CHRISTOPHER HADNAGY

Przedmowa

DR PAUL EKMAN

SOCJOTECHNIKA

Metody manipulacji i ludzki aspekt bezpieczeństwa

WILEY

onepress Helion

Tytuł oryginału: Unmasking the Social Engineer: The Human Element of Security

Tłumaczenie: Joanna Sugiero

ISBN: 978-83-283-6948-1

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://onepress.pl/user/opinie/socjom
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *http://onepress.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

2

Czym jest socjotechnika?

Oświecenie to nie jest wyobrażanie sobie świetlistych postaci, lecz wniesienie świadomości do ciemności.

— *Carl Gustav Jung*

Oto moja definicja socjotechniki: jest to dowolne działanie, które wpływa na drugą osobę, żeby zrobiła coś, co może — lub nie — leżeć w jej interesie. W rozdziale 1. krótko wspomniałem o zleceniu, które polegało na infiltracji magazynów bez włamywania się do nich. Aby osiągnąć ten cel, użyłem metod socjotechniki związanych z używaniem pretekstu, odgrywaniem ról, a także z trzema lub czterema innymi aspektami wpływania na ludzi. Moim zadaniem było przetestowanie mechanizmów obronnych firmy i sprawdzenie, czy pracownicy przestrzegają ustalonych reguł. Miałem również zrobić zdjęcia wyjść i kamer, a także innych kluczowych miejsc w firmie — czyli zdobyć informacje, które prawdopodobnie interesowałyby prawdziwego przestępcę planującego włamanie się do magazynu. Oto typowy scenariusz takiego zlecenia.

Podjechałem do magazynu i nacisnąłem guzik domofonu przy drzwiach wejściowych. Odezwałem się:

— Dzień dobry, tu Paul z firmy wywożącej śmieci. Muszę sprawdzić numer seryjny waszej zgniatarki do śmieci.

Drzwi zabrzęczały — zostałem wpuszczony do wewnętrznej części magazynu. Stanąłem przed metalową śluzą mającą postać dwóch ścian od podłogi do sufitu. Podszedł do mnie ochroniarz i powiedział:

— Proszę poczekać. Zaraz przyjdzie do pana kierownik sali, który zaprowadzi pana dalej.

Po kilku minutach przyszedł Roy, kierownik sali, i przywitał się ze mną. Przeszedłem przez budzącą strach śluzę, po czym wysłano mnie do ochroniarza. Ten kazał mi się wylegitymować. Spojrzałem na niego, a potem na śluzę i powiedziałem:

— Zostawiłem dokumenty w samochodzie. Ale mam identyfikator firmowy. Czy to wystarczy?

Ochroniarz zeskanował moją plakietkę i dał mi identyfikator dla gościa. Potem Roy zaprowadził mnie do zgniatarki.

Po kilku sekundach powiedziałem:

— Macie szczęście. Nie ma waszego numeru na naszej liście.

— Co to oznacza? — spytał Paul.

— Nie trafił się wam wadliwy silnik, więc zgniatarka powinna działać bez zarzutu.

Podczas drogi powrotnej nagle wykrzyknąłem:

— Kurczę! Zostawiłem telefon na zgniatarce. Muszę po niego wrócić.

Kilka minut później podszedłem do Roya, który czekał już w swoim biurze, uścisnąłem mu dłoń, oddałem identyfikator dla gościa i wyszedłem z budynku.

Oprócz zdobycia oczywistego dowodu na to, że polityka firmy nie jest idealnie przestrzegana, opuściłem budynek z telefonem pełnym zdjęć, na których widać kamery monitoringu, wyjścia oraz miejsca, gdzie są przechowywane „towary".

Socjotechnika nie zawsze polega na oszukiwaniu lub zwodzeniu. Bardziej skupia się na tym, jak na co dzień komunikujemy się z ludźmi — w jaki sposób z nimi rozmawiamy i jak skutecznie przekazujemy im to, co chcemy powiedzieć.

W swojej pierwszej książce *Socjotechnika. Sztuka zdobywania władzy nad umysłami* opisałem dokładnie wszystkie fizyczne, psychologiczne i osobiste narzędzia potrzebne każdemu, kto chce zostać wykwalifikowanym socjotechnikiem. Nie będę tutaj powtarzał tego, co tam napisałem; jedynie krótko omówię techniki i metody stosowane przez socjotechników.

Pamiętaj, że dla socjotechnika kluczowe jest to, aby stać się częścią tego samego „plemienia", do którego należy jego cel. Tym plemieniem może być miejsce pracy, ale również grupa ludzi mających te same przekonania, noszących podobne ubrania albo słuchających jednego gatunku muzycznego. Jeżeli potrafisz wykorzystywać umiejętności opisane w następnych podrozdziałach, bez większego trudu dołączysz do plemienia swojego celu. A gdy już tak się stanie, zdobycie informacji albo zyskanie dostępu stanie się dużo prostsze.

Zdobywanie informacji

Informacje to fundament działalności socjotechnika. Im więcej informacji on posiada, tym więcej ataków (inaczej metod infiltracji) może przygotować, tym lepiej rozumie swój cel i tym skuteczniej potrafi zidentyfikować jego mocne i słabe strony.

Informacje można wyszukać w internecie, używając do tego takich narzędzi jak Google hacking i Maltego. Można również zgromadzić je osobiście, na przykład robiąc zdjęcia, obserwując jakieś miejsce albo stosując metodę wzbudzania.

Potęga internetu sprawiła, że gromadzenie informacji stało się dużo prostsze, a to oznacza, że socjotechnik jest w stanie pozyskać bardzo dużo danych. Umiejętność kategoryzowania i przechowywania tych informacji również jest bardzo ważna.

Mam nawyk opracowywania SPD (szczegółowych planów działania) dotyczących moich celów. Plany te obejmują zebrane informacje, zaobserwowane działania lub zachowania, a także uwagi na temat tego, jak zgromadziłem te informacje. Później koreluję to z atakami, które chcę przeprowadzić, i w ten sposób powstaje mój plan działania dla każdego celu.

Johnny Long, socjotechnik i etyczny haker, który został filantropem, opracował wstępną bazę danych Google Hacking Database, czyli listę wyszukiwań, jakie można przeprowadzić w Google, żeby znaleźć rozmaite pikantne informacje. W ostatnich latach ludzie z Offensive Security przejęli ten projekt i obecnie jest on prowadzony pod adresem *www.exploit-db.com*.

Oprócz tego typu narzędzi są jeszcze inne, takie jak Maltego, które pozwala na gromadzenie danych na temat ludzi, stron internetowych albo firm i kategoryzuje je w formacie graficznym, czytelnym i łatwym w użyciu. Więcej informacji znajdziesz na *www.paterva.com*.

Niedawno odkryłem jeszcze dwa inne narzędzia, które okazały się bardzo przydatne: są to Google Maps i Bing Maps. Jeżeli zrobisz wystarczająco duże zbliżenie, obie strony pokażą Ci *street view*, czyli rzeczywiste zdjęcia wybranej ulicy. Znając wygląd budynku, jego układ, ogrodzenie, lokalizację kamer i wiele innych szczegółów, zaoszczędzisz sporo czasu w porównaniu z sytuacją, gdybyś miał tego wszystkiego dowiedzieć się dopiero na miejscu.

Bez względu na to, w jaki sposób socjotechnik gromadzi informacje, ogólna zasada mówi: „Nie ma czegoś takiego jak nieprzydatne informacje". Nawet najdrobniejsze szczegóły mogą Ci bardzo pomóc w wykonaniu zlecenia.

