

## Wydobywanie

Być może najważniejszą umiejętnością w całym ataku inżynierii społecznej jest prowadzenie celów do punktu, w którym są one otwarte do wykorzystania. Wydobywanie na jaw jest potężną techniką stosowaną w kluczowych etapach ataku inżynierii społecznej, aby cele przyjęły ścieżkę zachowania pożądaną przez inżyniera społecznego. Interesującą definicją wydobywania amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA) jest to, że jest to subtelne pozyskiwanie informacji podczas normalnej rozmowy. Wydobywanie jest jedną z umiejętności, których nauczyli się szpiegowie, aby upewnić się, że potrafią wydobywać informacje z ludzi, nie sprawiając wrażenia, jakby byli szpiegowani. Rozmowy mogą odbywać się niemal wszędzie, a inżynierowie społeczni lubią zbliżać się do celów w miejscach, które znają (celom), a zatem czują się swobodnie już podczas rozmowy z nowymi ludźmi. Ludzie będą chcieli pozostać w strefie bezpieczeństwa, dlatego niektóre pytania wzbudzą podejrzenia. Jednak po fachowym wymyśleniu i zapytaniu respondent wyrzuci niektóre informacje, które w innym przypadku zostałyby ukryte. Omówimy, w jaki sposób inżynierowie społeczni określają swoje cele i zachęcają ich do działania lub reagowania w określony sposób, gdy są bardziej podatni na wykorzystywanie lub spełniają nietypowe prośby. Ważne jest, aby nauczyć się komunikować w bezpieczny sposób, aby uniknąć bycia ofiarą pobudzenia. Omówimy następujące tematy:

- \* Rozmowy z nieznanymi
- \* Wstępne ładowanie
- \* Jak skutecznie przeprowadzić pozyskiwanie?
- \* Opanowanie umiejętności pozyskiwania

## Wprowadzenie

Wywoływanie to jedna z dobrze ukrytych technik inżynierii społecznej o niskim ryzyku, która ma imponujące wyniki. Istnieje kilka czynników, które sprawiają, że wzbudzenie jest wyjątkowo skuteczne, które z czasem zostały uwikłane w ludzi. Są to:

- \*Pragnienie wielu osób uprzejmości wobec nieznanymi
- \*Pragnienie profesjonalistów, aby wyglądać na kompetentnych, gdy są pytani
- \*Pragnienie większości ludzi, aby nie okłamywać ludzi, którzy wydają się być naprawdę zaniepokojeni
- \*Gotowość wielu ludzi do odpowiedzi na dobrze postawione pytania o siebie

Weź przykład z życia, w którym niektóre z tych czynników odgrywają rolę w normalnych rozmowach i jak inżynier społeczny może z nich skorzystać. Powiedzmy, że odbywa się impreza firmowa, podczas której ludzie mogą wchodzić w interakcje z kluczowymi członkami personelu w organizacji. Inżynier społeczny może udać się do dyrektora finansowego (CFO) i twierdzić, że jest szefem bezpieczeństwa w mało znanej firmie. Mógł zainicjować krótką rozmowę na podstawie zarobków organizacji dyrektora finansowego i perspektyw firmy na przyszłość. Oczywiście dyrektor finansowy otworzy się i udostępni informacje na ten temat. W części atakującej inżynier społeczny może twierdzić, że szuka systemu bezpieczeństwa do drzwi i zapytać dyrektora finansowego, czy ma wiedzę na temat tego, z którego korzysta ich firma. Aby wyglądać na poinformowanego, dyrektor finansowy poinformuje inżyniera społecznego o systemie, który jest obecnie w użyciu. Z tego małego czatu inżynier społeczny dowie się więcej o wewnętrznych systemach bezpieczeństwa używanych przez tę organizację. Nie jest to gwarancja, że ta metoda zawsze będzie działać, ale omawiane czynniki są zwykle obecne u większości ludzi, a zatem są szybkim sposobem na uzyskanie poufnych informacji. Poniższy obraz przedstawia

dwie twarze inżynierii społecznej: Informacje zebrane w omawianej rozmowie, które dotyczyły pozyskiwania informacji o systemach bezpieczeństwa używanych przez pewną organizację, mogą zostać wykorzystane do przeprowadzenia późniejszego ataku. Inżynier społeczny może pojawić się w organizacji pod pretekstem mechanika wysłanego do naprawy wadliwego systemu bezpieczeństwa. Informacje dotyczące systemów bezpieczeństwa stosowanych w organizacji zostaną już ujawnione przez CFO, a zatem będą dokładne, a ochroniarze i recepcjoniści pozwolą inżynierowi socjalnemu wykonać jego naprawę. Gdyby inżynier społeczny skontaktował się z innymi pracownikami organizacji podczas spotkania i zebrał więcej informacji na temat organizacji, mógłby przeprowadzić atak na dużą skalę. Wywoływanie nie ogranicza się do gromadzenia informacji. Służy również do utrwalania pretekstu i uzyskiwania dostępu do dodatkowych informacji. Rzućmy okiem na niektóre cele pozyskiwania.

### **Rozmowy z nieznanymi**

W każdym ataku inżynierii społecznej inżynier społeczny chce, aby cel podjął działanie i albo coś powiedział, albo coś zrobił. Może to być tak niewiele, jak udzielenie odpowiedzi na niektóre pytania lub tak samo, jak oprowadzenie inżyniera społecznego po ograniczonym obszarze w organizacji. Wydobywanie odbywa się poprzez proste rozmowy z ludźmi. Codziennie odbywają się małe rozmowy między nieznanymi, dlatego ludzie nie są tak bardzo zaniepokojeni, gdy nieznanymi podchodzą do nich i angażują się w krótką rozmowę. Może znajdować się w kolejce w sklepie, przy stole w restauracji lub podczas imprezy. Istnieje duża szansa na zainicjowanie rozmowy z celem, jeśli wcześniej przeprowadzono na nim badania w celu znalezienia miejsc, które często odwiedzają i rzeczy, które lubią robić w takich miejscach. Istnieją trzy kroki do rozpoczęcia udanej małej rozmowy z nieznanymi. Są to:

Bycie naturalnym: Cel zabije rozmowę, jeśli osoba, która spróbuje ją utrzymać, wygląda na niewygodnego i nienaturalnego. Dlatego inżynier społeczny musi zawsze komunikować się poprzez postawę i inne niewerbalne sygnały zaufania i naturalności. Ponadto inżynier społeczny powinien inicjować rozmowy, o których ma pewną wiedzę. Nic nie wzbudza braku pewności szybciej niż brak rzeczy do powiedzenia celowi. To prowadzi nas do drugiego kroku.

