基づいて推論を行います。可用性のヒューリスティックは、5万年前のライオンの攻撃には問題ありませんでしたが、マスメディアがテロのイメージで私たちを攻撃したとき、間違った答えを出しました。 •ニューロンの処理のビジョンが増えているため、見たものよりも聞いたものに懐疑的になる可能性が高くなります。 •非常にありそうもないが非常に悪い結果をもたらす出来事について心配しすぎています。 •私たちが言われたことよりも、自分で解決したことを信じる可能性が高くなります。  
多くの人々は、テロリズムを伝染病、交通事故、さらには食中毒よりもはるかに悪い脅威であると認識しています。これは間違っていますが、行動経済学者にはほとんど驚くことではありません。  
（テロについて議論するときにパートIIIで探求する他の要因があります。）  
心理学者のダニエル・ギルバートは、挑発的に「ゲイのセックスだけが地球温暖化を引き起こした場合」と題された記事の中で、テロに対する恐怖と気候変動に対する恐怖を比較しています。  
 雷雨よりもはるかに悪い脅威でした。  
さらに多くのリスクバイアスがあります。たとえば、車や飛行機の乗客とは対照的に、車を運転しているときなど、私たちがコントロールしているときのほうが恐れが少なくなります。不確実性を恐れています。つまり、リスクの大きさが不明な場合（たとえ小さい場合でも）  
また、特に小規模なトランザクションの場合、確率を完全に計算しようとするのではなく、「十分に良い」代替案を採用することで満足度を高めます。  
 したがって、手にある鳥は茂みの中で2匹の価値があると言う人々から始めて、私たちはリスクに対する人々の態度を理解し、モデル化するのに役立つ非常に多くの機械を開発できます。3.2.5.2現在のバイアスと双曲線割引  
この現在のバイアスにより、多くの人が更新を拒否します。これは、長年オンラインでの技術的な脆弱性の主な原因でした。  
リマインダーにより、無視率が約90％から約34％に削減され、最終的には全体的なコンプライアンスが2倍になる可能性があります[726]。  
双曲線割引は、現在のバイアスを定量化するために意思決定科学者が使用するモデルです。  
そのようなモデルは、プライバシーのパラドックスを説明しようとするために適用されています-なぜ人々は調査でプライバシーに関心があるがオンラインでは行動しないと言うのか。  
まとめると、無料のものを手に入れることの即時かつ確定的な有用性は、あまりにも多くの個人情報を公開したり、疑わしいWebサイトに公開したりする将来のランダムなコストを上回ります。  
3.2.5.3デフォルトとナッジ  
多くの人々は通常、最も簡単な方法でシステムの標準構成を使用します。システムが十分であると想定しているからです。  
たとえば、会社のスタッフがデフォルトで年金プランに登録されている場合、ほとんどがオプトアウトする必要はありませんが、オプションである場合はほとんどオプトインしません。  
3番目の例は、フォームの情報が最後ではなく記入し始めたときに、フォームの情報が真実であることを納税者に宣言させることで、脱税を削減できることです。  
Sunnsteinはオバマ政権でこれらのアイデアのいくつかを実装する仕事を得、Thalerは2017年の経済ノーベル賞を受賞しました。  
たとえば、Facebookはデフォルトでかなりオープンな情報共有を行います。十分な数の人々がプライバシー設定を増やす方法を考え出したときはいつでも、アーキテクチャーが変更されるため、もう一度オプトアウトする必要があります。  
私たちは、コントロールを感じるのが好きです。私たちは、飛行機の中で他の人を飛ばすよりも、後者の方がはるかに安全であっても、車での運転をより快適に感じます。  
「Facebookはこれを設定しているので、非常にきめ細かい制御が可能になります。」 [1533]  
行動経済学者は、心理学の長い伝統に従い、心を「心」と「頭」、または「感情的」と「認知的」システムの相互作用する合理的で感情的な要素で構成されていると見なします。  
 そして物理現象。  
子どもたちは物理学を使って自分が見ているものを説明しようとしますが、理解が足りないときは、意図的な行動の観点から現象を説明します。  
ブルームはそれが興味深い副作用を持っていることを示唆しています：それは人間に体と魂が異なると信じるようにさせます、そしてそれゆえに宗教的信念の基礎を築きます。  
。  
最初に、それは根本的な帰属エラーを説明するための何らかの方法になります-人々はしばしば文脈からではなく意図性から物事を説明しようとすることによって誤りを犯します。  
理性が尽きるたびにエモーショナルが引き継ぐようにプログラムされている場合、フィッシャーマンとの技術指導と反指導の戦争に参加することは、彼らが上手くなるので不健全です。  
  
メカニズムではなく意図の観点から考えるように人々を誘惑すると、ポールスロビックおよび同僚[1787]が調査した影響ヒューリスティックを利用できます。  
そのため、感情を際立たせることで、マーケティング担当者や詐欺師は、理由ではなく感情を使用し、計算ではなく発見的方法を使用して、質問に回答してもらうことができます。  
」や「トランプ大統領についてどう思いますか？  
 人々を確率に鈍感にする。  
同様に、癌からテロまで恐怖感を呼び起こす出来事は、裸の確率が正当化する以上に人々を怖がらせるだけでなく、それらの確率を計算することを困難にし、人々が努力をすることさえも阻止します。  
私たちの自制能力はまた、肉体的および精神的に疲労しがちです。暗算によっては、リンゴではなくチョコレートを選ぶ確率が高くなります。  
  
社会心理学のもう1つの興味深い派生物は、認知的不協和理論です。  
現実的な結果の1つは、物事がうまくいかなかったという証拠が山積しているにもかかわらず、人々が誤った行動方針を継続的に継続できることです[1863]。  
セキュリティ専門家は「騒ぎを感じる」必要があります。つまり、最近確立された社会的手がかりと期待が、通常は予約していることを「ただやる」よう圧力をかけている状況に注意する必要があります。しかし、これを知覚するように人々を訓練することは十分に困難であり、平均的な人々に社会の流れを打ち破り、「やめろ！  
そのようなトレーニングを主流化することの問題は、そのトレーニングに利用できるお金が、顧客を混乱させるビジネスモデルを持っている企業のマーケティング予算よりも桁違いに少ないことです。  
3.2.5.7リスクサーモスタット  
ジョンアダムスは必須のシートベルト法を研究し、実際に命を救うのではなく、車両の乗員から歩行者や自転車に死傷者を移送するだけであることを証明しました[20]。  
彼はこれをリスクサーモスタットと呼び、モデルは他のアプリケーションでも実証されています[19]。  
  
これは私たちを理論から実践へと導きます。  
営業担当者が休暇用アパートのファイナンスプランの提案であなたを驚かせるかもしれませんが、警官は彼らの存在によってあなたをより注意深く運転するように注意を促し、パークレンジャーはキャンプ場を注意深く消火してクマに餌をやらないように指示するかもしれません。企業の弁護士があなたのウェブサイトから何かを削除するようにあなたを脅すかもしれません。  
しかし、エコノミストが、そのようなテクニックの利他的な使用がセルフィッシュのテクニックよりも一般的になると考えたことは奇妙です。  
スタンフォード大学の説得テクノロジーラボは、人々を画面に夢中にさせる技術を開発する最前線にあり、卒業生の1人である元Google社員のトリスタンハリスは、批評家になりました。  
スマートフォンやその他の画面はメニューを表示するため、選択肢を制御しますが、それだけではありません。  
 ボトムレスメッセージフィード（空腹でなくなったときでも消費し続けるため）  
しかし、コンピュータに先行する多くの古い技術があります。  
3.3.1セールスマンと詐欺師  
著名な作家は、貿易のトリックを文書化するために中古車から住宅改修、生命保険まですべてを販売する夏の仕事を取った心理学教授のロバート・チャルディーニです。  
これらは：1。  
コミットメントと一貫性：一貫性がないと感じた場合、人々は認知的不協和を被ります。 3。  
これは、メンバーであるグループの他のメンバーをフォローすることを意味し、グループが小さいほどプレッシャーが強くなります。 4。  
権威：ほとんどの人々は権威のある構成に敬意を払っています（上記のミルグラムの研究を思い出してください）  
希少性：必要なものが突然利用できなくなる可能性がある場合、見逃してしまうことを恐れています。  