Tworzenie pretekstu

Twoim pretekstem jest osoba, którą chcesz udawać — rola, którą będziesz odgrywać. Możesz to porównać do aktorstwa — stajesz się osobą, którą udajesz. Ubranie, identyfikator, mowa ciała i wiedza — to wszystko ma istotny wpływ na to, czy Twój pretekst będzie wiarygodny.

W przykładzie, który podałem na początku tego rozdziału, moim pretekstem był „Paul, pracownik firmy utylizującej odpady". Aby mój pretekst przyniósł pożądany efekt, musiałem najpierw wszystko zaplanować. Moje ubranie musiało być tak przekonujące, żeby moje cele uwierzyły, że jestem tym, za kogo się podaję. Tak jak wspomniałem w rozdziale 1., pisząc o koncepcji „ubranego poznania", musiałem mieć pewność, że moje ubranie pomoże mi wczuć się w rolę i będzie przekazywało odpowiedni komunikat.

Mój identyfikator musiał być realistyczny. Moja mowa ciała musiała sugerować, że jestem pracownikiem fizycznym i nie pełnię żadnej funkcji kierowniczej. Musiałem też znać się na artefaktach, których używałem, żeby potwierdzić swój pretekst. Musiałem zdobyć potrzebną wiedzę o zgniatarkach do śmieci, dowiedzieć się, w którym miejscu umieszczany jest numer seryjny i czego w ogóle mam szukać, jak również posiadać wszystkie narzędzia potrzebne do wykonania mojej „pracy".

Dlatego też pretekst nie zawsze jest osobą. W ciągu mojego pięciodniowego kursu każę uczestnikom każdego wieczoru wyjść do jakiegoś publicznego miejsca i zebrać informacje od ludzi — w ten sposób chcę im pokazać, jak mogą wykorzystywać nowe umiejętności do nawiązywania relacji, wzbudzania zaufania i szybkiego zdobywania informacji. Na jednym z kursów poprosiłem uczestników, żeby spotkali się w pokoju hotelowym i zdobyli informacje, udając, że pracują w call center.

Aby stworzyć ten pretekst, pobrali oni aplikację o nazwie „Thriving Office", która odgrywała w tle dźwięki typowe dla pracy biurowej. Jedna z osób odtwarzała te dźwięki na swoim telefonie komórkowym, a pozostałe zaczęły dzwonić do ludzi. Dla osoby po drugiej stronie słuchawki pretekst był kompletny w chwili, gdy usłyszała odgłosy „call center".

Pretekst socjotechnika — czy to w relacjach bezpośrednich, w rozmowach przez telefon czy w kontaktach za pośrednictwem poczty elektronicznej — musi obejmować ubranie, język i dobór słów, dźwięki, a także wszystkie pozostałe aspekty danej metody komunikacji, tak aby cel nie miał żadnych wątpliwości, że socjotechnik jest osobą, za którą się podaje.

Wzbudzanie

Wzbudzanie to sztuka zdobywania informacji bez zadawania pytań wprost, podczas prowadzenia zwykłej konwersacji. Wzbudzanie to rozmawianie z celem o jego życiu, rodzinie i pracy. Nawiązujesz relację z tą osobą (zobacz następny podrozdział) i zdobywasz jej sympatię, dzięki czemu otwiera się ona przed Tobą i podaje Ci szczegóły, które będziesz mógł później wykorzystać. Jest to bardzo prosta definicja, ale nie zapominajmy o tym, że mówimy tutaj o jednym z najważniejszych aspektów socjotechniki.

Pod koniec tej książki poświęcę sporo czasu na wyjaśnienie, w jaki sposób komunikacja niewerbalna wpływa na wzbudzanie i może zwiększyć Twoje szanse na to, że zostaniesz mistrzem wydobywania informacji.

Nawiązanie relacji

Robin Dreeke, mój przyjaciel i autor książek, definiuje i omawia umiejętności nawiązywania relacji w swojej książce *It's Not All About „Me"*. Robin potrafi każdego szybko nauczyć, jak sprawić, żeby osoby w naszym towarzystwie poczuły się lubiane, co jest niezbędne do stworzenia atmosfery zaufania. To właśnie zaufanie sprawia, że nasz rozmówca chętnie mówi i wyjawia informacje, które mogą okazać się dla nas cenne. Może ono również skłonić go do działania takiego jak kliknięcie złośliwego linku albo wpuszczenie socjotechnika do swojego domu czy biura.

Relacja to poczucie bliskości lub zaufania. Rodzi się ono wówczas, gdy ktoś psychologicznie otwiera się na drugą osobę i nie obawia się podać jej informacji dotyczących swojego życia.

Robin wyróżnił 10 różnych metod nawiązywania relacji. Oto ich krótka lista:

- **Sztuczne ograniczenia czasowe:** dajesz ludziom do zrozumienia, że będziesz się nimi „zajmował" tylko przez bardzo krótki czas.
- **Ukierunkowana komunikacja niewerbalna:** dbasz o to, aby Twoja komunikacja niewerbalna pasowała do słów, które wypowiadasz — w przeciwnym razie Twojemu rozmówcy zapali się w głowie czerwona lampka.

- **Spowolnienie tempa mówienia:** mówisz na tyle wolno, aby nie wyglądać na zdenerwowanego.
- **Wątki współczucia i sympatii:** używasz słów, które mają wielką moc, takich jak: „Możesz mi pomóc?".
- **Zrezygnowanie z ego:** ten ważny aspekt polega na zignorowaniu własnego ego, tak aby inni mieli rację, nawet jeśli jej nie mają.
- **Potwierdzenie:** w życzliwy i szczery sposób potwierdzasz wiedzę lub umiejętności drugiej osoby.
- **Pytania jak, kiedy i dlaczego:** zadajesz pytania otwarte, które zachęcają do dłuższej odpowiedzi.
- **Coś za coś:** podajesz drobną informację, żeby druga osoba poczuła się komfortowo, gdy będzie dzielić się informacjami o sobie.
- **Wzajemny altruizm:** dajesz prezent po to, aby otrzymać prezent.
- **Zarządzanie oczekiwaniami:** nie jesteś chciwy i potrafisz rozpoznać, gdy coś nie działa, a następnie wprowadzić potrzebne zmiany.

Każdy z tych dziesięciu aspektów ma ogromną moc i może być częścią arsenału skutecznego socjotechnika.

Wpływ i manipulacja

Ja definiuję wpływ jako nakłonienie kogoś, żeby *chciał* zrobić to, czego Ty od niego chcesz. Zasadniczo chodzi o to, żeby cel podjął określone działania z własnej woli, jak gdyby to był jego pomył — jakby od samego początku chciał to zrobić.

Jednym z największych ekspertów w tej dziedzinie jest dr Robert Cialdini. Poświęcił on całe życie na badanie wpływu i jego działania.

Dr Robert Cialdini definiuje osiem zasad wpływu:

- **Wzajemność:** wywoływanie uczucia zobowiązania poprzez bycie pierwszym, który coś daje.
- **Ustępstwo:** wpływanie na kogoś, żeby podjął określone działanie w oparciu o uczucie — może to być społeczna norma okazywania wdzięczności albo poczucie, że jest Ci coś winien.