Wiedza: Inżynier społeczny musi mieć wiedzę na temat rzeczy, z którymi zamierza rozpocząć rozmowę. W poprzednim przykładzie rozmowy z dyrektorem finansowym firmy inżynier społeczny rozpoczął rozmowę od wzmianki o sytuacji finansowej firmy. Musiał mieć czas, aby przejrzeć liczby, a tym samym mieć coś, co wzbudza zainteresowanie dyrektora finansowego podczas inicjowania rozmowy. Dzięki tej wiedzy inżynier społeczny miał coś, o czym mógłby śmiało rozmawiać z dyrektorem finansowym. Jeśli jednak niewiele jest informacji, że inżynier społeczny musi rozpocząć rozmowę z dyrektorem finansowym, istnieje możliwość wyboru pretekstu badacza lub dziennikarza.

Bycie hojnym: W poprzednich częściach omawiano kwestię wzajemności, w której gdy ktoś otrzymuje coś, zawsze istnieje potrzeba oddania czegoś. Aby rozpocząć lub utrzymać rozmowę, ważne jest, aby była to sytuacja dawania i przyjmowania. Dzięki takiemu podejściu inżynier społeczny może wnikać głębiej w organizację, udając, że podaje celowi więcej wewnętrznych szczegółów dotyczących jego domniemanej organizacji. Hojność może również przyjąć do gry z punktu widzenia tego, kto dominuje w rozmowie. W poprzednim rozdziale zauważono, że najlepsi rozmówcy to dobrzy słuchacze. Dlatego inżynier społeczny nigdy nie dominuje w rozmowie. On lub ona pozwala celowi mówić więcej i dlatego ujawnia więcej.

Omówione kroki zapewnią, że można rozpocząć i utrzymać zdrową rozmowę. Kroki te są skuteczne nie tylko w atakach inżynierii społecznej, ale także w normalnych rozmowach. Oprócz tych trzech kroków jest energia. Wyraża się to tonem głosu, wyglądem i niewerbalnych wskazówek. Podczas sesji

szkoleniowych nowym właścicielom mówi się, że ich energia wpływa na energię ich psów. Dlatego muszą podchodzić do swoich psów z odpowiednią energią i unikać napięcia i niepokoju. To samo dotyczy inżynierii społecznej. Inżynierowie społeczni zaprezentują się swoim celom z odpowiednią energią w zależności od pretekstu, który wybiorą.

### **Ładowanie wstępne**

Wstępne ładowanie jest techniką, która została szeroko zastosowana w marketingu z ogromnym sukcesem i ma również zastosowanie w inżynierii społecznej. Weźmy przykład kina. Kupując bilety do kina, popcorn i napoje, na wszystkich nadchodzących filmach będą plakaty. Siedząc w sali kinowej, pokazywane są zwiastuny niektórych nadchodzących filmów z narratorem zaczynającym się od słów, takich jak najstraszniejszy film ... lub najbardziej wypełniony akcją film .... Jest to reklama nadchodzącego filmu, który zostanie pokazany w kino i reklama już mówi, jak się czuć i czego się spodziewać. To rodzi w tobie pragnienie obejrzenia filmu. W reklamach restauracyjnych przeważnie będą szczęśliwe osoby, które będą cieszyć się doskonałymi posiłkami z napisami takimi jak pyszne! aby dać ci wyobrażenie o tym, jakie jest jedzenie, zanim jeszcze go spróbujesz. Te dwa przykłady dają wgląd w to, co to jest wstępne ładowanie. Jest to technika ładowania celów z kilkoma pomysłami, jak reagować na pewne rzeczy lub informacje. W ataku socjotechnicznym atakujący wymyśli najpierw cel interakcji z celem. W odpowiedzi będzie to gromadzić pewne informacje. Następnie atakujący wymyśli szereg pytań, aby zadać celowi, a następnie wymyśli sposób na wstępne załadowanie celu, zanim on lub ona odpowie na te pytania.

Aby lepiej zrozumieć wstępne ładowanie w prawdziwym życiu, rzućmy okiem na film o nazwie Focus, który został wydany w 2015 roku z udziałem Willa Smitha. Ikoniczną częścią filmu było to, że Will Smith postawił u hazardzisty Liyuan Tse wszystkie pieniądze, które zarobił (Will). Jeden ze współników Smitha dosłownie oszalał, ponieważ pieniądze, które zarobili, są teraz na granicy zagubienia. Liyun Tse ma wybrać dowolnego gracza na boisku, a jeśli Smith nie zgadnie, który z nich, Smith przegrywa. Tse wybiera gracza noszącego koszulkę z numerem 55, a ponieważ Smith odgadł, że ten gracz wygrywa. Wyjaśniając kobiecie współnikowi, skąd był pewien, że Tse wybierze numer 55, wyjaśnia jej, że ustawili wszystko tak, aby hazardzista był fabrycznie załadowany numerem 55, gdziekolwiek by nie poszedł. Muzyka w tle, światła w kasynie i klauni zostały użyte do wstępnego załadowania numeru do gracza. Dlatego kwestią czasu był wybór zawodnika z koszulką o numerze 55, ponieważ ta liczba była wielokrotnie sadzana w jego nieprzytomnym mózgu. Wstępne ładowanie jest warunkiem wstępnym udanej próby wywołania. Przygotowanie wymaga więcej niż samego procesu wywoływania zadawania dociekliwych pytań celowi. Wstępne ładowanie może być bardzo złożone w zależności od pomysłu, że inżynier społeczny chce wszczepić się w cel. W omawianym filmie Willa Smitha widać, że wiele wysiłku włożono w to, by dać przeciwnikowi wkład 55. Podjęli nawet próbę zmiany muzyki w tle w momencie, gdy Liyun Tse wybierał gracza w terenie. Piosenka w tle była również azjatycka, a jej refren był powtórzeniem numeru 55. Oczywiście jest, że planowanie zajęło trochę czasu, aby wstępnie załadować cel numerem 55. Podobnie inżynier społeczny przejdzie wszystkie kłopoty z posadzeniem wkładu, który sprawia, że decyzja celu jest bardziej przewidywalna. Wstępne ładowanie zajmuje zatem czas i ważne jest, aby inżynier społeczny był cierpliwy. Czasami może to nawet obejmować emocje, a budowanie ich zajmuje trochę czasu.