彼らはまた、食料不足が本当の脅威であった祖先の進化的環境における圧力にたどることができます。見知らぬ人は危険であり、彼らに対する集団連帯をする可能性があります（そして食料と避難所の提供において）  
すべてが繰り返し広告やその他のメッセージで頻繁に使用されます。  
ウィルソンは、最も一般的な詐欺「The Real Hustle」について、9シーズンのテレビ番組を調査して登場しました。そこでは、疑いを持たない一般の人々に詐欺が行われ、彼らは返金され、報告を受け、ビデオの許可を求めました。テレビで使われる映像。  
1。  
これはほとんどの魔法のパフォーマンスの中心です。  
社会的コンプライアンス–社会は、権威を持っているように見える人々に質問しないように私たちを訓練し、銀行や警察から来たふりをするconmenに対して脆弱な人々を残しています。  
群れの原則–周りの誰もが同じリスクを共有しているように見えるとき、人々は警戒を怠ります。  
4。  
多くの人は「違法だから大金を手に入れている」という考えに惹かれ、詐欺で入手した飛行機のチケットの再販など、詐欺家族全体がこれを有効にします。  
優しさ–これは不正直さのフリップ面であり、Cialdiniの相互主義の原則を採用したものです。  
6。  
良い詐欺師は、マークが夢を夢見るのを助け、これを使って搾乳することができます。  
時間のプレッシャー–これにより、人々は考えるのをやめるのではなく、内臓的に行動するようになります。  
;詐欺師もそうです。  
皮肉屋は、詐欺は単にマーケティングの細分であると言うかもしれません。それとも、マーケティングがますます攻撃的になるにつれて、詐欺のように見えるようになります。  
実際、詐欺師の行動はCialdiniのモデルによってすでに十分に説明されていましたが、詐欺師は同情への訴え、自身の信頼性を確立するための議論、および異議への対処方法を追加しました[2062]。ああ、私たちも同じことをソフトウェアで見つけます。そこでは、違法なマルウェアと合法くらいの「潜在的に望ましくないプログラム」（PUP）のあいまいな境界線があります。  
優れた区別の1つは技術的なもののようです。マルウェアは、逮捕のリスクがあるため、多くの小さなボットネットによって配布されますが、PUPは、主に1つの大きなネットワークによって配布されます[954]。  
悪質な企業は、WebサイトでのTRUSTeプライバシー証明書などの安価な信頼信号を示す可能性も高かった。  
そして、「合法」ビジネスの不正なマーケティング慣行があります。  
これらのうち少なくとも183は明らかに欺瞞的でした[1242]。  
詐欺の起訴のしきい値にわずかに近い詐欺からのこの一定の圧力は、一般に信頼に冷酷な影響を及ぼします。  
また、ソフトウェアの更新に対する信頼が失われることさえあります。調査によると、セキュリティに関する機能のアップグレードを適用する可能性は、セキュリティパッチよりも低いと言われていますが、アップグレードに関するフィールドデータは（まだ）ありません  
  
システムを操作する人々によるシステムのハッキングは新しいものではありません。  
民間の調査機関はそれほど遅れていません。  
産業プロセスの例は、英国の私立探偵がどのように人々を追跡したかでした。  
私の同僚は1996年にイギリスで実験を行い、そのような呼びかけを特定して報告するように地方の保健当局のスタッフを訓練しました1。  
これは最終的には修正されましたが、10年以上かかりました。  
20世紀のもう1つの古い詐欺は、誰かのATMカードを盗んで、銀行から来たふりをして、カードが盗まれたかどうかを尋ねる電話をかけることです。  
話は詳しくは、この本の第2版の第9章で詳しく説明されています。オンラインで無料で入手できます。  
アートフォームに関しては、これまでに発行された最も不安なセキュリティブックの1つは、ケビンミトニックの「Art of Deception」です。  
彼の典型的なハックは、電話会社の従業員に同僚であるふりをして、パスワードなどの「助け」を求めることでした。  
嫌がらせを受けたシステム管理者は、CEOのパーソナルアシスタントであると主張する誰かによって、些細な問題について1回または2回呼び出されます。このアイデアが受け入れられると、発信者は上司に新しいパスワードを要求します。  
ソーシャルエンジニアリングは2006年9月に世界的なニュースになりました。Hewlett-Packardの会長であるPatricia Dunnが、彼女に不審な他の取締役と彼女が敵対的であると考えたジャーナリストの電話記録を入手するために口実を使用した私立探偵を雇ったことが明らかになったときです。  
探偵は詐欺的な有線通信で有罪判決を受け、コミュニティサービスを行うように宣告された[138]。  
ソーシャルエンジニアリングに関する知名度が高まる中、2007年に税務管理の財務総監によるIRSの監査があり、そのスタッフはすべてのレベルで102人のIRS従業員に電話をかけ、ユーザーIDを要求し、パスワードを既知の値。 62人がそうしました。  
それ以来、多くの監査事務所がソーシャルエンジニアリングをサービスとして提供してきました。監査クライアントをフィッシングして、それがいかに簡単かを示します。  
ソーシャルエンジニアリングは、個人情報の盗用に限定されません。  
この章の冒頭にあるブルースシュナイアーの引用は、株式詐欺の報告に出ており、偽のプレスリリースでは、会社のCEOが辞任し、その収益は修正されると述べています。  
この種の偽のニュースは永遠に存在していますが、インターネットにより宣伝が容易になり、ソーシャルメディアが普及しているようです。  
2非常にまれに、顧客が銀行を混乱させることがあります。 2019年のイノベーションは「コールハンマー」攻撃で、誰かが繰り返し電話をかけて「彼の名前」のスペルを「修正」し、一度に1文字ずつ別の名前に変更しました。  
3.3.3フィッシング  
オペレーターにはスパイとスパイの両方が含まれますが、ターゲットはスタッフと顧客の両方です。  
彼らはあなたが彼らを騒がせようとしている、あなたの警告を無視し、あなたのシステムから彼らが望むものを得る最も簡単な方法を見つけ出そうとしていると仮定します。  
英語を上手に話せない人、失読症の人、または学習が困難な人がシステムを使用するのが安全でない場合は、深刻な法的問題を求めています。「フィッシング」という言葉は、1996年にAOLパスワードの盗難に関連して出現しました。  
また1996年に、トニー・グリーニングは体系的な実験的研究を報告しました：シドニー大学の336人のコンピューターサイエンスの学生に、中断の疑いがある場合にパスワードデータベースを「検証」する必要があるという口実にパスワードを提供するように求める電子メールメッセージが送信されました-に。  
一部は疑わしいものでした。30人は見た目は妥当であるが無効なパスワードを返し、200人以上が公式なプロンプトなしにパスワードを変更しました。  
銀行に対するフィッシング攻撃は7年後の2003年に始まり、半ダースの試みが報告されました[441]。  
ほとんどの顧客はネズミを精錬します。  
もちろん、www.paypal.comを入力したり、既存のブックマークを使用したりするのではなく、提供されたリンクを使用した顧客は、アカウントを空にします。  
彼らは、ロシアの詐欺グループによって最初に使用されたクライムウェアツールを使用しました。  
より複雑なログオンスキーム（2要素認証またはその低コストのいとこ、パスワードのランダムな文字列の要求を使用）など、いくつかの対策が事態を制御しやすくしました  
フィステルマンは、顧客の資格情報を盗むことと、アカウントを使用して盗まれた資金を洗浄することの両方の点で、各国でいつでも最も簡単な目標を達成するという点で、競争の状況は厳しいものでした。  
それ以来、Amazonのような非金融企業に対する大規模な攻撃が見られました。 2000年代後半に、詐欺師はメールと住所を変更し、クレジットカードを使用してワイドスクリーンテレビを注文します。  
前章で述べたように、フィッシングはボットマスターがボットネットに新しいマシンをリクルートするために大規模に使用され、特定の人々または企業を狙う詐欺師と諜報機関の両方が標的を絞って使用します。  
ターゲットのラップトップまたは電話にインストールされているクライムウェアが同じ厩舎からのものである場合でも、使用されるルアーとテクニックは異なります。  