- **Przyzwolenie:** przekonanie kogoś, żeby udzielił mniej znaczących odpowiedzi. Jeżeli cel ulegnie i odpowie na podstawowe pytania, łatwiej będzie go skłonić, żeby odpowiedział na większe, ważniejsze pytania.
- **Niedobór:** kiedy ludzie są przekonani, że dany przedmiot (albo informacja) jest trudny do zdobycia, jest na wyczerpaniu albo może stać się zupełnie niedostępny, rzecz ta staje się czymś rzadkim, a przez to cenniejszym.
- **Autorytet:** odwołanie się do naszego wrodzonego pragnienia, aby przestrzegać reguł i postępować zgodnie z zasadami, zwłaszcza gdy pochodzą one od kogoś zajmującego wyższą pozycję.
- **Zobowiązanie i konsekwencja:** tutaj chodzi o sytuacje, gdy cel zaczyna już podążać wyznaczoną ścieżką. Chce on zachować konsekwencję w swoich działaniach i reakcjach, a to wywołuje poczucie zobowiązania do udzielenia spójnych odpowiedzi.
- **Lubienie kogoś:** ludzie lubią tych, którzy ich lubią. Jeżeli nasz cel czuje się lubiany, chętniej polubi nas i wyjawi nam informacje, których potrzebujemy.
- **Dowód społeczny:** jeśli wszyscy coś robią, to nie może to być nic złego. Ta zasada jest oparta na potrzebie bycia częścią grupy.

Zrozumienie, opanowanie i używanie tych ośmiu zasad może uczynić z Ciebie prawdziwego mistrza socjotechniki. Kiedy się dobrze przyjrzysz zasadom manipulacji, uświadomisz sobie, że są one bardzo podobne do zasad wpływu. Jednak odróżnienie jednych od drugich jest bardzo ważne. Wpływanie na drugą osobę polega na przekonaniu jej, żeby chciała zrobić to, czego Ty od niej chcesz, natomiast manipulacja to skłonienie kogoś do zrobienia czegoś, czego on nie chce zrobić.

Zasadniczo podczas wpływania na drugą osobę Twoim celem jest sprawienie, aby poczuła się ona lepiej w związku z tym, że Cię poznała. Kiedy kimś manipulujesz, nie skupiasz się na jego uczuciach; Twoim celem jest zdobycie tego, czego pragniesz, bez względu na to, co czuje druga osoba.

Jako socjotechnik staram się nigdy nie stosować manipulacji, ponieważ psuje ona samopoczucie moich klientów, niszczy nasze relacje i sprawia, że pracownicy nie są otwarci na zdobywanie nowej wiedzy podczas szkolenia. Jednocześnie zawsze staram się wpływać na pracowników, ponieważ dzięki temu klienci otwierają się na rady, naukę i zmiany.

Oto wspaniały przykład: kiedyś mój przyjaciel powiedział mi, że manipulacja jest jak przekonanie dziecka, żeby zgodziło się na zrobienie mu zastrzyku, którego potrzebuje. Dzięki lekarstwu dziecko poczuje się lepiej, ale igła trochę zakłuje. Jako profesjonalny socjotechnik — bez względu na to, w jaki sposób Cię skłonię do wyjawienia informacji — dobrze wiem, że trochę zakłuje, ale stosuję metodę, która zminimalizuje to ukłucie, tak abyś je zaakceptował i zwiększył swoje bezpieczeństwo.

Ramowanie

Ramy człowieka można porównać do podstawowej struktury domu: jest to jego historia emocjonalna, psychologiczna, osobista i rodzinna. Co sprawia, że myśli, zachowuje się i mówi w taki, a nie inny sposób? Wewnętrzna motywacja to właśnie jego ramy.

Wszystko, co dana osoba przeżyła, ma wpływ na to, jak postrzega ona świat wokół siebie i jak reaguje na różne wydarzenia. Jeżeli socjotechnik zrozumie jej ramy, będzie mógł zacząć budować most między nimi a własnymi ramami.

Najprostszym sposobem, aby to zrobić, jest znalezienie czegoś, co łączy go z tą osobą, a potem nawiązanie z nią relacji. Takie podejście bardzo ułatwia połączenie obu ram. Kiedy już do tego dojdzie, socjotechnik i jego cel staną się częścią tego samego „plemienia", a wówczas wydobycie informacji od celu przyjdzie socjotechnikowi z większą łatwością.

Komunikacja niewerbalna

W rozdziale 1. szczegółowo omówiłem zagadnienie komunikacji niewerbalnej. Jak napisałem w pierwszej książce, ten rodzaj komunikacji bardzo zmienił nasze postrzeganie socjotechniki. Połączenie komunikacji niewerbalnej z innymi aspektami, które przed chwilą opisałem, może z każdego zrobić skutecznego socjotechnika.

Komunikaty niewerbalne stanowią dużą część tego, jak się porozumiewamy. To, co mówimy, jest potwierdzane albo negowane przez to, w jaki sposób to mówimy i jak wtedy wyglądamy. Zdobycie umiejętności wykrywania, analizowania i odczytywania mikroekspresji, makroekspresji, sygnałów

konwersacyjnych oraz mowy ciała może pomóc socjotechnikowi w zrozumieniu stanu emocjonalnego jego celu.

Poznanie tego stanu jeszcze przed nawiązaniem interakcji jest potrzebne do tego, żeby odpowiednio dostosować własne nastawienie, jak najlepiej zacząć rozmowę, zadawać właściwe pytania, a także w odpowiedni sposób pokierować całą rozmową.

W swojej pierwszej książce poruszyłem te kwestie tylko pobieżnie i omówiłem jedynie podstawy ekspresji mimicznych. Ta książka, dzięki pomocy dr. Paula Ekmana, zawiera szczegółową analizę ruchów mimicznych, a także ruchów dłoni, ciała, nóg i tułowia. Już niedługo wyjaśnię, jakie informacje na temat emocji odczuwanych przez osobę będącą naszym celem można wyciągnąć z obserwacji wymienionych tutaj części ciała.

Najpierw jednak musimy zastanowić się nad tym, jaką rolę odgrywa komunikacja niewerbalna w różnych rodzajach socjotechniki.

Trzy podstawowe formy socjotechniki

Nieetyczne działania z zakresu inżynierii społecznej są zazwyczaj dzielone na trzy kategorie. Ważne jest, aby wiedzieć, czym się one różnią, ponieważ komunikacja niewerbalna odgrywa ważną rolę w każdej z nich. Przyjrzyjmy się im po kolei. Są to: phishing, wyłudzanie informacji przez telefon i personifikacja.

Łowienie ludzi na haczyk

Najpowszechniej stosowaną formą socjotechniki jest phishing — wysyłanie do wybranych odbiorców masowych e-maili albo wiadomości zawierających złośliwe pliki, linki bądź instrukcje. Jeżeli odbiorca otworzy plik, kliknie link albo postąpi zgodnie z instrukcją, umożliwi włamanie się, wykradzenie danych oraz wiele innych niebezpiecznych działań.

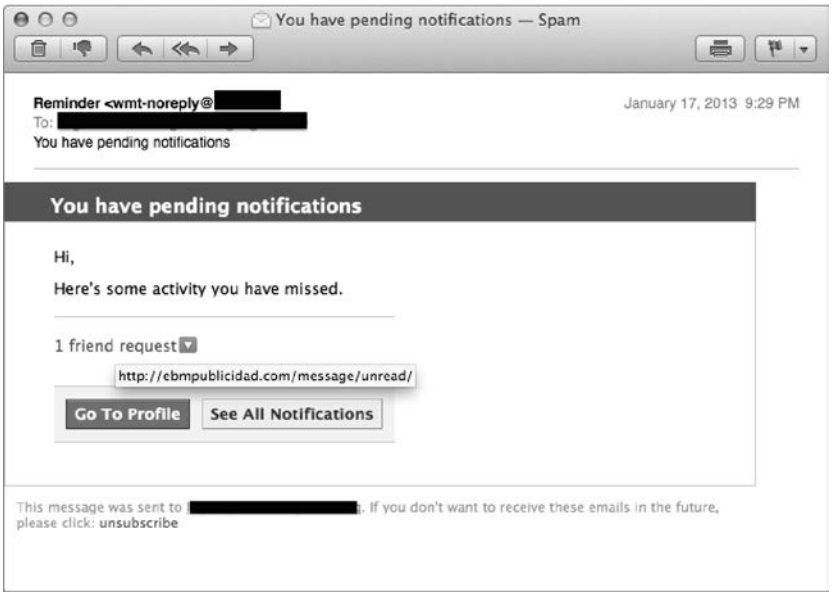
Kiedy pisałem ten rozdział, w wiadomościach mówili właśnie o działaniu, które należy do kategorii phishingu. Jeden z dyrektorów pracujących w Coca-Coli otrzymał e-mail z instrukcją, aby otworzyć plik od dyrektora generalnego dotyczący oszczędzania energii — była to inicjatywa silnie promowana przez firmę w tamtym czasie. Wiadomość, zawierająca załącznik, nie pochodziła ze sprawdzonego źródła. Kiedy dyrektor otworzył plik, na jego

komputerze uruchomił się program, który dał hakerom zdalny dostęp do jego sprzętu. To z kolei spowodowało osłabienie bezpieczeństwa całej sieci. Minęło wiele miesięcy, zanim wykryto tę lukę.