### **Unikanie wydobywania**

Jest wiele rzeczy, które wchodzi w grę, gdy inżynier społeczny próbuje przeprowadzić wzbudzenie. Istnieje kilka doskonałych taktyk, które można zastosować, aby zapewnić pomyslną próbę wywołania. Obejmują one od zakupu celu trochę alkoholu po pochlebne ich ego. Niektóre z tych taktyk zostaną teraz omówione:

## **Odwolywanie się do ego**

Wiele osób, zwłaszcza na wyższych stanowiskach, lubi głąskać ego. Robi się to, aby odwołać się do celu, ale należy to zrobić ostrożnie, ponieważ możliwe jest również, że cel Cię odetnie, jeśli zostanie przekroczony. Dobrym sposobem na to jest po prostu uznanie podstawowych rzeczy i zachowanie subtelności. Na przykład po prezentacji możesz przejść do jednego z prezydentów i powiedzieć mu, co za miła prezentacja. Przybyłem tutaj, nic o tym nie wiedząc, a teraz czuję się ekspertem. Takie proste pochlebstwo skutecznie rozpoczyna rozmowę z celem, od którego inżynier społeczny może uruchomić próbę wywołania

## **Wykazanie wzajemnego zainteresowania**

Ludzie docenią relację, która wykracza poza początkowe spotkanie i to właśnie tam pojawia się wzajemne zainteresowanie. Nie tylko sprawia, że bieżąca rozmowa jest bardziej interesująca, ale pozwala inżynierowi społecznemu ustawić cel w łatwiejszym miejscu do ataku. Na przykład CSO mógł wspomnieć na dorocznym spotkaniu, że organizacja jest narażona na zwiększone ataki. Po spotkaniu inżynier społeczny może zbliżyć się do starszego pracownika i rozpocząć rozmowę, a następnie w połowie poruszać temat, który ujmuje interesy dyrektora finansowego. Mógł wspomnieć, że jest szefem działu IT w innej organizacji i wdrożył specjalny program w celu ograniczenia problemów związanych z cyberbezpieczeństwem. Inżynier społeczny może zaoferować zainstalowanie wersji demo w organizacji GUS, aby zobaczyć, jak to będzie działać. Spowoduje to zbudowanie wzajemnego zainteresowania między nimi i nie tylko CSO zgodzi się na dalszy kontakt, ale da socjologowi szansę bezpośredniego dostępu do komputerów organizacyjnych. Wspólne zainteresowanie jest korzystne, ponieważ szybko tworzy połączenie między inżynierem społecznym a celem. Jest stosowany głównie, gdy cel ujawnia się, że stoi przed konkretnym wyzwaniem.

## **Oświadczenia fałszujące**

W odpowiedzi inżynier społeczny stara się zdobyć zainteresowanie celu i wszystko, co się dzieje, w tym celowe fałszywe oświadczenia. Po złożeniu fałszywego oświadczenia poinformowana osoba spróbuje skontaktować się z inżynierem społecznym i poprawić go. Osoba poinformowana będzie niewinnie próbować naprawić coś źle powiedzianego przez inżyniera społecznego. W rzeczywistości na wszystkich inżynierów społecznych czekała odpowiedź od celu. Fałszywe stwierdzenia to szybki sposób na wzywanie ludzi do ujawnienia faktów.

Ci, którzy chcą poprawić, zwykle chcą sprawiać wrażenie nietolerancyjnych błędów i lepiej poinformowani. Jest również uwikłane w naturę ludzką, aby poprawić, gdy inna osoba dokonuje nieprawidłowego oświadczenia lub oceny. Po tym, jak cel poprawi fałszywe oświadczenie, inżynier społeczny ma motywację do rozmowy z nim lub nią. Dlatego mógł później zbliżyć się do celu i poprosić o więcej informacji na temat faktów. Chęć bycia poinformowanym sprawi, że cel ujawni inżynierowi społecznemu pewne informacje. Weźmy przykład inżyniera społecznego, który chce dowiedzieć się więcej o systemach bezpieczeństwa w organizacji. Podczas nieformalnego czatu mógł powiedzieć (w obecności pracownika tej organizacji), że organizacja nie ma prawie żadnych systemów bezpieczeństwa i może zostać zaatakowana przez źle myślących ludzi. Pracownik będzie wywierany presją, aby zaprzeczył temu oświadczeniu i powiedział, że firma stosuje jedno z najbardziej wyrafinowanych kontroli bezpieczeństwa fizycznego i oprogramowania. Następnie inżynier społeczny mógł przeprosić za złożenie fałszywego oświadczenia i poprosić o udzielenie dodatkowych informacji na temat zastosowanych systemów bezpieczeństwa. Pracownik pójdzie dalej i wyrzuci szczegóły inżynierowi społecznemu.

## **Pochlebstwa**

Może się to wydawać oczywistą techniką, która może odnieść niewielki sukces, ale w rzeczywistości działa jak urok. Ludzie naturalnie chcą być doceniani za swoje osiągnięcia, ale nie chcą się chwalić sobą, ponieważ na ogół nie należy się tym chwalić. Kiedy cel jest pochlebiony, on lub ona otrzyma komplement, ale czasami próbuje go zlekceważyć. W tym momencie cel jest podatny na ujawnienie niektórych informacji na temat tego, o tym za co on lub ona została pochwalona. Powiedzmy na przykład pracownikowi IT, że jesteś prawdziwym bohaterem w tej firmie, chroniąc taką firmę przed wszystkimi zagrożeniami cybernetycznymi, o których nikt inny nie pozna każdego dnia. Pracownik działu IT przyjmie komplement lub spróbuje go zlekceważyć i jest to odpowiedni moment, aby inżynier społeczny zapytał go o narzędzia, które są używane do ochrony systemów firmy. Gdy wspomniano o narzędziach, inżynier społeczny mógłby podać więcej komplementów na temat zestawu używanych narzędzi. Na przykład inżynier społeczny może powiedzieć „Wow, masz to wszystko”. Czy masz własne serwery, skoro ten zestaw narzędzi sugeruje, że wykonujesz już wodoszczelną pracę, aby rozstawić te duże maszyny? Ten komplement ponownie otworzy pracownika IT, aby mógł więcej mówić o wewnętrznej infrastrukturze obliczeniowej, podając informacje o serwerach przechowywanych w organizacji. Ta informacja jest bardzo przydatna. Inżynier społeczny dowie się, jakie narzędzia bezpieczeństwa zastosowano do ochrony infrastruktury komputerowej celu. Również wewnętrzna wiedza na temat serwerów przechowywanych w organizacji może pomóc w planowaniu kolejnego ataku. Inżynier społeczny może wysłać kogoś, aby pojawił się w siedzibie organizacji, uzbrojony w informacje na temat bezpieczeństwa wewnętrznego i struktury obliczeniowej organizacji. Wysłany agent powinien najlepiej przyjechać w dniu, w którym starszy oficer IT jest na zewnątrz i powiedzieć młodszemu, że został wysłany przez ich wyższego szczebla do naprawy serwera XYZ lub sprawdzenia narzędzia bezpieczeństwa ABC. Wszystkie te informacje umożliwią mu dostęp do serwerowni, w której będzie mógł wykonać złośliwe działania. Wszystko to powstanie z prostego pochlebstwa dla oficera IT.