結局のところ、私たちがコンピューターに依存していること、すべてのコンピューターが安全でないこと、そして常に攻撃が行われていることを考えると、なぜ文明は崩壊していないのでしょうか。  
もう1つの要因は、イノベーションの開発と普及に時間がかかることです。  
別の例として、Tom Jagaticと同僚による2007年の論文は、ターゲットのソーシャルネットワークからマイニングされたコンテキストを使用して各フィッシングを自動的にパーソナライズすることにより、フィッシングをより効果的にする方法を示しました[971]。  
これは粗雑なようで、実際にはうまくいっていませんが、悪者がそれを突き止めると、将来、スピアフィッシングが大規模に見られる可能性があり、どのように対応するかを考えるのは興味深いことです。  
私が書いているように、犯罪組織は、ランサムウェアをインストールしたり、ギフトクーポンを盗んだり、他の詐欺を仕掛けたりする企業に対する標的型攻撃で、スピアフィッシングをますます利用しています。  
彼らは、SIMスワップ詐欺についてのスピアフィッシングスキルを磨いたようです。これについては、後でセクション3.4.1および12.7.4で説明します。  
  
部外者が電話やオンラインで秘密を明かそうとする企てに抵抗するようにスタッフに要求することは、軍事界では、運用上のセキュリティまたはOpsecとして知られています。  
ルールが存在するだけでは不十分です。あなたはアクセスできるスタッフを訓練し、ルールの背後にある理由を説明し、組織に社会的に埋め込む必要があります。  
スタッフがいくつかの偽プリテキストコールを検出して無効にしたら、それについて話し、メッセージは全員の作業方法に埋め込まれます。  
空港スタイルのIDチェック、またはカードでアクティブ化されたターンスタイルでさえこれを止めると、雰囲気が変わり、文化と衝突します。  
偽の電話と同様に、重要な要素は、単なるトレーニングではなく、社会的な埋め込みです。  
私自身の銀行での経験では、トレーニングすることができなかった人々は、ディーリングルームのトレーダーのように、あなたよりも多く支払われた人々でした。  
それほど明白ではないのは、信頼できる人々を訓練する必要性です。  
人々は彼らがしなければならないシステムを操作します、そして、これは通常彼らの仕事を成し遂げるためにいくつかのルールを破ることを意味します。あなたはこの予算が何であるかを考え出し、それを賢く使う必要があります。  
しかし、企業の顧客はどうですか？  
また、顧客がビジネスプロセスの脆弱性を見つけたときに試行する小さな詐欺も数多くあります。  
  
最後に、欺瞞研究についての言葉。  
ポリグラフは、心拍数と皮膚コンダクタンスを介してストレスを測定します。これは1920年代から存在しており、米国の一部の州では刑事捜査に使用されているほか、連邦政府によって最高機密のクリアランスを求める人々をスクリーニングする際にも使用されています。  
熟練した尋問者にとっては効果的な小道具になり得ますが、重要な要素は小道具ではなくスキルです。  
皮膚のコンダクタンスを介してストレスを測定するだけでなく、目の動きや上半身の動きによる罪悪感を利用して気晴らしを測定できます。  
ただし、このようなテクノロジーは質問者のスキルを最大限に高めることができ、それらがうまく機能すると主張するのはジャンクサイエンスとして扱う必要があります。  
欺瞞に対処するための2番目のアプローチは、実際の顧客の行動について機械学習分類子を訓練することです。  
たとえば、Noam BrownとTuomas Sandholmは、テキサスホールデムの10,000ハンドの12日間のマラソンで12人のエキスパートプレーヤーを倒したPluribusと呼ばれるポーカープレイボットを作成しました。  
対戦相手の顔のジェスチャーやボディランゲージなどの「テル」にアクセスせずに、常にエキスパートを倒すことができること自体が物語っています。  
  
パスワードの管理は、ユーザビリティ、応用心理学、セキュリティが調和する有益なコンテキストを提供します。  
実際、ユーザビリティ研究者のAngela Sasseが言うように、人間の記憶について私たちが知っていることを考えると、パスワードよりも悪い認証メカニズムを考えるのは困難です。使用頻度の低いアイテムや頻繁に変更されるアイテムを覚えることはできません。オンデマンドを忘れることはできません。想起は認識より難しい。意味のない言葉はもっと難しいです  
現代のメディアエコシステムは、ページビューと登録ユーザーベースの両方を最大化して、販売時の価値を最大化しようとするWebサイトによって推進されています。  
クリックすると、広告のページがあります。  
CAPTCHAが間違っているので、もう一度入力して、広告の別のページを表示します。  
これで、誰も読まないコメントを追加できます。  
主要なニュースサイトでさえ、読者の利益に反してパスワードを使用します。たとえば、別のブラウザーで再度登録しない限り、毎月の無料ページビューの数を制限します。  
次に、より正直な使用法に目を向けると、現代の大手サービス会社で使用されているパスワードシステムには、いくつかのコンポーネントがあります。  
表示されている部分はログオンページで、登録時にパスワードを選択するように求め、おそらく何らかの方法でその強度をチェックします。  
2。  
3。  
4。  
また、これらのメカニズムにより、アクセスできたすべてのサービスのパスワードをリセットする必要なく、盗まれた電話をブラックリストに載せることができます。  
パスワードの1つがおそらく本来あるべきではない場所で使用された場合、アラームを伝達する侵入検知メカニズムがあります。  
GoogleまたはFacebookアカウントを使用して新聞にログオンするときのように、1つのログオンを多くのWebサイトに使用するシングルサインオンメカニズムがあります。  
フル機能のパスワード管理システムを開発するのは大変な作業であり、パスワード回復のサポートを提供することも費用がかかります（数年前、英国の電話会社BTはパスワードリセットセンターに2人の障害者を抱えていました）。  
したがって、「アイデンティティ管理」をアウトソーシングすることは、ビジネスに意味をなすことができます。  
パスワードを悪用しようとする主な原因は、ある企業がハッキングされ、何百万もの電子メールアドレスとパスワードを公開したことです。大きな企業はこれをすぐに見つけますが、小さな企業はそうではありません。  
繰り返しになりますが、小規模なWebサイトや、頻繁にアクセスされないWebサイトの場合は、そうすることは困難です。  
これにより、パスワードを回復できます。  
3.4.1パスワードの回復  
スタッフなどの知っている人がパスワードを忘れた場合は、それらを知っている管理者またはマネージャーと連絡を取ることができます。  
また、大規模なサービス会社は毎日数万件のアカウントを回復するため、ほとんどの場合、人間の介入なしにそれを実行する方法が必要です。このようなほぼ公開されている情報は、多くの場合簡単に推測できるため、パスワード自体を推測するよりも簡単にアカウントに侵入できます。  
有名人の場合、または以前の親しいパートナーによる虐待の場合、使用できる秘密がない可能性があります。  
これらは両方とも公開情報でした。  
これは2013年にピークに達しました。それを修正した対策は、常に口座の変更を郵送で受取人に通知することでした。  
たとえば、攻撃者は「お気に入りの食べ物」に対して19.7％の成功率を得る可能性があります。  
37％の人が間違った答えを出しましたが、場合によっては強くすることもありましたが、そうでない場合もあります。  
安全ではないことに加えて、「セキュリティの質問」は使いにくいことがわかりました。英語を話す米国のユーザーの40％は、必要なときに回答を思い出せず、SMSリセットコードを使用して2倍のアカウントを回復できました[291 ]。  
しかし、誰かがその電子メールアカウントを侵害すると、依存しているアカウントもすべて取得される可能性があります。  
これは通常、SMSによって携帯電話に送信されるコードです。コードを暗号化して特定のハンドセットに結び付けることができるアプリを使用することをお勧めします。  
Googleの調査によると、SMSはボットによるバルクパスワードの推測、バルクフィッシングの96％、標的型攻撃の76％を阻止します[574]。  
2020年の問題は、SMS認証コードのインターセプトに基づく攻撃が急速に増加していることです。これは、主にSIMスワップに関係しているようで、攻撃者はあなたをあなたの携帯電話会社に偽装し、アカウントの代わりのSIMカードを入手します。  