E-maile phishingowe są tak popularną metodą, że pewna grupa twierdzi, iż jeden na każde 300 odebranych e-maili to wiadomość phishingowa — i to nie uwzględniając sytuacji, w których celem ataku są konkretne osoby. Kiedy socjotechnik obiera sobie kogoś za cel, używa metody spear phishing — wysyła bardzo spersonalizowane e-maile, które zawierają szczegóły nawiązujące do tego, co odbiorca lubi i czego nie lubi. Może też zastosować whaling — jest to ukierunkowany atak na ważny cel z branży biznesowej, taki jak dyrektor generalny dużego banku.

W każdej z wymienionych metod socjotechnik pisze e-maile, które wykorzystują strach, ciekawość albo władzę, żeby nakłonić odbiorcę do zrobienia czegoś, co jest sprzeczne z jego interesem.

Spójrzmy na przykład phishingu i przekonajmy się, dlaczego ta taktyka jest tak skuteczna. Obecnie najwięcej ataków phishingowych jest ukierunkowanych na Facebooka. Portal ten, mający ponad miliard użytkowników, jest bez wątpienia atrakcyjnym celem. Spójrzmy na rysunek 2.1.



Rysunek 2.1. Podszywanie się pod Facebooka to jeden z najbardziej popularnych form ataków phishingowych

Warto zwrócić uwagę na kilka ważnych kwestii dotyczących tej formy phishingu. Po pierwsze jest ona skuteczna, bo wiadomość wygląda jak prawdziwy e-mail od Facebooka. Ma takie same kolory, styl i układ. Jest prosta i nieprzekombinowana. Ponadto temat został skopiowany z prawdziwych e-maili od Facebooka.

Jest jednak kilka szczegółów, które świadczą o tym, że ta wiadomość jest fałszywa:

- Adres w polu „Od" nie jest adresem Facebooka. Czasami socjotechnicy używają bardzo podobnych nazw, na przykład facbook.com, faceboook.com albo facebook.co — tego typu literówki mogą pozostać niezauważone.
- Powitanie jest ogólne, zaczyna się od „Hi", czyli „Cześć". Normalnie powinno się tu pojawić Twoje imię albo nazwa użytkownika.
- Ważną wskazówką, która często pozostaje niezauważona, jest link. Kiedy umieścisz nad nim znacznik myszki, zobaczysz, że wcale nie przekierowuje Cię on do Facebooka, lecz do strony internetowej przygotowanej przez socjotechnika.
- Przykład z rysunku jest sprytnie przemyślany, ponieważ nie tylko link do Facebooka, ale też przyciski, a nawet link „Wypisz się", prowadzą do strony-pułapki.

Innym przykładem pokazującym, jak poważnym problemem może być phishing, jest fałszywy e-mail udający wiadomość od PayPala, taki jak ten widoczny na rysunku 2.2.

Takie wiadomości przyciągają naszą uwagę, ponieważ uderzają nas po kieszeni — a raczej wmawiają nam, że tak się stało. Strach przed tym, że ktoś mógł zyskać dostęp do naszych pieniędzy i nas okraść, często jest tak silnym bodźcem, iż klikamy link i szybko logujemy się na konto, chcąc sprawdzić sytuację. I dokładnie o to chodzi atakującemu. Dane, które wpisujesz, są wykradane za pośrednictwem fałszywej strony internetowej, fałszywego loginu i prostego skryptu. Kiedy atakujący je zdobędzie, zaloguje się na Twoje konto i zrobi dokładnie to, czego tak bardzo się wystraszyłeś: ukradnie Ci pieniądze.


This message is Highest priority.
From: Paypal <service@paypal-web.com
Reply-To: Paypal <service@paypal-web.com
Date: Tuesday, February 19, 2012
To: c[redacted]
Subject: Receipt of your payment

PayPal

Dear Customer,

This email confirms that you have paid PHONEDEPOTUSA (sales@phonedepotusa.com) $239.95 USD using PayPal.

This credit card transaction will appear on your bill as "PAYPAL PHONEDEPOT*".

PayPal Shopping Cart Contents

Item Name: New MOTOROLA V3 PINK RAZR RAZOR QUAD-BAND CELL PHONE
Quantity: 1
Total: $219.95 USD
Cart Subtotal: $219.95 USD
Shipping Charge: $20.00 USD
Cart Total: $230.05 USD

Shipping Information

Shipping info: Bill Chang
202 N Magnolia Dr.
Saco, ME 04072
United States
Address Status: Unconfirmed

If you haven't authorized this charge, click the link below to cancel the payment and get a full refound.

Dispute Transaction

Rysunek 2.2. PayPal jest często wykorzystywany w atakach phishingowych

Używanie komunikacji niewerbalnej w phishingu

Na pierwszy rzut oka może się wydawać, że nie da się używać komunikacji niewerbalnej w sytuacji, gdy porozumiewamy się wyłącznie za pomocą słowa pisanego. Przypomnij sobie jednak koncepcję ramowania, czyli struktury, na której zbudowany jest umysłowy i psychologiczny dom każdej osoby. Socjotechnik chce zmienić te ramy i sprawić, że jego cel zacznie myśleć, odczuwać i reagować w jego — socjotechnika — ramach. Nazywamy to łączeniem ram. Jedna osoba buduje „most" między własną ramą a ramą drugiej osoby, ułatwiając w ten sposób spotkanie się pośrodku albo znalezienie wspólnej płaszczyzny.

Jedną z podstawowych zasad ramowania jest to, że wszystkie słowa, których używamy, przywołują ramę. Nasze myśli mają postać obrazów, dlatego słowa kreują określone wizualne scenariusze. Obrazy te wywołują

emocjonalne reakcje — i to pod ich wpływem cel podejmuje działanie, które może mu służyć lub nie.

Nieetyczny socjotechnik, pisząc wiadomość, używa zbioru czynników wywołujących określone emocje, żeby skłonić cel do podjęcia pożądanego działania. Często w takich przypadkach wykorzystuje on emocje strachu (przed utratą, kradzieżą itd.) albo smutku (na przykład budząc współczucie bądź błagając o pomoc), aby wywołać reakcję, na której mu zależy.

Takie zdania jak: „Należy to wykonać w ciągu 24 godzin, w przeciwnym razie Twoje konto zostanie zawieszone" wywołują reakcję lękową. Jeśli połączysz ją z obawą, że Twoje konto mogło zostać wykorzystane bez Twojej wiedzy, otrzymasz doskonały przepis na reakcję wywołaną strachem. Jest ona oparta na słowach, które nakreśliły w Twojej głowie konkretny obraz, uruchamiający emocjonalną reakcję.