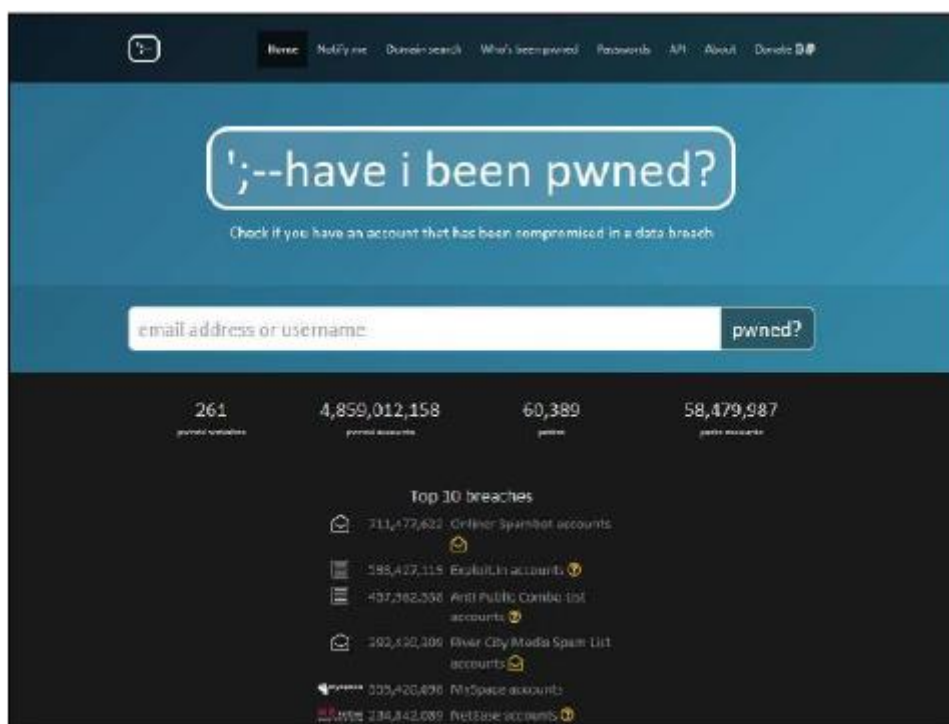
### **Informacje o wolontariacie**

Jest to również podobne do wzajemności, jak omówiono we wcześniejszych częściach. Podsumowując, powiedziano, że gdy inżynier społeczny da celowi coś wartościowego, cel prawdopodobnie zareaguje, oddając coś z powrotem. To samo dotyczy informacji. Cele, po zaoferowaniu pewnych informacji, które wydają się być wartościowe, będą skłonne zwrócić inżynierowi społecznemu własne cenne informacje. Prawie zawsze czują się zobowiązani do oddania czegoś tylko po to, aby być nawet z inżynierem społecznym. Informacje o wolontariacie to często stosowana taktyka, aby wydobyć cele, które w innym przypadku ukrywają niektóre informacje. Dlatego inżynierowie społeczni będą gotowi udzielić pewnych informacji celom, aby nieświadomie zmusić ich do przekazania niektórych informacji w zamian. Istnieje popularne powiedzenie, że nędza kocha towarzystwo. Aby uniknąć wyjścia z kontekstu, możemy luźno zinterpretować to powiedzenie w ten sposób, że ludzie często będą chcieli dzielić podobne opowieści. Dlatego, jeśli inżynier społeczny spotka się z oficerem IT podczas spotkania organizacji, może do niego podejść pod pretekstem innego oficera IT i zacząć mówić o słabościach bezpieczeństwa. Inżynier społeczny może nawet powiedzieć, że zdał sobie sprawę, że dyrektor zarządzający wykorzystuje swoje urodziny jako hasło. Ten schemat myślenia wygeneruje podobne historie od prawowitego informatyka i w krótkim czasie ujawnione zostaną wrażliwe szczegóły dotyczące poświadczeń.

### **Zakładając wiedzę**

Powszechne jest zachowanie, w którym jeśli ktoś ma dużą wiedzę na temat czegoś, dobrze jest nawiązać rozmowę na podstawie tej wiedzy. Dlatego jeśli ktoś może założyć, że posiada wiedzę na temat czegoś, w konsekwencji zaprosi pewną liczbę dociekliwych ludzi na temat tej wiedzy. Powstaną rozmowy, które nie zostaną przeprowadzone, a ludzie, którzy nie wykażą zainteresowania inżynierem społecznym, będą mieli do tego motywację. Gdy ludzie chcą dowiedzieć się więcej, może to być

odpowiedni moment, aby spróbować uzyskać zaproszenia do ich organizacji lub do ich ulubionych restauracji, aby porozmawiać więcej. Gdy spotkanie jest zabezpieczone, można łatwo zastosować inne techniki inżynierii społecznej, ponieważ cel zostanie już zwabiony do punktu, w którym można go wykorzystać. Dobrym sposobem, aby dowiedzieć się, czy twoje hasło zostało skradzione, jest bardzo dobrze znana strona internetowa. Przez większość czasu zgaduję Czy zostałem Pwned? lub znalezienie adresów e-mail nie jest takie trudne. Ponowne użycie hasła jest dość normalne, chociaż nie zalecamy tego jako eksperta ds. bezpieczeństwa. Ponowne użycie hasła jest wygodne, łatwe, a ludzie nie są świadomi potencjalnego wpływu. Jeśli jesteś ciekawy, czy twoje hasło zostało skradzione, możesz to sprawdzić samodzielnie. Witryna <https://haveibeenpwned.com/Passwords> jest dość bezpieczne:



Wykonaj następujące czynności:

Jak widać na poprzednim zrzucie ekranu, wszystko, co musisz zrobić, to wpisać swoją nazwę użytkownika lub adres e-mail,

Jak tylko klikniesz przycisk pwned, zobaczysz następujące wyniki:

Home Mail/VPN/ DNS/ Search Who's been pwned Passwords API About Donate

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

erozkaya@outlook.com **pwned?**

**Oh no — pwned!**  
Print or 3 Breached sites and how to protect (subscribe to search engine Breaches)

**3 Steps to better security** [Get help from us](#)

**Step 1** Protect yourself using Password generators and have strong passwords for each website.

**Step 2** Enable 2 Factor authentication and share the code's code your smartphone app.

**Step 3** Subscribe to notifications for any other breaches, they just change that unique password.

Facebook Twitter YouTube Donate

### Breaches you were pwned in

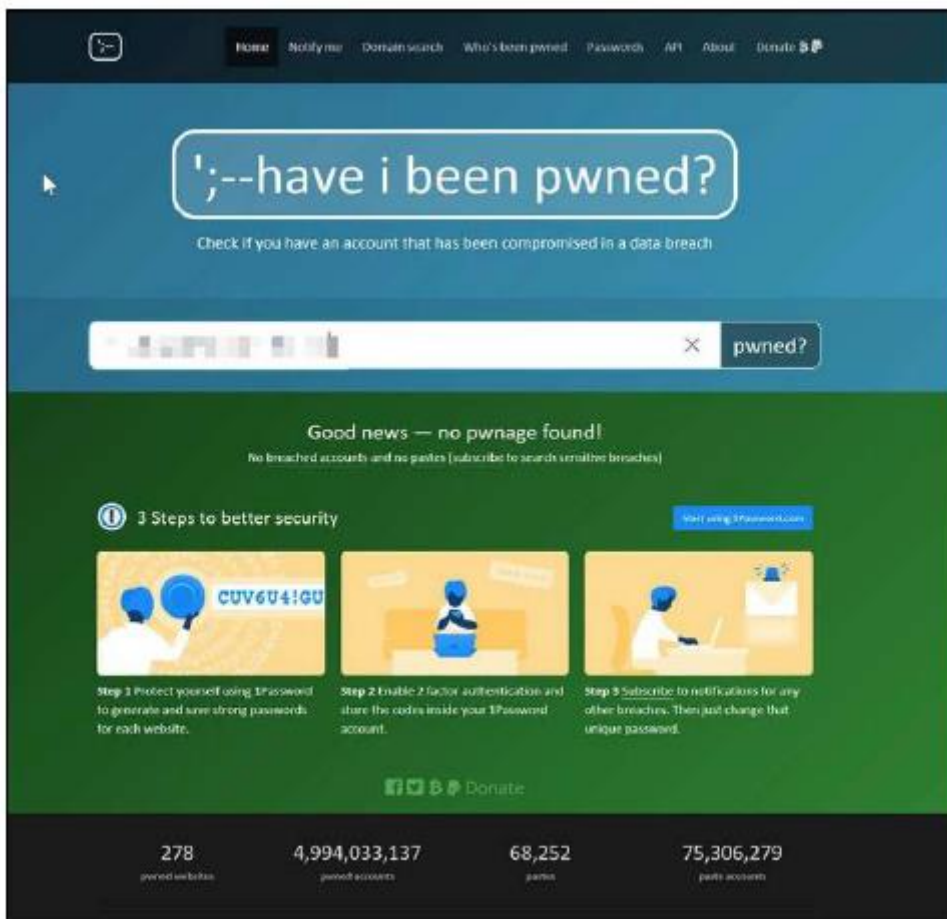
A "breach" is an incident where data has been inadvertently exposed to the public. Using the Password password manager helps you ensure all your passwords are strong and unique each that a breach of one service doesn't put your other services at risk.

**LinkedIn** LinkedIn In May 2016, LinkedIn had 124 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark corner site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.  
**Compromised data:** Email addresses, Passwords

**Dropbox** Dropbox In mid 2016, Dropbox suffered a data breach which exposed the email addresses of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totaling over 60 million records was subsequently leaked online and included email addresses and hashed hashes of passwords (half of them SHA1, half of them bcrypt).  
**Compromised data:** Email addresses, Passwords

**Online Spambot** Online Spambot In August 2016, a spambot by the name of Online Spambot was identified by security researchers. This malicious software mimicked a normal browser component located on an IP address in the Netherlands which exposed a big number of data including personal information. In total, there were 715 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled [Inside the Massive 715 Million Breached Online Spambot Data](#).  
**Compromised data:** Email addresses, Passwords

Jeśli wyniki docelowe są takie, jak pokazano na zrzucie ekranu, masz dobry sposób na rozpoczęcie rozmowy. Jeśli Twoje konto jest tam wymienione, pamiętaj o zmianie hasła i nigdy go nie używaj ponownie. Ostatecznym celem tego ćwiczenia jest uzyskanie Dobrej wiadomości - nie znaleziono strony głównej !, zgodnie z poniższym zrzutem ekranu:



Jeśli chcesz, możesz otrzymać powiadomienie ze strony internetowej, jeśli zostaniesz poinformowany:



### Używanie ignorancji

Większość ludzi pragnie przekazywać informacje innym osobom, zwłaszcza jeśli wykazują one pewną uwagę i chęć do nauki. Inżynierowie społeczni wykorzystują niewiedzę, sztucznie ją zakładając, aby uzyskać od swoich celów pewne informacje. Po prostu wyglądając na niedoświadczonych i nieświadomych czegoś, podburzają innych do ich nauczania. Może to być wiedza ogólna lub określona umiejętność. Weźmy przykład z filmu z 2016 roku, o którym mowa we wcześniejszych rozdziałach, zatytułowanego The Catch. W jednym z odcinków oszust Christopher Hall jest w stanie uzyskać kod resetowania wszystkich sejfów w hotelu, używając sztucznej ignorancji. On rezerwuje pokój hotelowy, zamyka coś w swoim sejfie i dzwoni do hotelu, by pomógł mu go otworzyć, ponieważ zapomniał hasła i sposobu działania sejfu. Obsługujący pokazuje Hallowi kod główny, którego hotel używa do resetowania wszystkich sejfów. W końcu wykorzystuje tę wiedzę do okradania wielu innych sejfów w pokojach hotelowych wspomaganym przez swoich współników. Ten przykład pokazuje, w jaki sposób