SIMスワップ攻撃については、セクション12.7.4で詳しく説明します。  
このような攻撃については、電話と銀行の章で詳しく説明します。  
標的型攻撃については、Ariana Mirianによる他の研究とUCSDおよびGoogleの同僚がオンラインで「ハッキングフォーハイヤー」サービスを宣伝しているギャングにアプローチし、Gmailパスワードのフィッシングを依頼しました。  
これはまだ未熟な犯罪市場ですが、このような攻撃を阻止するには、アプリまたは認証トークンが適しています。  
Gmailでハードウェアセキュリティキーを使用している場合、回復メカニズムとして金庫に2つ目のキーが必要ですか？  
 スマートフォンで1つのアプリを使用して銀行取引を行い、別のアプリを認証システムとして使用する場合、2要素認証のルールに準拠していますか？  
 電子メール通知は、疑わしいログイン試行だけでなく、コードの助けを借りて成功した新しいデバイスへのログインを人々に知らせるためのデフォルトです。  
次に被害者がどのように回復するかが次の問題です。  
ただし、このようなシステムを設計するときは、制御が不十分なメールプロバイダーとの回復メールループ、SIMスワッピングまたはモバイルマルウェアに対して脆弱な電話コード、またはソーシャルエンジニアリングにオープンな人間。  
3.4.2パスワードの選択  
2.3.1.4で説明したように、電子メールアカウントを使用してスパムを送信したり、ボットネットにマシンを募集したりするために、パスワードとパスワード回復の質問を推測することにより、オンラインアカウントに常に侵入するボットネットがあります。  
最近の例は暗号通貨のウォレットです：匿名の「ビットコイン盗賊」は、イーサリアムのウォレットにたくさんの弱いパスワードを試すことで5,000万ドルを盗むことができました[809]。  
したがって、パスワードは重要であり、重要性と難易度の昇順で、基本的に3つの大きな懸念事項があります.1。  
 2。  
 3。  
   
人的要因の最初の問題は、パスワードが長すぎるか複雑な場合、ユーザーがパスワードを正しく入力するのが困難になる可能性があることです。  
顧客がソフトウェア製品のアクティベーションコードを入力するのが難しい場合、サポートデスクへの高額な通話が発生する可能性があります。  
これは、3ワードまたは4ワードのパスフレーズなど、人々をより長く単純な秘密に向ける要因の1つです。  
 多くの発展途上国で電力を販売するために使用されるSTS前払いメーターについて興味深い研究が行われました。  
彼らはこの領収書を家に持ち帰り、メーターのキーパッドで数字を入力すると、ライトが点灯します。  
しかし、文盲は問題ではありませんでした。読むことができなかった人々でさえ、数字に問題はありませんでした（エンジニアの1人が言ったように、「誰でも電話を使用できます」）。  
最大の問題は入力エラーであり、2行に20桁を印刷し、最初の行に4桁の3つのグループ、次に2行目に2つの数字を印刷することで対処しました[93]。まったく異なるアプリケーションは、米国の核兵器の発射コードです。  
それらがこれまでに使用された場合、オペレーターは極度のストレスにさらされ、おそらく即興または時代遅れの通信チャネルを使用します。  
これが15.2でどのように進化したかについて説明します。  
3.4.4パスワードを覚える難しさ  
12桁から20桁は、電報やメーターのチケットからコピーするのは簡単ですが、顧客がパスワードを覚える必要がある場合は、攻撃者が推測しやすい値を選択するか、書き留めるか、またはその両方を行います。  
問題はコンピュータへのアクセスに限定されません。  
ホテルに着いたら、受付機でクレジットカードをスワイプし、数字のアクセスコードが記載された領収書を受け取って、部屋のドアのロックを解除します。  
よくある失敗モードは、真夜中に起きてトイレに行き、アクセスコードを忘れて、レシートを持っていなかったことに気づくというものでした。  
パスワードの覚えやすさは、5つの主要な見出しの下で議論できます。素朴な選択、ユーザーの能力とトレーニング、設計エラー、操作の失敗、ソーシャルエンジニアリング攻撃に対する脆弱性です。  
3.4.4.1ナイーブな選択  
1980年のUnixシステムからのテープの暗号解析は、開拓者のデニス・リッチーが「dmac」を使用したことを示しました（彼のミドルネームはMacAlistairでした）  
 ブライアンカーニハンは「/.,/。」を使用しました[795]。  
これらの200のパスワードのうち、少なくとも1つは、調査した数十台のマシンのそれぞれで使用されていました。  
他の調査では、文字以外を要求するだけで最も一般的なパスワードが「password」から「password1」に変更されただけであることが示されました[1672]。  
辞書の単語は7.4％、一般的な名前は4％、ユーザー名とアカウント名の組み合わせは2.7％を占め、以下同様に、サイエンスフィクションの単語（0.4％）などの可能性の低い選択肢のリストを示しています。  
。  
クライン、およびklone、klone1、klone123、dvk、dvkdvk、leinad、neilk、DvkkvDなどの試行パスワード。  
私が知っているパスワード選択に関する最大の学術的研究は、2012年に漏洩したパスワードファイルの数千万のパスワードを分析したJoe Bonneauによるもので、Yahooにインターンし、ログインシステムに機器の選択に関するライブ統計を収集するように仕掛けました。 7000万人のユーザー。  
この作業により、大手サービス会社でのパスワード強度チェッカーとその他の現在の慣行の設計がわかりました。  
3.4.4.2ユーザーの能力とトレーニング  
パスワードチェッカーは、数字と文字を含むより長いパスワードを使用するように彼らを訓練し、その効果はそれらを使用しないWebサイトに波及します[444]。  
実際、調査によると、パスワードルールの適用はリスクのある価値の関数ではなく、Webサイトが独占的であるかどうかの関数です。  
企業環境や軍事環境では、パスワード選択ルールやパスワード変更ルールを適用したり、ランダムなパスワードを発行したりできます。  
したがって、パスワードは保護するデータと同じように扱われると主張できます。銀行のマスターパスワードは一夜にして金庫に保管されますが、軍の「トップシークレット」のパスワードは封筒、金庫、鍵のかかる部屋に封をする必要があります。警備員がパトロールした建物で、占有されていません。  
ただし、優秀な人材を採用して定着させたい場合は、もう少し慎重に考えてください。  
国内の同等品は、wifiルーターの背面にあるカードとパスワードです。  
。  
したがって、トレーニングによって何が達成できるかを確認することにし、初年度の科学学生[2055]から約100人のボランティアからなる3つのグループを選択しました[2055]。•赤（コントロール）  
 •緑のグループは、パスフレーズを考え、そこから文字を選択してパスワードを作成するように指示されました。  
 パスワードを覚えてから1週間か2週間後に、テーブルから無作為に選んでメモし、このメモを破棄します。  
、続いて緑、次に赤。  
コントロールグループの約30％は、他の2つのグループの約10％に対して、Alec Muffettの「クラック」ソフトウェアを使用して推測できるパスワードを選択しました。  
パスワードのリセット率を調べたところ、3つのグループ間に大きな違いはありませんでした。  
、黄色のグループは他の2つのグループよりも著しく多くの問題を抱えていました。しかし、赤と緑の間に大きな違いはありませんでした。•指示に従うユーザーにとって、ニーモニックフレーズに基づくパスワードは、両方の長所を提供します。  
•次に、問題はユーザーコンプライアンスの1つになります。  
 彼らが言われたことをしないでください。  
。  
一般にサービスを提供する場合、顧客は競合他社と同じインターフェースを広く提示することを期待しています。  
（GCHQは、オンラインパスワードダンプで最も一般的に見られる100,000個のパスワードの「不正なパスワードリスト」を使用することを推奨しています。）  
。  
結局のところ、財布や財布を盗んだ泥棒は、最初にすべてのカードで最も一般的なPINをオフラインモードでオンラインモードで試した場合、約11分の1の確率で幸運になる可能性があります。それぞれに6ゴーを取得します。  
  