Innym aspektem jest wykorzystywanie emotikonów, które są coraz popularniejszymi elementami wiadomości tekstowych, e-maili i SMS-ów. Dr Audrey Nelson, autorka książki *The Gender Communication Handbook: Conquering Conversational Collisions Between Men and Women* opowiada o emotikonach wykorzystywanych w komunikacji pisemnej. Definiuje ona emotikony jako „niewerbalne pisemne wskaźniki emocji".

Która z poniższych wiadomości złagodzi reakcję odbiorcy?

- O, nie! Naprawdę tego nie przemyślałeś!
- O, nie! Naprawdę tego nie przemyślałeś! ☹
- O, nie! Naprawdę tego nie przemyślałeś! ☺

Użycie uśmiechniętej buźki w trzecim przykładzie sugeruje, że poprzedzające ją zdanie nie powinno zostać odebrane jako krytyka, lecz jako żart. Emocja, którą przekazujemy odbiorcy, może wpłynąć na to, jak zareaguje on na naszą wiadomość. Emotikony nie są raczej używane w tych e-mailach, których głównym zadaniem jest wzbudzenie strachu, ale są popularne w e-mailach phishingowych udających wiadomości od znajomych (na przykład e-mail od znajomego z Facebooka) albo od potencjalnych partnerów (na przykład wiadomości z popularnych portali randkowych). W tych scenariuszach używa się emotikonów, aby zaprezentować nadawcę jako osobę radosną, przyjazną i otwartą.

Kiedy telefon jest bardziej niebezpieczny niż złośliwe oprogramowanie

Drugą pod względem popularności formą socjotechniki jest stosowanie wzbudzania w rozmowach telefonicznych. W ciągu ostatnich 18 – 24 miesięcy ataki haktywistów (hakerów używających komputerów do prowadzenia akcji politycznych i społecznych) na duże przedsiębiorstwa coraz częściej były oparte na metodzie wzbudzania przez telefon. W jednym z takich przypadków grupa hackerów UG-NAZI zaatakowała firmę fakturującą, która prowadziła działalność w internecie. UG-NAZI zebrali bardzo dużo informacji na temat administratora bazy danych tej firmy, a potem wykonali jeden telefon do firmy odpowiedzialnej za wsparcie techniczne, prosząc o zresetowanie hasła. Dzięki temu, że grupa posiadała przeróżne informacje dotyczące administratora, zdołała odpowiedzieć na pytania zabezpieczające i doprowadzić do zmiany hasła na nowe.

Co było dalej? UG-NAZI pobrali gigabajty danych z numerami kart kredytowych klientów, a potem dla zabawy zlikwidowali swoje serwery. A to jest tylko jedna z dziesiątek podobnych historii, które miały miejsce w ostatnim czasie.

Dlaczego liczba ataków przez telefon wzrosła? Po pierwsze podszywanie się pod określony numer dzwoniący (nazywane spoofingiem informacji dzwoniącego) jest tanie i proste. Spoofing, czyli udawanie, że dzwonisz z innego numeru niż w rzeczywistości, umożliwia socjotechnikowi podszycie się pod dowolny numer. Odbiorca może pomyśleć, że dzwoni do niego ktoś ze wsparcia technicznego, dostawca, a nawet prezydent Stanów Zjednoczonych. Spoofing informacji dzwoniącego to metoda, która pozwala na szybkie stworzenie atmosfery zaufania, ponieważ wyświetlony numer jest „dowodem" świadczącym o wiarygodności dzwoniącego.

A po drugie tak jest łatwiej. Socjotechnik nie musi być blisko — ani nawet znajdować się w tym samym kraju — żeby wykorzystać telefon do wyłudzenia określonych informacji. Wystarczy odrobina praktyki, aby stworzyć wiarygodną historię i wzbudzić zaufanie odbiorcy.

Podczas jednego ze zleceń przeprowadziłem atak składający się z trzech etapów. Najpierw przeprowadziłem atak phishingowy — wysłałem e-maile do pracowników firmy będącej celem ataku, oferując im darmowego iPhone'a 5

(w tamtym czasie był to najnowszy model). Aby wziąć udział w losowaniu nagrody, trzeba było wypełnić formularz, podając dane do logowania w domenie firmy. Setki pracowników wypełniły ten formularz.

Na drugim etapie dzwoniłem do tych osób i informowałem je, że padły ofiarami ataku phishingowego. Powiedziałem, że zainstalowaliśmy na ich urządzeniu nadajnik, a jego usunięcie wymaga uruchomienia pliku wykonywalnego. W rzeczywistości nie było to narzędzie czyszczące, lecz szkodliwy plik, który dawał nam zdalny dostęp do ich komputerów. Spośród odbiorców wszystkich telefonów, jakie wykonałem tamtego dnia, jakieś 98 procent spełniło moją prośbę, nie pytając nawet, kim jestem. A tym nielicznym, którzy zapytali, odpowiedziałem po prostu, że jestem pracownikiem działu technicznego i że musimy działać szybko.

W latach 60. XX wieku psycholog Stanley Milgram przeprowadził eksperyment, żeby sprawdzić skłonność ludzi do słuchania autorytetów nawet wtedy, gdy polecenie było sprzeczne z ich zasadami moralnymi. Uczestników badania poproszono, żeby obserwowali osobę odpowiadającą na pytania i włączali wstrząs elektryczny za każdym razem, gdy udzieli ona złej odpowiedzi. Uczestnicy mieli świadomość rosnącego dyskomfortu u osób rażonych prądem. Widzieli, że odczuwają one coraz większy ból. Ci, którzy grali rolę naukowców, mówili wtedy: „Nie możemy przerwać tego eksperymentu. Proszę kontynuować".

Podobnie jak we wspomnianym eksperymencie badającym posłuszeństwo wobec autorytetów, ja również wygłaszałem tylko krótkie komunikaty w stylu: „Musimy wyczyścić system" i „Jeśli tego nie zrobimy, narazimy sieć na jeszcze większe szkody". Kluczem do sukcesu było mówienie tego z pewnością siebie i posługiwanie się autorytetem.

Na tym etapie testu penetracji miałem już dowody na to, że system zabezpieczeń firmy ma poważne luki, ale wspólnie z zespołem chcieliśmy przeprowadzić jeszcze jeden test — wiedząc, że zdołaliśmy zainstalować złośliwe oprogramowanie na komputerach pracowników. Zadzwoniłem do wsparcia technicznego, podając się za pracownika, z którym rozmawiałem nieco wcześniej o uruchomieniu pliku wykonywalnego. Powiedziałem, że moje dane z wirtualnej sieci prywatnej zostały usunięte, i poprosiłem o ich ponowne podanie. Mając tę informację, zyskałbym dostęp do najbardziej chronionych części sieci.

Nasza rozmowa przebiegła mniej więcej tak:

— Wsparcie techniczne. Sylwia przy telefonie. W czym mogę pomóc?

Zastosowałem spoofing, zmieniając swój numer w taki sposób, aby wyglądał, jakby połączenie zostało wykonane z biura osoby, pod którą się podszywałem.

— Cześć, tu James. Właśnie zainstalowałem na swoim komputerze coś, czego nie powinienem. Przeprowadziłem skanowanie wirusów, żeby usunąć ten program, a przy okazji usunąłem również swoje dane do logowania w sieci VPN. Możesz mi je podać?

— Oczywiście, chętnie ci pomogę. Podaj mi swoje imię i nazwisko.

— James Smith. Możesz mi mówić Jim.

— Jim? Smith?

— Tak.

— Nie poznajesz mnie po głosie? Tu Sylvia.

Musiałem szybko coś wymyślić. Nie wiedziałem, jaka relacja łączyła tych dwoje, a jedna zła odpowiedź mogłaby mnie zdemaskować.