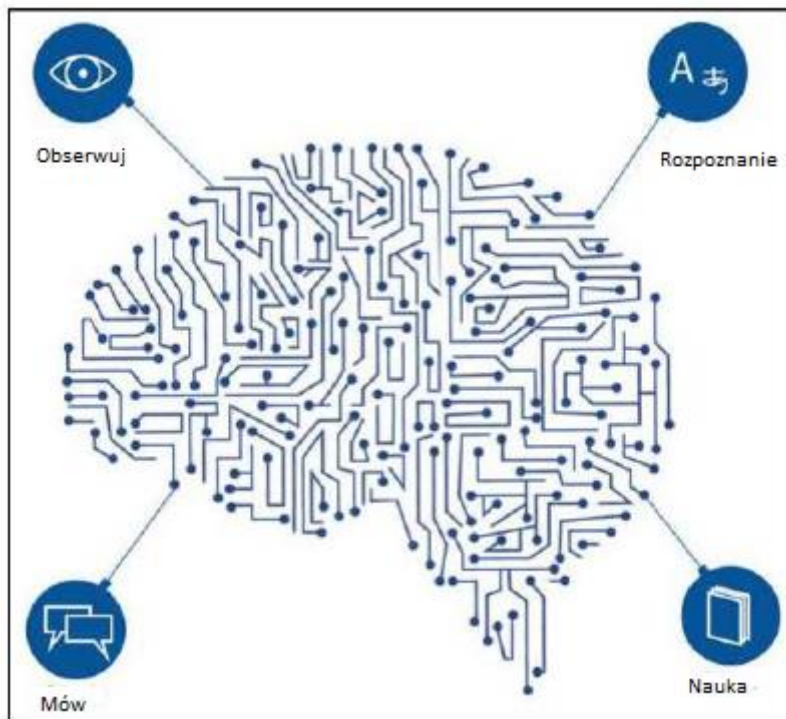
może powstać moc, grając głupiego i źle poinformowanego z innymi, posiadającymi wiedzę. Niewiedza jest jeszcze bardziej skuteczna w połączeniu z innymi technikami wywoływania, takimi jak pochlebstwa. Wzmocnienie ego ma dodatkową zaletę w otwieraniu celu. Ta technika jest bardzo skuteczna w przypadku gadatliwych celów, ponieważ można je przenieść, aby powiedzieć nieco więcej poprzez komplementy. Podobnie technika ta nie odniesie sukcesu w przypadku celów, które nie lubią się chwalić i są głównie zamknięte w sobie.

### **Czerpanie korzyści z napojów alkoholowych**

Napoje alkoholowe szybko rozluźniają mocno zamknięte usta. Właściwie, we wszystkich omawianych przykładach, gdyby wprowadzono alkohol, inżynier społeczny uzyskałby lepsze wyniki. Alkohol sprawia, że ludzie się odprężają i mówią rzeczy, których inaczej nie powiedzieliby, gdy byliby trzeźwi. Inżynier społeczny może poświęcić trochę czasu na śledzenie ulubionych pasków swoich celów. Po dłuższym przestudiowaniu tych stawów inżynier społeczny może zacząć robić regularne uderzenia w każdy cel na kilka dni. Gdy upewni się, że cel zauważył go kilka razy, inżynier społeczny może spróbować użyć alkoholu, aby uzyskać od niego informacje. Inżynier społeczny może zaoferować kupującemu pewną liczbę napojów, a gdy cel zostanie odurzony, można rozpocząć gromadzenie informacji. Pijany cel będzie bardziej podatny na wyciek poufnych informacji do inżyniera społecznego. Jednak ta technika ma zastosowanie tylko do kilku celów, którzy w pierwszej kolejności zgadzają się kupować piwo innym osobom. Kiedy cel odrzuca ofertę, technika kończy się niepowodzeniem.

### **Będąc dobrym słuchaczem**

Nie jest niczym niezwykłym, że ludzie ujawniają swoje uczucia i powierzają swoje sekrety innym ludziom, nawet całkowicie nieznanym. Odczuwa się pewną ulgę, gdy ktoś udostępnia niepokojące informacje. Wielu ludzi powstrzymuje się od wszystkiego i wszystko, czego potrzebują, to słuchanie. Ludzie ci odwiedzają częste miejsca, takie jak bary, a także kościoły, w których mają nadzieję na chwilowe złagodzenie swoich zmartwień. Inżynierowie społeczni wiedzą o tym i dlatego będą czekać w takich miejscach. Kiedy wchodzi w interakcję z kimś, kto wydaje się mieć na co narzekać, słuchają go, pozwalając celowi wyrazić swoje uczucia i po prostu je potwierdzić. Walidacja przybliży cel do inżyniera społecznego, ponieważ uważają, że utworzono połączenie z osobą, która jest w stanie go zrozumieć. Jeśli inżynier społeczny pozostaje w kontakcie z celem przez dłuższy czas, ujawnienia mogą wzrosnąć i stać się nieco bardziej wrażliwe. Inżynier społeczny będzie miał również wyjątkową możliwość zażądania od celu dodatkowych informacji, które w innym przypadku nigdy nie zostałyby ujawnione. Język ciała, kontakt wzrokowy i ton głosu inżyniera społecznego muszą wykazywać zainteresowanie tym, co mówi cel. Aby uzyskać więcej wyników, inżynier społeczny może dodać swoje osobiste, ale zmyślane historie, aby zachęcić cel do kontynuowania. Inżynieria społeczna jest sztuką hakowania ludzi i może być wykonywana przez inżynierów społecznych łatwiej, niż wielu ludziom się wydaje. Jak pokazano na poniższym obrazku, wszystko, co musisz zrobić, to uważnie obserwować, mówić ostrożnie, obserwować cel i uczyć się jak najwięcej, aby uzyskać cel, który dostarczy ci wszelkich potrzebnych informacji:



### Używając inteligentnie postawionych pytań

W uzyskaniu, inżynier społeczny nie podejździe do celu i poprosi go o podanie poufnych danych uwierzytelniających. Chociaż ta informacja jest głównym celem, należy jej szukać ostrożnie, aby uniknąć podejrzeń. Dlatego inżynierowie społeczni muszą nauczyć się zadawać pytania we właściwy sposób. W większości inżynierowie społeczni będą używać pytań, które z punktu widzenia celu będą wydawać się bezużyteczne, a zatem nie będą niechętni do udzielenia na nie odpowiedzi. Dopiero po połączeniu tych drobnych fragmentów informacji widoczny jest duży obraz. Przyjrzyjmy się bliżej rodzajom pytań, z których korzystają inżynierowie społecznościowi w celu zebrania informacji od celu:

\* Pytania otwarte: są to pytania wymagające nieco więcej niż odpowiedzi typu tak lub nie. Dlatego, jeśli są skierowane do celu, można zebrać więcej informacji. Pytania otwarte są często używane w wywiadach, aby zachęcić respondentów do dalszego udzielania odpowiedzi. Po każdym pytaniu następuje pytanie uzupełniające z pytaniem o to, dlaczego udzielono odpowiedzi i dlaczego. Dlatego cel będzie dodawał więcej szczegółów do wcześniej udzielonych odpowiedzi. Ponieważ niektóre cele mogą wykazywać pewien opór podczas odpowiadania na pytania, najlepiej zastosować podejście piramidalne, w którym inżynier społeczny zacznie od wąskich pytań i zachowa szersze pytania na końcowe części wywiadu.