パスワードを覚えやすいものにしようとすると、重大な設計エラーが頻繁に発生します。  
驚くほど多くの銀行、政府機関、およびその他の組織は、この方法で顧客を認証していますが、現在では、パスワードではなくパスワードの回復に関する質問になりがちです。  
銀行に電話をかけて、母親の旧姓をYngstromからyGt5r4ad、さらにはSmithに変更することを決めたと伝えたら、幸運を祈ります。  
一部の組織では、コンテキストセキュリティ情報を使用しています。  
理論的には、これは役立つ可能性があります。電話での取引を誰かが私に耳にした場合、それは長期的な妥協ではありません。  
このシステムが最初に導入されたとき、私は小切手を書いたばかりのサプライヤーが私になりすましているかどうか疑問に思い、最後の3つの小切手の値を尋ねるほうが安全だと結論付けました。  
年次監査のために小切手帳を会計士に渡したので、銀行と話すことができませんでした。  
現在、パスワードを要求するアプリケーションの数は、人間の記憶力を超えています。  
Bonneauは、2012年にさらに詳細な統計を公開しました[289]が、それ以降、スマートフォンのおかげで、ユーザーパスワードの入力頻度は低下しています。  
しかし、多くの人々はさまざまな目的で同じパスワードを使用しており、銀行、ソーシャルメディアアカウント、電子メールなどの重要なログオンに対処するための特別なプロセスを考えていません。  
（ウェブサイトhttp://haveibeenpwned.comもあり、どのセキュリティ違反があなたのメールアドレスとパスワードを漏らしたかを教えてくれます。）  
1980年代に毎月実施される強制的なパスワードの変更に初めて遭遇したとき、3月は「julia03」、4月は「julia04」などのパスワードを選択するようになり、最初の多くのことを述べました（ 2001）  
。  
これは、Big Fourの監査人によって採用され、すべての監査クライアントにプッシュされました3。  
Yinqian Zhang、Fabian Monrose、Mike Reiterによる、ユーザーが発明したパスワード変換手法に関する最初の体系的な調査では、強制失効のあるシステムでは、パスワードの40％以上が以前のものから推測され、強制変更では推測されなかった弱いパスワードを選択した人々を助けるために多く、そして定期的なパスワード選択の努力もパスワードの品質を低下させたかもしれないこと[2070]。  
2017年、NISTは撤回しました。彼らは現在、妥協でのみ変更される長いパスフレーズを推奨しています4。  
ただし、多くの企業は、クレジットカード発行者によって設定されたPCI標準に引っかかっており、それらは追いついておらず、3か月ごとの変更を要求しています。もう1つの問題は、監査人が多くの企業にコンプライアンスを要求し、追いつくのに間違いなく時間がかかることです。  
これは、「正しい馬のバッテリーの定番」をパスワードとして提案した有名なxkcdの漫画によって宣伝されました。  
Electronic Frontier Foundationは、サイコロを使って単語を選択するようになりました。彼らは7,776語のリストを持っています（65なので、5つのサイコロを振って単語を選びます）  
  
最も一般的な操作エラーは、デフォルトのパスワードのリセットに失敗しています。  
特に悪い例は、パッチを適用できないソフトウェアによってチェックされ、変更できないデフォルトのパスワードがシステムにある場合です。  
第2章で説明したように、Miraiボットネットは、それらを採用して悪用するために出現しました。  
初期の有名なケースはR vゴールドとシフリーンで、ブリティッシュテレコムが運営する初期のパブリックメールサービスであるプレステルの開発バージョンの電話番号が展示会の端末に貼られたメモで見られました。彼らは、この3年間の大学の監査人が3年間続けて年次報告書に書き込んだパスワードの変更を毎月実施する必要があることを試みましたが、これを裏付ける証拠を提供することはできず、彼らのポリシーが最終的にNISTからのものであることさえ知りませんでした。  
4NIST SP 800-63-3もライブシステムで動作しました。彼らはエディンバラ公の電子メールアカウントに侵入し、「彼」から嫌いな人にメールを送り、騎士団の賞を発表しました。  
3番目の運用上の問題は、このセクションの冒頭で説明したように、パスワードが本当に必要ない場合、または不正な理由でパスワードが必要な場合に、パスワードを要求することです。  
したがって、パスワードフィールドに「123456」を入力することで、あからさまな言葉を入力することで、そのサイトに再度アクセスすることを決して計画しないユーザーにとっては、まったく合理的です。  
しかし、おそらく最大の運用上の問題は、ソーシャルエンジニアリング攻撃に対する脆弱性です。  
3.4.4.5ソーシャルエンジニアリング攻撃  
たとえば、NSAには色の異なる内線電話と外線電話があり、部屋の外付け電話がオフフックになっていると、分類された資料を部屋で話し合うことすらできず、電話では話せません。  
フィッシングは蔓延しているため、メールのリンクをクリックして銀行にログオンするのは賢明ではないため、常にブラウザのブックマークを使用するか、URLを手動で入力する必要があります。  
実際、マーケティング業界の多くは、人々にリンクをクリックしてもらうことに専念しています。  
銀行の顧客は、間違ったことを行うようによく訓練されています。  
Bank of Americaからのスパムにより、英国の顧客がmynew-card.comに誘導され、証明書が間違っていました（mynewcard.bankofamerica.comに対するものでした）。  
ドメイン名を無視し、証明書の警告を無視し、リンクを陽気にクリックする[582]ことにより、安全ではないコンピューティングを実践するように顧客をトレーニングしている大手銀行の例は他にもたくさんあります。  
身元不明の発信者に電話でセキュリティ情報を提供することは賢明ではありませんが、セキュリティ情報を要求する銀行のスタッフから全員に電話がかかります。  
（運転中に銀行のセキュリティチームから電話があったため、カードがブロックされました。ハンズフリーモード以外での通話の処理は法律に違反し、安全な場所はありませんでした。）  
 店で;また、シティバンクは、PINやアカウントの詳細などの個人情報を要求する電子メールを無視して報告するように顧客に要求しています。  
 お察しのとおり、オーストラリアの顧客に「セキュリティアップグレードの一環として」ウェブサイトにログオンし、カード番号とATM PIN [1087]を使用して認証するよう依頼するメールを送信しました。  
次に、学生はISPに連絡して不正行為を報告し、URLとサービスが本物であることがわかりました[1241]。  
。  
3.4.4.6顧客教育  
これは、一部はリスクの軽減ですが、一部はリスクのダンピングです。説明を理解していない、または指示に従えない顧客は、結果として生じた損失の責任を負う可能性があることに注意してください。  
当初、アドバイスは「英語をチェックする」でしたので、悪意のある人は英語を書くことができる誰かを手に入れるか、単に銀行の独自の電子メールを使い始めましたが、URLは変更されました。  
。  
。  
そのときのアドバイスは、リンクの上にマウスを置いて、リンクが実際にどこに行くかを確認することでした。次に、悪意のある人物がURLに非印刷文字を挿入してInternet Explorerに残りの文字を表示しないようにするか、（多くの銀行もそうであるように）管理できないほど長いURLを使用しました  
この種の軍拡競争は、攻撃者に利益をもたらす可能性が最も高いです。  
安全性とユーザビリティのコミュニティは、「非難と訓練」が使用できないシステムに対処する方法ではないことを長年にわたって認識してきました。唯一の真の修正は、そもそも安全なユーザビリティを設計することです[1451]。  
3.4.4.7フィッシング警告  
最新のブラウザーは、内部でさまざまなメカニズムを使用して、邪魔なURLに警告します。  
第二に、期限切れの証明書やその他のコンプライアンスの失敗を探すためのロジックがあります（これらのアラートの大部分は誤警報であるため）  
警告に注意を向けさせる方法について、産業界と学界の両方で多くの研究が行われてきました。  