— Sylvio, przepraszam cię. Jestem taki zestresowany. Kliknąłem ten fałszywy link i zainstalowałem u siebie jakieś złośliwe oprogramowanie. Kiedy próbowałem to naprawić, narobiłem jeszcze większego bałaganu. Już mi głowa od tego pęka. Do tego łapie mnie przeziębienie i chyba dlatego mam trochę inny głos. A teraz jeszcze straciłem swoje dane do logowania. Przepraszam cię. Możesz mi pomóc?

— Pewnie, żaden problem. Zaraz poszukam twoich danych.

Kilka sekund później miałem już w rękach klucze do królestwa. Dlaczego moja metoda okazała się tak skuteczna? Nie musiałem udowadniać, kim jestem, bo dzwoniłem z odpowiedniego numeru, użyłem odpowiedniego nazwiska i miałem odpowiednią wymówkę. Byłem zbyt wiarygodny, żeby wzbudzić jakiekolwiek wątpliwości.

Używanie komunikacji niewerbalnej w wyłudzaniu informacji przez telefon

Kiedy się uśmiechasz, Twój głos brzmi radośnie. Według Scharlemanna, Eckela, Kacelnika i Wilsona (2001) uśmiech sprawia, że bardziej ufamy innym, a oni bardziej ufają nam. To prawda: nawet gdy nie można zobaczyć naszego uśmiechu, można go poczuć. Badacze ci przeprowadzili eksperyment o nazwie „Wartość uśmiechu: teoria gier w odniesieniu do twarzy człowieka",

który przyniósł następujący wniosek: „Uśmiech zwiększa poziom zaufania w relacjach między nieznajomymi. Badani, oglądając zdjęcia różnych osób, chętniej obdarzali zaufaniem daną osobę wtedy, gdy się uśmiechała, niż gdy była poważna" (str. 13).

Nie tylko uśmiech wpływa na to, jak osoba po drugiej stronie słuchawki będzie postrzegać nas i naszą historię. Równie ważne są: postawa, gesty, ton i wysokość głosu, a także to, czy mówimy głośno, czy cicho. Wszystkie te cechy są aspektami komunikacji niewerbalnej i zwiększają naszą zdolność do wpływania na osoby, które są naszymi celami.

Kiedy podczas wspomnianego trzyetapowego ataku udawałem przedstawiciela wsparcia technicznego, ważne było, aby ton mojego głosu sugerował autorytet, dlatego nie można było wyczuć w nim zdenerwowania. Mimo że cel nie mógł widzieć mojej twarzy, mógł on „usłyszeć" mój uśmiech, który ułatwił mi zbudowanie zaufania. Także moja postawa sugerowała autorytet i kontrolę nad sytuacją.

Na trzecim etapie, kiedy wcieliłem się w pracownika dzwoniącego do wsparcia technicznego, musiałem się zmienić: aby mój pretekst był wiarygodny, moja twarz musiała pokazywać, że jestem wystraszony, a natężenie mojego głosu, a także ton, wysokość oraz tempo mówienia musiały być niższe, wolniejsze. W sposób niewerbalny przekazywałem komunikat: „Przepraszam. Spieprzyłem sprawę. Pomóż mi, proszę". Ponieważ dostosowałem swoją mimikę tak, aby pasowała do emocji, które odczuwała udawana przeze mnie osoba, mój pretekst był silniejszy.

Niektórzy twierdzą nawet, że na nasz ton podczas rozmowy telefonicznej może wpływać to, jak siedzimy i jak się ubieramy. W 34. newsletterze strony *social-engineer.org* (*http://www.social-engineer.org/newsletter/Social-Engineer.Org%20Newsletter%20Vol.%2003%20Iss.%2034.html*) opisałem eksperyment dotyczący „ubranego poznania" przeprowadzony przez badaczy Adama i Galinsky'ego. Doszli oni do wniosku, że nasze postrzeganie ubrania wpływa na to, jak wykonujemy określone zadania i jak zabieramy się do pracy, którą nam zlecono.

Badanie to jest kolejnym dowodem na to, że ton głosu i to, jak brzmimy w rozmowie z naszymi celami, zależą od tego, w co jesteśmy ubrani, jakie niewerbalne komunikaty przekazujemy, a także od wielu innych czynników. Powtórzę to, co już napisałem wcześniej: ten sam element ubrania, który otrzymał dwa różne „znaczenia", stworzył psychologiczny most, który sprawił,

że uczestnicy badania zachowywali się w określony sposób. A to oznacza, że strój, jaki mam na sobie podczas wykonywania określonych zleceń, wpływa na to, jak się będę zachowywać.

Nie jestem socjotechnikiem, którego szukasz

W czasach przed epoką telefonów i internetu oszustwa wymagały kontaktu osobistego. Od Victora Lustiga, który dwa razy „sprzedał" wieżę Eiffla, po zwykłe codzienne uliczne kradzieże, ludzie od zawsze stosowali osobiste formy inżynierii społecznej.

Ostatnio wciąż słyszymy historie o przestępcach, którzy wcielili się w kogoś innego, żeby skłonić swoje ofiary do zrobienia czegoś, czego nie powinny robić. Oto przykład: w Stanach Zjednoczonych mężczyzna namówił kilku kumpli, żeby napadli na bank. Tuż przed napadem wszedł do banku, udając klienta. Kiedy jego koledzy zaczęli okradać bank, ujawnił się jako agent federalny działający pod przykrywką, po czym natychmiast zareagował i „uratował" całą sytuację. „Aresztował" rabusiów i zabrał pieniądze, twierdząc, że stanowią one dowód przestępstwa. Kiedy opuszczał bank razem z przestępcami skutymi kajdankami i z torbami gotówki w rękach, pracownicy banku czuli się bezpieczni i uratowani. Ale żaden radiowóz nie nadjechał.

Dlaczego takie ataki są skuteczne? Wcielenie się w określoną osobę ułatwia zdobycie zaufania. Kiedy ktoś pokazuje plakietkę z nazwiskiem; ma charakterystyczny strój; a także mówi, zachowuje się i działa tak, jak osoba, za którą się podaje, nasze umysły dostają odpowiedzi na pytania, których nawet nie zdążyły zadać:

- „Kim jest ta osoba?",
- „Jakie ma dowody na potwierdzenie tego, co mówi?",
- „Czy jestem bezpieczny(-a)?".

Cel otrzymuje odpowiedzi na te pytania, dzięki czemu jego umysł się uspokaja. Na tym polega moc podszywania się. W historii, którą opisałem na początku rozdziału — dotyczącej włamania się do magazynu — nie musiałem wokalizować tych szczegółów, bo mój strój mówił za mnie. Musiałem tylko odpowiedzieć na dodatkowe pytania: „Czego chcesz?" i „Dlaczego tu jesteś?".

Kiedy cel otrzymał swoje odpowiedzi, resztę pracy wykonał mój pretekst. Oprócz fizycznego podszywania się, osobiste ataki socjotechniczne pozwalają na wykorzystanie szerokiej gamy technik, z których trudno byłoby korzystać w przypadku innych form ataku. Na przykład wiele firewalli i innych narzędzi zatrzymuje załączniki z rozszerzeniem PDF i EXE, nie wpuszczając ich do skrzynki odbiorczej i uniemożliwiając otwarcie tych plików. Jeżeli jednak takie same pliki zostaną zapisane na nośniku USB, można je zainstalować na urządzeniu pracownika i tam je uruchomić, a ryzyko, że ktokolwiek będzie próbował nas powstrzymać, jest dużo mniejsze.

Wiele razy udało mi się podrzucić w wybranej firmie nośnik USB albo płytę DVD z opisem „poufne", „premia dla pracowników" albo (niestety) „prywatne zdjęcia", żeby wzbudzić ciekawość mojego celu. Wystarczyło, że podłączył nośnik albo włożył płytę, żeby jego komputer został zainfekowany.