\* Pytania zamknięte: Tego rodzaju pytania służą do poprowadzenia respondentów określoną ścieżką. Zazwyczaj można na nie odpowiedzieć tylko za pomocą kilku opcji. Celem nie jest zebranie informacji, ale doprowadzenie respondenta do określonego kąta, w którym można użyć innych pytań w celu zebrania potrzebnych informacji. Adwokaci i policjanci często używają tych pytań, gdy próbują przypiąć je do określonej ścieżki. Pytania mogą wydawać się krótkie i podzielone na segmenty, ale powoli powstrzymują respondenta przed przejściem do innej wersji historii.

\* Wiodące pytania: zazwyczaj pożyczają najlepsze pytania zarówno otwarte, jak i zamknięte. Są otwarte, ale dają respondentowi wskazówkę na temat oczekiwanej odpowiedzi. Na przykład widziałem, jak pewnego dnia firma drukarska przysłała kilku techników; Twoja firma musi mieć problemy techniczne z drukarkami, prawda? To pytanie zachęca do odpowiedzi tak lub nie, po której

następuje wąskie wyjaśnienie. Sugeruje również respondentowi, że masz wiedzę na temat tego, co mówisz. Nawet jeśli respondent udzieli odpowiedzi tylko tak lub nie, wiodące pytanie będzie miało inne skutki. Wiele informacji trafia do mózgu respondenta i sugeruje się więcej faktów, z którymi mógłby się zgodzić lub nie. Respondent jest zachęcany do dalszej rozmowy. Wiodące pytania są również szczególnie potężnymi narzędziami, ponieważ mogą zniekształcać wspomnienia. Można ich używać do manipulowania pamięcią celu. Badanie przeprowadzone w 1932 r. przez psychologa Bartletta doszło do wniosku, że ludzie z trudem przypominają sobie wydarzenie dokładnie i całkowicie. Dzieje się tak, ponieważ ludzie tworzą wspomnienia na różne sposoby w oparciu o to, co ich mózg uważa za ważne. Gdy respondent odwołuje się do tych samych wspomnień, niektóre z nich zostaną utracone, a te uznane za ważne zostaną przywołane. Aby zatuszować deficyt, wykonuje się pewne uogólnienia w celu uzupełnienia braków.

Dlatego jeśli respondentowi zostanie wstępnie załadowana jakaś informacja przed zadaniem pytania, wstępnie załadowane informacje będą miały zniekształcający wpływ na pamięć. Wiodące pytania są zatem bardzo ważnymi narzędziami do silnego, ale nieświadomego wyszukiwania informacji, które prowadzą respondenta na określoną ścieżkę.

### **Przypuszczalne pytania**

To tutaj zakłada się, że cel ma wiedzę na temat niektórych rzeczy, dlatego zadaje się pytania na tej podstawie. Na podstawie udzielonych odpowiedzi inżynier społeczny będzie w stanie ustalić, czy cel był w posiadaniu założonej wiedzy. W egzekwowaniu prawa funkcjonariusze często korzystają z tego rodzaju pytań. Na przykład mogą zapytać cel: Gdzie mieszka Pan X, ofiara? Ważną częścią tego pytania jest to, że funkcjonariusz zakłada, że to respondent ma pewne informacje na temat ofiary. Istnieje prawdopodobieństwo, że podejrzany go nie zna, ale może on. Odpowiedź, którą udzieli, ujawni, ile podejrzany wie. Inżynierowie społeczni nie wykorzystują jednak przypuszczalnych pytań, aby umieścić cele w niewłaściwym celu. Unikają też dawania ofiarom całego obrazu. Takie postępowanie pozbawiłoby moc założeń. Przyjęte pytania są wykorzystywane, gdy inżynier społeczny ma jakąś faktyczną wiedzę o czymś. Na przykład inżynier społeczny może zapytać: Masz zainstalowane nowe systemy bezpieczeństwa, prawda? Inżynier społeczny mógł zobaczyć, jak van firmy zajmującej się systemami bezpieczeństwa wjeżdża do miejsca pracy celu.

Na tej podstawie mógł założyć, że byli tam, aby zainstalować niektóre systemy bezpieczeństwa. To są informacje, których używa, by postawić przypuszczalne pytanie do celu. Cel udzieli odpowiedzi takich jak: Tak, nie, właśnie przeprowadzali naprawy lub dodali system biometryczny, wśród wielu innych rodzajów odpowiedzi. Każda odpowiedź mówi inżynierowi społecznemu, ile cel wie o systemach bezpieczeństwa i opiera się tylko na obserwacji furgonetki firmy zajmującej się systemami bezpieczeństwa, która wjeżdża do organizacji. Do celu wstępnie wczytuje również założenie, że inżynier społeczny jest dość poinformowany, a zatem będzie świadomy, gdy zostanie podana błędna odpowiedź.

### **Bracketing**

Jest to również powiązane z dwoma poprzednimi tematami, założonymi i inteligentnymi pytaniami. Bracketing jest stosowany w scenariuszach, w których inżynier społeczny chce uzyskać dokładne informacje od celu, nie wydaje się, aby bezpośrednio o to prosił. Jest używany głównie podczas wyszukiwania informacji liczbowych. Inżynier społeczny zadaje pytanie, po którym następuje przybliżenie, które jest celowo podawane w celu nakłonienia celu do podania dokładnej liczby w odpowiedzi. Na przykład inżynier społeczny może zapytać pracownika: Hej! Idąc za odznaką, zakładam, że pracujesz w firmie XYZ. Słyszałem, że twoje bezpieczeństwo jest silniejsze niż w naszej organizacji, ale przed wejściem do obiektu mamy dwa strzeżone punkty kontrolne i weryfikację biometryczną. Cel

udzieli odpowiedzi, w której znajdzie się dokładna liczba fizycznych kontroli bezpieczeństwa, które trzeba przejść, aby dostać się do organizacji. Są to informacje, które mogą być wykorzystane przez inżyniera społecznego do zaplanowania, jak fizycznie wejść do organizacji. Bracketing jest szczególnie przydatny w atakach inżynierii społecznej podczas interakcji z pracownikami ochrony w organizacji. Najłatwiej jest je otworzyć, gdy ktoś, kto wydaje się ważny, wdaje się z nimi w krótką rozmowę. Są również bardziej zaznajomieni z fizycznymi kontrolami bezpieczeństwa w organizacji. Zapytani o liczbę kamer monitorujących przednie i tylne wejścia, są najlepiej przygotowani do podania tych informacji. Powiedzmy na przykład, że inżynier społeczny planuje wkraść się do organizacji i nurkować w śmietniku. Dla celów przypomnienia nurkowanie w śmietnikach jest techniką zbierania informacji z inżynierii społecznej, która polega na przechodzeniu przez śmieci. Jeśli inżynier społeczny zauważy, że śmieci znajdują się w pobliżu tylnego wejścia, może on chcieć zebrać informacje na temat liczby kamer obserwujących tyły. Oczywiście jest, aby przejść bezpośrednio i poprosić strażników o podanie tych informacji. Dlatego inżynier społeczny może do nich podejść i powiedzieć coś takiego, co muszę powiedzieć, że masz tutaj najtrudniejszą pracę. Dość rozległy obszar, który musisz pilnować. Założę się, że masz dwie kamery z tyłu i pięć z przodu. Czy się mylę? To pytanie spowoduje prawidłowe wyjaśnienie liczby kamer i ich obszarów zasięgu. Ponieważ oświadczenie to po raz pierwszy ociera ego strażnika, on lub ona będzie chciał podzielić się więcej na temat delikatnych kontroli bezpieczeństwa wprowadzonych w celu pomocy w monitorowaniu.