では、人々はいつ注意を払うのでしょうか？ただし、具体的かつ具体的です（「これからアクセスしようとしているサイトには、目に見える利益をもたらすことなく、重大なリスクをもたらすソフトウェアが含まれていることが確認されています。  
 [1327]。  
、テキストの簡略化（これは役立ちます）  
。  
ただし、大多数の人が既知の不正なURLをクリックするのを止めたい場合は、自主的なコンプライアンスでは不十分です。  
。  
3.4.5システムの問題  
一部には、いくつかのより広範なシステムの問題とともに、パスワードの入力と保存に関連する技術的なメカニズムが含まれます。  
推測が制限されている場合（ATM PINの場合など）、セキュリティエンジニアはパスワードシステムを「オンライン」と呼ぶことがあります。  
。  
一部のオンラインシステムではできませんが、物理的な改ざん防止を使用してPINの推測を3つに制限する支払いカードなど、一部のオフラインシステムは推測を制限できます。  
ここで最も一般的なトラップは、通常はパスワードの推測を制限するシステムですが、ハッキングされて一方向の暗号化されたパスワードファイルが暗号化キーと一緒に漏洩すると、突然それを失敗します。  
パスワードの推測可能性は、最終的には選択したパスワードのエントロピーと許可される推測の数に依存しますが、これは特定の脅威モデルのコンテキストで機能するため、防御しようとしている攻撃のタイプを考慮する必要があります。  
1つのアカウントに対する標的型攻撃：侵入者は特定のユーザーのパスワードを推測しようとします。  
特定のターゲットに属するアカウントへの侵入を試みます。敵は、所有しているアカウントをどこからでもハッキングし、他のアカウントを乗っ取ったり、直接害を及ぼす可能性のある情報を入手しようとします。  
これは、フィッシング詐欺師が標的の銀行の口座をハッキングして、盗まれたお金をそれを介して洗い流す典型的な例です。  
例としては、侵害されたアカウントからスパムを送信できるようにオンライン電子メールサービスのパスワードを推測しようとする悪者や、標的となる企業のドメイン内の任意のランダムなマシンにビーチヘッドとしてログオンしたい標的型攻撃者があります。  
サービス拒否攻撃：攻撃者は、1人以上の正当なユーザーがシステムを使用するのをブロックしたい場合があります。  
この分類法は、パスワードシステムを評価するときに関連する質問をするのに役立ちます。  
3.4.6サービスを拒否できますか？  
銀行は、3つの間違ったPINの後でカードを凍結することがあります。しかし、不正なパスワードを3回入力した後でオンラインアカウントがフリーズした場合、サービス拒否攻撃を受けます。  
現在、多くの商用Webサイトでは、ロックアウトではなくスロットルを使用しています。  
この場合、保護的な監視が推奨されるオプションとなる可能性があり、危機的状況にある場合はレート制限を放棄する計画があります。  
彼らは、人気のある成長している有能なサイトは、支払いサイトと同様に、より安全である傾向があることを発見しましたが、コンテンツサイトは最悪です。  
、弱いパスワードを選択したユーザーを保護する際により積極的になり、同じ間違ったパスワードを繰り返し送信するIPまたはクライアントを罰しない[1888]。  
3.4.7自分自身または他者を保護しますか？  
 携帯電話システムや現金自動預け払いシステムなど、誰でもアカウントを取得できるグローバルシステムでは、攻撃者がすでに正当なユーザーであると想定し、だれかが他人の費用でサービスを利用できないようにする必要があります。  
これには、個人的な側面とシステム的な側面の両方があります。  
システム側には、サブシステム間の相互認証に使用されるあらゆる種類のパスワード、サーバー/サーバー環境でパスワード品質を実施するメカニズムがほとんどないこと、および多くの既知の問題（たとえば、Javaの信頼できるキーストアのデフォルトのパスワード）があります。ファイルは「changeit」です）  
開発チームは多くの場合、実際のシステムで最終的に使用されるパスワードを共有します。この慣行がセクション3.4.4.4で説明されているエジンバラ公の電子メールの広く知られているハッキングにつながった後でも30年です。  
しかし、これには実際のお金がかかり、お金だけが問題ではありません。  
その結果、サーバーのパスワードはスクリプトやその他のプレーンテキストファイルに表示されることが多く、最終的にDropboxやSplunkに保存される可能性があります。  
後の章では、Kerberosやsshなどのプロトコルについて見ていきます。とりあえず、典型的な大企業をハックするのは簡単だったというエドスノーデンの発言を思い出してください。システム管理者をスピアフィッシングして、あなたの道に鎖でつないでください。多くの場合、パスワード入力は十分に保護されていません。  
3.4.8.1インターフェース設計  
現金自動支払機のいくつかの一般的な種類には、頭の高さに縦型キーボードがあり、ハンドバッグから財布を持ち上げる前に、女性がPINに入るのをピックポケットで簡単に確認できます。  
公共の場所でカード番号またはPINを入力するとき、私は通常、タイピングする手を私の体または私のもう一方の手で覆いますが、すべての顧客がそうすることはできません。  
英国の銀行は、ユーザーの20％がPINを決してシールドしないことを発見し[127]、これを使用して、より良いPIN入力デバイスを設計するのではなく、オーバーヘッドのCCTVカメラによってPINが侵害された顧客を非難しました。  
3.4.8.2高信頼パスと偽のターミナル  
偽の端末攻撃は、時分割コンピューティングの黎明期にまでさかのぼります。  
疑いを持たないユーザーがこれを行った場合、パスワードを保存し、「申し訳ありませんが、間違ったパスワード」と返信してから消え、正規のパスワードプログラムを呼び出します。  
これが、Windowsに安全な注意シーケンスがあった理由です。 ctrl-alt-delを押すと、本物のパスワードプロンプトが表示されることが保証されていました。  
ATMスキマーは、ATMの喉に座ってカードの詳細をコピーし、顧客のPINを記録するカメラを備えたデバイスです。  
詐欺師は不正なPIN入力デバイスも配備し、銀行の支店の端末にパスワードを盗むハードウェアを取り付けたとしても投獄されています。  
いずれの場合でも、端末に悪意のあるハードウェアまたはソフトウェアが含まれている可能性がある場合、パスワードだけでは十分ではありません。  
3.4.8.3パスワード再試行カウンターの技術的な敗北  
同じ考えが多くのコンピュータシステムに対して有効でした。  
これにより、タイミング攻撃が開始されました。攻撃者は、推測したパスワードを適切な場所のメモリに繰り返し配置し、ファイルアクセスリクエストの一部として検証し、拒否されるまでの時間を確認します[1129]。  
したがって、次々に文字を推測することができ、平均してAN / 2の推測をするA文字のアルファベットからN文字のパスワードを抽出する代わりに、AN / 2がかかりました。  
 組み込みシステムの世界では、これらの同じ間違いが何度も繰り返されています。  
一部のスマートカードでは、可能な各入力値を試し、カードの電力消費量を調べ、入力が間違っている場合はリセットを発行することにより、顧客のPINを特定することが可能でした。  
これらの実装の詳細は重要です。  
最近の注目度の高い問題は、iPhoneのPIN再試行カウンターでした。  
これにより、彼は、Appleが課した10のPIN制限ではなく、10,000の可能なすべてのPINを試すことができました[1777] 5。  
3.4.9パスワード保存に対する攻撃  
MITの1960年代のマルチックの前身である「互換性のあるタイムシェアリングシステム」では、ある人がその日のメッセージを編集し、別の人がパスワードファイルを編集していたことがありました。  
別の恐ろしいプログラミングエラーが1980年代後半に英国の銀行を襲い、誤って同じPINをすべての顧客に発行しました[54]。  
大きな失敗が続いています：2019年に、BistarとAEOS生体認証ロックシステムを使用して、企業の管理を構築し、83か国の銀行や警察などの顧客が100万人以上のIDと平文のパスワードを使用してデータベースをオンラインで保護せずに放置しました。指紋と顔認識データ;これをインターネットスキャンから発見したセキュリティ研究者は、自分自身をユーザーとして追加することができました[1864]。  
監査は別の危険をもたらします。  