Niesławny atak wykorzystujący robaka komputerowego o nazwie Stuxnet, a także niedawna próba ataku na holenderską firmę chemiczną DSM pokazują, że ataki przy użyciu pendrive'a wciąż są popularne. Element ciekawości w połączeniu ze złośliwym oprogramowaniem może stworzyć bardzo niebezpieczną mieszankę.

Używanie komunikacji niewerbalnej w podszywaniu się

To, że komunikacja niewerbalna jest wykorzystywana podczas podszywania się, może się wydawać oczywiste, ale bardzo ważne jest, aby to dobrze zrozumieć. Ponieważ w atakach wykorzystujących podszywanie się dochodzi do osobistego kontaktu, komunikacja niewerbalna ma największy wpływ na cel.

To naturalne, że się denerwujesz albo jesteś wystraszony, kiedy się boisz, że zostaniesz przyłapany. Jeżeli Twoim pretekstem jest autorytet, nerwy i strach mogą zniszczyć niewerbalne powiązanie, które mówi: „Jestem pewny siebie".

Dokładniej omówię to w rozdziale 8., w którym skupię się na niewerbalnych aspektach wzbudzania. Jeżeli socjotechnik robi miny wyrażające gniew, smutek i strach, takie same stany emocjonalne zostaną odzwierciedlone w mózgu jego celu.

Zrozumienie, w jaki sposób komunikacja niewerbalna może wpływać na osoby będące Twoimi celami, jest niezbędne — nie tylko po to, abyś umiał rozpoznać różne niewerbalne znaki, ale też po to, aby kontrolować sygnały, które sam wysyłasz. Oto przykład: wiedząc, że trzymanie rąk w kieszeni może

być postrzegane jako oznaka słabości, możesz albo ten gest wykonać — jeżeli Twój pretekst ma okazywać uległość — albo go unikać, jeśli Twój pretekst reprezentuje jakąś władzę.

Czasami socjotechnik, stosując metodę podszywania się, może polegać wyłącznie na komunikacji niewerbalnej. Dzieje się tak często podczas prób przejścia przez *śluzę*, kiedy ktoś, kto nie ma dostępu do określonego miejsca, zdobywa go, naśladując pracowników, którzy ten dostęp mają. Można to zrobić na kilka sposobów:

- **Palarnie dla pracowników.** Miejsca te, zazwyczaj zlokalizowane za budynkiem, często nie są ściśle chronione, dzięki czemu pracownicy mogą bez większych trudności wychodzić z budynku i do niego wracać. Socjotechnik może dołączyć z zewnątrz do „plemienia" palaczy, a potem spróbować wejść do budynku razem z nimi.
- **Wniesienie pudła albo dużego przedmiotu.** Nie zliczę, ile razy wszedłem do jakiegoś budynku tylko dlatego, że niosłem w rękach jakiś karton. Kiedy podchodziłem do drzwi i zaczynałem się z nimi szarpać, żeby je otworzyć, zwykle podchodził do mnie jakiś pomocny pracownik i pomagał mi wejść. A jeśli duże pudło niesie drobna, atrakcyjna kobieta, mężczyźni będą walczyć ze sobą o to, kto przytrzyma jej drzwi.
- **Fałszywy identyfikator.** Inną skuteczną metodą, której dodatkową korzyścią jest wzbudzenie zaufania, jest fałszywy identyfikator. Socjotechnik przygotowuje sobie realistycznie wyglądającą plakietkę, która, rzecz jasna, nie otworzy mu drzwi do budynku. Po kilku nieskutecznych próbach przyłożenia karty do czytnika jakiś życzliwy pracownik postanowi mu pomóc i wpuści go do środka.

To tylko kilka sposobów na podszycie się, w których socjotechnik mówi niewiele albo nawet wcale się nie odzywa, dlatego musi całkowicie polegać na swoich umiejętnościach z zakresu komunikacji niewerbalnej. Każdy człowiek posiada wewnętrzny radar, który włącza się, kiedy coś jest nie tak, a działanie tego radaru jest uzależnione od tego, jakie uczucia wywołuje w nas komunikacja niewerbalna drugiej osoby. Dlatego socjotechnik musi mieć dobrze rozwiniętą umiejętność kontrolowania i wykorzystywania tych znaków, dzięki której będzie on w stanie wywoływać odpowiednie „przeczucie".

Używanie umiejętności socjotechnicznych

Umiejętności socjotechniczne nie zawsze muszą być wykorzystywane do złych celów; mogą również pełnić użyteczne funkcje. Pokrótce omówię ten temat, żeby nadać właściwy kontekst temu, co przeczytasz w dalszej części tej książki. Na początku powtórzę, że moją definicją inżynierii społecznej jest dowolne działanie, które skłania drugą osobę do zrobienia czegoś, co może leżeć w jej interesie lub nie.

Dobre

Łatwo zrozumieć, czym jest pozytywna inżynieria społeczna. Załóżmy, że dziecko chce czegoś od swoich rodziców. Podchodzi do mamy i pyta:

— Mamo, kupicie mi nową lalkę Barbie?

Mama odpowiada:

— Nie wiem. Zapytaj tatę.

Dziewczynka idzie do taty, który siedzi na kanapie. Przytula się do niego i mówi:

— Mama powiedziała, że kupicie mi nową lalkę Barbie, jeśli się zgodzisz. Zgódź się, tatusiu, proooooszę!

— Oczywiście, kochanie — odpowiada tata, patrząc w piękne, duże oczy swojej córeczki.

Co tutaj się wydarzyło? Mała dziewczynka, która kompletnie nie zna się na psychologii, komunikacji niewerbalnej czy modelowaniu komunikacji, zastosowała wszystkie skuteczne techniki.

Z mojego doświadczenia wynika, że pierwsza prośba do mamy zazwyczaj jest kierowana po zrobieniu jakiegoś dobrego uczynku albo po chwili emocjonalnej bliskości — w sytuacji, gdy organizm produkuje duże ilości hormonów miłości i zaufania. Jednak prawdziwa socjotechnika pojawia się podczas rozmowy z tatą.

Najpierw mamy potęgę dotyku. Kiedy dziewczynka zbliża się do taty i przytula się do niego, tworzy z nim emocjonalną więź. Potem, zaczynając od podstawowej techniki „mama już się zgodziła", wykorzystuje dowód społeczny. Z tego połączenia rodzi się niepowstrzymana siła, dzięki której dziewczynka dostaje to, czego chce.

Innymi, poważniejszymi przykładami stosowania socjotechniki w dobrym celu są rehabilitacja i terapia, gdzie pacjenci podlegają przeramowaniu i zmieniają swój system wartości. Analizują własne przekonania, a potem świadomie wybierają inną ścieżkę. Można więc powiedzieć, że inni ludzie wpływają na nich, żeby zrobili coś, co pomoże im zerwać z negatywnym myśleniem, przestać nadużywać alkoholu lub narkotyków albo odciąć się od innych zachowań, które powodują różnego rodzaju nadużycia.

Socjotechniki można używać, żeby skłonić kogoś do podjęcia działań, które są dla niego dobre. Można ją wykorzystać, żeby przeramować myślenie drugiej osoby, stworzyć atmosferę sprzyjającą rozwojowi, a także pomóc w zerwaniu ze złymi nawykami.

Jedno z moich dzieci miało taki okres, że nie chciało jeść śniadania. Wiedziałem, o co chodzi — to była próba siły. Mój syn chciał przejąć kontrolę nad tym aspektem swojego życia. To nie był bunt ani sprzeciwianie się rodzicom. Wiedząc, że tym, co kierowało moim dzieckiem, była potrzeba samodzielnego dokonywania wyborów — pragnienie, abyśmy mu na to pozwolili — któregoś ranka po prostu powiedziałem: „Wiem, że masz problem ze śniadaniem przed szkołą, więc decyzja należy do ciebie. Chcesz płatki czy jajka?".