### **Nauka umiejętności pozyskiwania**

W poprzednich częściach wskazaliśmy kilka wskazówek i technik, które pomogą Ci opanować nauczane umiejętności, dzięki czemu będziesz lepiej przygotowany do obrony przed niektórymi technikami inżynierii społecznej. Dlatego przejdziemy przez kilka wskazówek, jak zostać mistrzem w pozyskiwaniu. Należy jednak pamiętać o następujących kwestiach:

\* Inżynier społeczny nigdy nie zadaje celowi zbyt wielu pytań, ponieważ to prawdopodobnie go wyłączy. Nic nie jest tak denerwujące, jak bycie zarzucanym pytaniem za pytaniem za pytaniem. Zapamiętaj trzy podane wcześniej wskazówki dotyczące rozpoczynania i prowadzenia rozmów z celami.

\* Inżynier społeczny nigdy nie zadaje za dużo pytań, aby uniknąć podejrzeń i niezręczności. Nigdy nie zostawiliby celu zastanawiając się, dlaczego zadano niektóre pytania, a następnie szybko porzucono. Będą wiedzieć, jak polubownie zamknąć szereg pytań.

\* Inżynierowie społeczni nigdy nie zadają więcej niż jednego pytania na raz. Spowoduje to nie tylko zamieszanie, ale także zmniejszy ilość informacji, które cel będzie skłonny przekazać.

Wydobywanie wymaga delikatnej równowagi. Inżynier społeczny nie może nigdy unikać ekstremum albo za małego, albo za dużego. Również wzbudzenie dotyczy nie tylko inżynierii społecznej. W przeciwieństwie do niektórych innych umiejętności nauczanych w poprzednich rozdziałach, umiejętności tu nauczane mają zastosowanie w zwykłych i nie złośliwych rozmowach. Wywoływanie powinno odbywać się zgodnie z tym samym przebiegiem normalnej rozmowy; po prostu inżynier społeczny powinien kontrolować ścieżkę rozmowy. Pomyśl o wzbudzeniu jak o lejku, szerokim u góry i zwężającym się głębiej. Na początku rozmowy rozmowa jest neutralna, a zadawane pytania są losowe. Jednak w miarę postępu rozmowy rozmowa koncentruje się na kilku tematach, na których inżynier społeczny chce gromadzić dane. Dlatego pytania otwarte mogą być wykorzystane do rozpoczęcia rozmowy i kontynuowania jej, a stamtąd można zadać pytania zamknięte, aby skierować rozmowę w dół ścieżki. Na końcu lejka inżynier społeczny otrzyma dobry strumień informacji od klienta, przefiltrowany w celu podania tylko niezbędnych szczegółów. Proces musi przebiegać ostrożnie, aby

zapewnić, że inne elementy inżynierii społecznej, takie jak relacje i zaufanie, zostaną zbudowane wcześniej w trakcie rozmowy, aby uniknąć oporności celu na odpowiedzi na niektóre pytania.

## **Porady**

Wskazówki dotyczące unikania wywoływania są następujące:

- \* Wydobywanie to sztuka uzyskiwania odpowiedzi bez zadawania pytań. Innymi słowy, wzbudzenie jest tym, co mówisz i jak to mówisz. W oparciu o NSA, pozyskiwanie jest procesem pozyskiwania informacji z czegoś lub kogoś, a to, co powiesz i jak to określisz, określi Twój sukces.
- \* Najślabszymi ogniwami łańcucha bezpieczeństwa informacji są ludzie i sieci społecznościowe.
- \* Społeczne interakcje z ludźmi są znacznie łatwiejsze w obsłudze niż złożone systemy informatyczne.
- \* Narzędzia są ważnym aspektem inżynierii społecznej, ale nie są inżynierem społecznym. Samo narzędzie jest bezużyteczne; ale wiedza o tym, jak wykorzystać i wykorzystać to narzędzie, jest nieoceniona (Christopher Hadnagy).
- \* Najlepszym środkiem zaradczym przeciwko pozyskaniu jest wiedzieć, co powiedzieć i ile powiedzieć. Dotyczy to również witryn mediów społecznościowych; udostępnianie jest dobre, ale tylko wtedy, gdy wiesz, co i ile powinieneś udostępnić.

## **Podsumowanie**

W tej krótkiej części omówiono bardzo potężną umiejętność wykorzystywaną w inżynierii społecznej do wydobywania celów i stawiania ich w miejscu, z którego można je wykorzystać. Sprawdził, jak można nawiązać rozmowę z całkowicie nieznanym i utrzymać ją. Co ważniejsze, przyjrano się, jak inżynier społeczny może wstępnie załadować cel pewnymi informacjami, aby wpłynąć na odpowiedź celu. Wreszcie, rozdział przeanalizował szereg taktyk, które można zastosować, aby skutecznie przeprowadzić wzbudzenie. Aby wspomnieć tylko kilka, przeanalizowano, w jaki sposób można użyć inteligentnych pytań, pytań przypuszczających i bracketingu, aby uzyskać cel i podać pewne informacje z dokładnością. Pogłaskanie ego i pochlebstwo celów było również dyskutowane jako sposób na to, aby cel przekroczył niektóre szczegóły, które wydają się wrażliwe. Wreszcie, alkohol i uważne uszy zostały omówione jako świetna taktyka, aby skłonić ludzi do powierzenia poufnych informacji innym osobom.

Wydobycie, e wydobywa ludzi z granic określonych stref bezpieczeństwa i zachęca ich do dzielenia się szczegółami, których w innym przypadku unikaliby dzielenia się z obcymi. Omówiono kilka taktyk, które są stosowane, aby zapewnić, że wywołanie przebiegnie pomyślnie i że cele zostaną przekonane do podzielenia się wrażliwymi szczegółami z nieznanymi.