ログが十分に保護されていない場合、存在しないユーザー名e5gv \* 8ypで失敗したログインの監査レコードを見る人は、すべての有効なユーザー名のパスワードとしてこれを試す必要があります。  
3.4.9.1一方向暗号化  
パスワードは、入力されると一方向の関数を介して渡され、ユーザーは以前に保存された値と一致する場合にのみログオンします。  
これを行う正しい方法は、これまでこのコンテキストでソルトとして知られているランダムキーを生成することです。低速で暗号学的に強力な一方向関数を使用して、パスワードをソルトと組み合わせます。ソルトとハッシュの両方を保存します。  
3.4.9.2パスワードクラッキング  
UNIXが主な例でした–パスワードファイル/ etc / passwdはすべてのユーザーが読み取ることができました。  
3.4.4.1で、この目的のために人々が長年使用してきた「クラック」ソフトウェアについてはすでに触れました。ただし、たとえば、忘れたパスワードを使用してOfficeドキュメントを暗号化した場合に役立つパスワード回復ツールはまだあります[1674]。  
資格情報の詰め物もあります。システムがハッキングされ、パスワードが解読された（または暗号化されていないことが判明した）場合  
これは未解決の問題のままです。  
検討する価値のある対策の1つは欺瞞です。これはスタックのすべてのレベルで機能します。  
  
多くのシステムはパスワードをリモートでチェックし、暗号化プロトコルを使用して転送中のパスワードを保護します。パスワードのセキュリティとネットワークのセキュリティの相互作用は複雑になる場合があります。  
これについては、次の章のセクション4.7.4で説明します。暗号化されたトラフィックを盗聴できる相手から弱いパスワードを常に保護するわけではありません。  
サーバーがハッキングされた場合、TLSはユーザーを保護しません。  
 これは、パスワードが推測可能な場所でも安全なセッションをセットアップするように設計されており、WiFi認証のWPA3標準で2018年から採用されています。  
さらに、アクセスの委任を可能にするプロトコルであるOAuthがあります。これにより、あるWebサイトに、別のWebサイトが提供するメカニズムを使用して認証する権利を付与できます。  
メカニズムについても後で説明します。  
 地方の人権擁護家をフィッシングするために、OAuthが作家主義諸国の国家関係者によって使用されているのを目にしています。  
 そして、Microsoftからのアクセスを求めるメールを送信します。  
3.4.10絶対制限パスワードを保護する暗号化アルゴリズムとオペレーティングシステムのセキュリティメカニズムに自信がある場合、パスワードが一元的に割り当てられている場合、パスワード推測攻撃が成功する確率は、パスワードのエントロピーの関数です。ユーザーが選択を許可されている場合のユーザーの心理。  
たとえば、Lがパスワードの最大有効期間、Rがログイン試行率、Sがパスワードスペースのサイズの場合、パスワードが有効期間内に推測される確率は、P = LR / Sです。米国国防総省のパスワード管理ガイドライン[546]。  
ターゲットアカウントをクラックしたいですか、それとも任意のアカウントをクラックしたいですか？  
これを止めたい場合は、すべてのアカウントだけでなく、すべてのアカウントに対してレート制御を行う必要があります。  
CVCNCVCNなどの、子音、母音、数字を覚えやすくするために設計された固定テンプレートを使用してランダムに選択されたパスワードを発行するために使用されていた英国政府のシステム（例：  
。  
したがって、攻撃者が1秒あたり100個のパスワードを推測できる場合、おそらくネットワーク上の何百ものマシンにある10,000アカウントに分散されているため、アラームが発生しないようにするには、侵入に約500万秒（2か月）必要です。  
失敗したログオンの試行をカウントして分析することもできます。ボットネットを使用した攻撃者やその他の侵入の試みを示唆する一連の推測はありますか？  
 システムを終了しますか？  
商用Webサイトでは、ユーザーパスワードの選択が適切でないため、1秒あたり100個のパスワードが1秒あたり1つの侵害されたユーザーアカウントに変換される可能性があります。  
少数のIPアドレスからのものである場合はブロックできますが、上記のセクション3.4.6で説明したように、これを適切に行うことは見かけよりも困難です。  
3.4.11パスワードマネージャの使用1980年代以降、企業は複数のアプリケーションのパスワードを記憶するシングルサインオンシステムを販売してきました。1990年代半ばにブラウザが登場し、人々が数十のWebサイトにログインし始めたとき、パスワードマネージャーは大衆市場の製品になりました。  
ランダムなパスワードを選択し、ブラウザにそれらを記憶させることは、実用的な操作方法になる場合があります。  
 または同じホスト名とフィールド名（Firefox）  
ブラウザーでは、マスターパスワードを設定できます。マスターパスワードは、個々のサイトのすべてのパスワードを暗号化し、ブラウザーの更新時にのみ入力する必要があります。  
これはブラウザを使用する場合の特定の問題であり、もう1つは、マスターパスワードが常にデフォルトではないため、多くのユーザーが設定しない場合があることです。  
 ブラウザを使用する利点は、携帯電話のブラウザとラップトップのブラウザの間でパスワードを同期できる可能性があることです。  
（ブラウザーを使用する場合、これはラップトップまたは電話全体をバックアップすることになります。）欠点は、多くの製品が本当に恐ろしいことであり、一部のハードウェアパスワードマネージャーでもすべての秘密がクリアに保存されている[130]一方で、上位5つのソフトウェア製品は、オートコンプリートからサブドメインを無視するなど、深刻でシステム上の脆弱性に苦しんでいる[389] 。  
 多くの銀行は、Webページでautocomplete = "off"を設定するか、パスワードマネージャーをブロックする他のトリックを使用して、ストレージを無効にしようとします。  
パスワードマネージャーまたはブラウザの独自のストレージを使用しているユーザーを停止すると、ほとんどのユーザーは脆弱なパスワードを使用するようになります。  
また、不便です。顧客からの反応があったため、パスワードの保存を突然無効にした銀行の1つが翌日に取り下げられました[1278]。  
私は個人的に、さまざまな目的でさまざまなブラウザーを使用し、それらに価値の低いパスワードを保存させています。メールやバンキングなどの重要なアカウントの場合、私は常にパスワードを手動で入力し、リンクをクリックするのではなくブックマークを使用して常にそれらに移動します。  
また、バックアップとリカバリについて十分に検討し、実際に機能することを確認してください。  
 あなたの電話が死んだとき？  
 あなたが死んだとき、またはあなたが病気になり、あなたのパートナーがあなたのものを管理する必要があるとき？  
 本にそれらを書き留めることは、もしあなたすべて（そしてあなたの執行者）ならば、理にかなっています。  
これをすべて正しく行う人はほとんどいません。  
 パスワードは煩わしいので、多くの人がパスワードを取り除くことについて話し合っており、ラップトップから電話に移行することでチャンスが生まれます。  
一握りの企業がそれらを完全に取り除こうとしました。  
指紋、パターンロック、PIN、またはパスワードを使用して電話を保護するかどうかは、顧客に任せます。  
パスワードではなくSMSを使用して認証する最も人気のあるアプリはWhatsAppかもしれません。  
そのような場合、回復はメールループを意味し、メールパスワードをこれまでになく重要なものにします-またはコールセンターに電話して母親の旧姓を伝えます。  
Joe Bonneauと同僚は、2012年にオプションを分析しました[292]。  
その他の要因には、使いやすさ、学習のしやすさ、余分なものを運ぶ必要があるかどうか、エラー率、回復のしやすさ、ユーザーあたりのコスト、誰でも使用できるオープンなデザインかどうかなどがあります。  
さらに、セキュリティの改善には、パスワードの利点の1つ以上を放棄することが含まれます。つまり、パスワードは簡単で効率的で安価です。  
銀行カードに関連付けられたものを使用すると、少なくとも従来のハイストリート銀行では、より伝統的な信頼のルートが得られます。顧客は支店に行き、新しいカードを注文できます7。  
調査で何か見落としはありましたか？  
3番目のオプションであるバイオメトリクスは、ハイエンドの携帯電話が指紋リーダーを提供し始めて以来、広く使用され始めています。  
バイオメトリクスについては、本の後半の独自の章で説明します。  
したがって、パスワードは（不安定な）ままです  
これを変更する可能性があるのは、ユーザーインターフェイスがまったくないため、他のメカニズムを使用して認証する必要があるデバイスの数の増加です。  
これについては、次の章で説明します。また、車両のセキュリティなどの特定のアプリケーションについても説明します。  
2019年、ジェームズパヴールは150件のそのようなリクエストを会社に送り、彼の親友になりすました[1886]。  
身元保証における政府の役割を定着させる試みには多くの問題がありました。これについては、バイオメトリクスに関する章でさらに説明し、オンラインサービスから選挙のセキュリティに至る問題に波及しています。  
しかし、2019年にAppleは、よりプライバシーに配慮した新しいシングルサインオンメカニズムを提供し、アプリストアの市場力を利用してWebサイトに強制的にサポートさせることを発表しました。  
これについては、経済学の章でさらに詳しく分析します。  
彼女についての情報であり、多くは彼女を認証するために彼女のログオンとパスワードを要求する感覚を持っていました。  
彼は、彼女のクレジットカード番号、社会保障番号、母親の旧姓など、彼女に関する完全な個人情報を収集しました。  
30日以内にそのような要求に応じない場合、企業はEUで大きな問題に直面することを考えると、法律事務所のアシスタントに任せて即興で処理するのではなく、事前にそれらに対処する方法を考えたほうがよいでしょう。手順。また、顧客になったことがない人の個人データを保持している場合、どのようにしてそれらを特定しますか？  
3.5 CAPTCHA  
 この分野で最も成功したイノベーションは、CAPTCHA、つまり「コンピュータと人間を区別するための完全に自動化されたパブリックチューリングテスト」でしょう。  
人々がそのような問題を簡単に解決できる一方で、コンピュータがそれらを見つけるのは難しいという考え方です。  
それらは、コンピューターがインテリジェントであるかどうかについてアランチューリングによって提唱された有名なテストに触発されたルイスフォンアンおよび同僚[1969]によって発明されました。ある部屋にコンピューターを置き、別の部屋に人間を置き、人間をそれらを区別してみてください。  
初期のバージョンでは、ノイズのある背景に対する歪んだテキストの認識など、AIの既知の「難しい問題」を使用するようになりました。  
人間は歪んだテキストを読むのが得意でしたが、プログラムはそれほど良くありませんでした。  
CAPTCHAに対する攻撃の多くは、今日まで、実装の詳細を悪用しています。  
プロトコルレベルの攻撃もあります。フォン・アンは、理論的にはスパマーが無料ポルノへのアクセスの代償として人々にそれらを解決させることができると述べた[1968]。  
数年のうちに、CAPTCHAを破壊する商用ツールが市場に登場するようになりました[843]。  
そして、地下市場における安全保障経済学の研究は、2011年までに行動は人間を使用することに移ったことを示しました。 1日に数ドルの収入がある国の人々は、CAPTCHAを1000あたり約50セントで解決します。  
ここでのアイデアは、いくつかのユーザーにいくつかの有用な作業を行わせ、それらの回答を相互にチェックすることです。  
それは、迅速な応答を可能にするのではなく、2つまたは3つの多肢選択パズルを配置し、その上に数十秒かかることによって、安価な労働力攻撃を押し戻します。  
また、ポルトガル語がよく分からないので、何を探しているのかを理解できない場合は、ウェブサイトに画像付きのオブジェクトを表示するよう画像を表示するポルトガル語の通行料を支払ってみてください。  
詐欺と使いやすさのため、心理学はセキュリティエンジニアにとって重要です。  
さまざまな種類のフィッシングは、国家安全保障の主要な脅威であり、サイバー犯罪インフラストラクチャを開発および維持するための主要な手段であり、オンラインバンキングシステムに対する主要な脅威の1つです。  
救済策の一部はセキュリティの使いやすさですが、この分野の研究は長い間無視されており、暗号化やオペレーティングシステムほど魅力的ではないと見なされていました。  
2010年代半ば以降、私たちは一般のプログラマーにとっても物事を容易にする必要があることにも気づき始めました。実際のシステムを破壊したセキュリティバグの多くは、安全でないデフォルトを使用する暗号化APIからCプログラミング言語まで、使用するのが難しすぎるツールの結果です。  
この章では、詐欺や人々が犯す種類のエラーに関連する心理学の調査を通して、ホイッスルストップツアーを行い、ケーススタディとして認証に取り組みました。  
私たちは、ReCAPTCHAが「ヘリコプターを含むすべての画像をクリックしてください」と言っており、軍事AIの研究に協力したくないというユーザーからの反発がありました。  
しかし、他のユーザーはまだ無料でGoogleで働くことに反対しています。  
推測可能性、記憶可能性、ユーザーのトレーニング可能性など、ラボで測定できるものだけでなく、実際のシステムがどのように破壊されるか、実際の攻撃がどのようにスケーリングされるかなど、フィールドでのみ観察できる要素に関するデータが増えていますさまざまなプレイヤーが直面しているインセンティブがどのように危険な均衡をもたらすか。  
「人々はテロにあまりにも多くの注意を払っており、サイバー犯罪には十分ではないことに同意します」と彼は言った。  
空港でもっとリラックスしてもらいたい場合は、戦車と銃を取り除き、スピーカーに素敵なソファとモーツァルトを入れれば、人々はすぐにリラックスできます。  
しかし、コンピューター業界は、コンピューターを以前ほど恐ろしくなくするために道をはずしているので、それは起こりません。」そしてもちろん、政府は警察の予算を引き上げ、政治家の再選を助けるため、人々がテロを心配することを望んでいます。  
心理学、経済学、工学の要求間の多くの緊張を理解することは、地球規模で堅牢なシステムを構築するために不可欠です。この本の第2版では、2001年の第1版以来、安全保障経済学の分野全体が活気づいていることを指摘し、「心理学と安全保障の関係について、より根本的な考え方も必要です」と書きました。  
研究トピックを見つけるための私のメタアルゴリズムは、最初にアプリケーションを調べ、次に隣接する分野を調べることです。  
 2番目の例、およびセキュリティと人間行動に関するワークショップのテーマは、人類学や心理学から社会学、歴史や哲学に至るまで、人々がリスクに対処する方法を研究する学問から学べるものです。  
パンデミックは、建築家と協力する必要があるかもしれないことを示唆しています。  
コードをハッキングするだけでなく、設計する必要があります。  
一方、ソーシャルエンジニアリングに関する最良の本は、依然としてケビンミトニックの「詐欺の芸術」[1325]です。  
マーケティングで社会心理学がどのように使用され、悪用されるかについて、必読の本はTim Wuの「The Attention Merchants」であり、広告の歴史を物語っています[2050]。  
次に、[1544]のような標準のHCIテキストがありますが、セキュリティの使いやすさに関する初期の論文は[493]と表示され、フィッシングについては[976]と表示されました。  
自動運転車に関する同様の調査によると、人格が与えられた場合、人々はそのような車をより信頼し、乗客はルートを選択したり、単に車を停止するように命令するなどの戦略的制御を与えられます。  
より技術的な詳細については、ダニーがトムギロビッチとデイルグリフィンによってその直前に編集された大量の論文[769]、または彼が後に書いたポップサイエンスブック「Thinking、Fast and Slow」[1005]があります。  
この理論を政府や他の場所に適用する場合、標準的な参照はディックターラーとキャスサンスタインの「ナッジ」[1876]です。  
パスワードと関連するメカニズムの詳細な履歴、および多くの経験的結果と推測可能性と再現率の両方を測定するための統計的手法の分析については、ジョーボンノーの論文[289]を強くお勧めします。上記。  
拷問者の聖書として知られ、囚人を尋問し、洗脳するときの感覚剥奪、薬物、催眠、社会的圧力などの相対的な有効性を説明しています。