Synek z radością wybrał jedną z możliwości, ponieważ dało mu to poczucie kontroli. Ostatecznie więc każdy z nas był wygrany. Ja się cieszyłem, że moje dziecko je, a ono się cieszyło, że ma władzę, jaką dała mu możliwość wyboru. Jest to pozytywny przykład zastosowania socjotechniki, ponieważ jej celem jest to, żeby obie strony były wygrane. W takiej interakcji nie ma przegranego, a wszyscy są zadowoleni ze zmiany, która nastąpiła na skutek podjętych działań.

Złe

Umiejętności, o których przed chwilą wspomniałem, mogą być również wykorzystywane przez nieetycznych socjotechników. Podstawową różnicą między „dobrym" a „złym" jest intencja. W tym drugim przypadku socjotechnik nie chce Ci pomóc ani wprowadzić pozytywnej zmiany w Twoim życiu — zależy mu tylko na tym, żeby samemu coś zyskać.

18 marca 1990 roku ktoś zapukał do bocznych drzwi Gardner Museum. Były zamknięte i nie wolno było ich otwierać, ale pukali do nich umundurowani policjanci. Ochroniarz otworzył drzwi i wpuścił ich do środka; zaraz potem się przekonał, że to wcale nie była policja. Nie używając żadnej broni, mężczyźni obezwładnili dwóch ochroniarzy muzeum, związali ich i w ciągu niespełna 90 minut ukradli 13 dzieł sztuki wartych 300 – 500 milionów dolarów.

Podczas tego rabunku użyto zasad wpływu i autorytetu. Wszyscy wiemy, że należy słuchać autorytetów, zwłaszcza policji. Złodzieje wykorzystali ten fakt, żeby ukraść dzieła warte ponad 300 milionów dolarów.

Z kolei w Antwerpii w 2003 roku ukradziono drogie diamenty. Leonardo Notarbartolo przez trzy lata wynajmował powierzchnię w biurowcu, w którym znajdowało się duże Centrum Diamentów — w ten sposób zbudował swoją wiarygodność i nawiązał relacje z odpowiednimi osobami. Razem z kumplami zaplanował atak, w którym udawali handlarzy diamentami. Włamali się do sejfu chronionego przez wielu ochroniarzy i zabrali z niego szlachetne kamienie warte ponad 100 milionów dolarów. Co ciekawe, zostali złapani, bo jeden z pięciu członków ekipy zapomniał spalić torbę ze śmieciami, która zawierała dowody przestępstwa.

Ataki hakerskie, takie jak te na HBGary Federal, stronę internetową PBS czy Coca-Colę, zaczęły się od wiadomości phishingowej. Inne operacje, takie jak Night Dragon i Stuxnet, mogły obejmować rozmowy telefoniczne i wyspecjalizowany sprzęt komputerowy. Wszędzie użyto umiejętności socjotechnicznych (albo wręcz się na nich skoncentrowano) i to one zapewniły przestępcom sukces. Zarówno wyrafinowane ataki na korporacje, jak i codzienne przekręty (takie jak metoda „na wnuczka", w której ktoś dzwoni do dziadków, udając ich wnuka, i prosi ich o pieniądze) wiążą się z wykorzystywaniem tych umiejętności. Oba rodzaje oszustw wymagają planowania, zdobycia potrzebnych informacji oraz dużej ilości komunikacji niewerbalnej.

Brzydkie

Niestety to prawda: w kontekście wykorzystywania umiejętności socjotechnicznych istnieje jeszcze jeden poziom, który jest gorszy od „złego". Nie będę go tu szczegółowo omawiał, bo to nie jest mój obszar specjalizacji. Niedawno miałem okazję przeprowadzić wywiad z Mary Ellen O'Toole, byłą

agentką FBI i psycholożką. Rozmawialiśmy o tym, w jaki sposób psychopaci wykorzystują swoje umiejętności z dziedziny inżynierii społecznej. Mary podała kilka przykładów z własnej pracy, a także parę innych, w których umiejętności socjotechniczne wykorzystano z tragicznymi skutkami. Weźmy na przykład Teda Bundy'ego, który w latach 70. XX wieku przez ponad cztery lata terroryzował kobiety i w końcu przyznał się do ponad 30 zabójstw. Planując swoje zbrodnie, wykorzystywał umiejętności socjotechniczne. W wielu swoich atakach podawał się za policjanta — czyli używał autorytetu. Jego najskuteczniejszą metodą było udawanie, że jest ranny: chodził o kulach albo z założonym gipsem i prosił o pomoc, szybko zjednując sobie sympatię swoich celów. Jego ofiary współczuły mu i chciały mu pomóc. Niestety w większości przypadków przypłaciły to własnym życiem.

Jak już napisałem wcześniej, nie chcę rozwodzić się na ten temat, ale pragnę zwrócić uwagę na jedną rzecz: analiza wszystkich trzech poziomów wykazała, że wszędzie wykorzystuje się te same zestawy umiejętności. Bez względu na to, czy mamy do czynienia z dobrą, złą czy brzydką formą używania socjotechniki, zawsze wygląda ona tak samo. Różni je tylko jedna ważna rzecz: intencja.

Podsumowanie

Pozwól, że w podsumowaniu powtórzę definicję socjotechniki: „Dowolne działanie, które skłania drugą osobę do zrobienia czegoś, co może leżeć w jej interesie lub nie". Wiedza na temat tego, jak ludzie wykorzystują komunikację niewerbalną — czy to w e-mailach, w rozmowach telefonicznych czy w kontaktach osobistych — nie tylko przydaje się wtedy, gdy chcesz udoskonalić własne umiejętności komunikacji, ale też pomaga dbać o swoje bezpieczeństwo.

Poszerzanie wiedzy na temat inżynierii społecznej i uświadomienie sobie, że mamy z nią do czynienia każdego dnia, ponieważ jest ona elementem wszystkich interakcji międzyludzkich, jest przyjemne i ekscytujące. Dzięki temu komunikacja staje się interesującym doświadczeniem, a jednocześnie polem do nauki.

Przechodząc do następnych rozdziałów, chcę zaznaczyć, że ta książka nie obejmuje wszystkich zagadnień z dziedziny inżynierii społecznej. Jej celem jest to, aby Ci pomóc — bez względu na to, czy jesteś specjalistą od bezpieczeństwa, nauczycielem, rodzicem, dyrektorem generalnym, czy terapeutą — w lepszym zrozumieniu najpopularniejszych komunikatów niewerbalnych.

W każdym z następnych rozdziałów opiszę określoną część ciała oraz niewerbalne komunikaty, które ona wysyła. W następnym rozdziale zajmę się jedną z najbardziej komunikatywnych części ciała: dłońmi. Co mówią nasze dłonie — celowo i nieświadomie? Jak można czytać język dłoni? I wreszcie, jak możesz wykorzystać swoje dłonie do tego, by wpływać na emocje innych ludzi?

Na wszystkie te pytania odpowiem w rozdziale 3.

SOCJOTECHNIKA: TAM, GDZIE LUDZKIE CECHY SĄ NAJSŁABSZYM OGNIWEM!

Człowiek jest istotą społeczną. To zrozumiałe, że każda część ciała informuje o emocjach danej osoby. Umiejętność świadomego korzystania z komunikacji niewerbalnej pomaga w zrozumieniu odczuć rozmówcy. Pomaga też w dostrzeżeniu dyskomfortu, a nawet zauważeniu ukrywanych emocji, takich jak gniew, radość, strach czy smutek. Zdolność do rozpoznawania tych oznak i ich prawidłowa interpretacja z pewnością poprawiają komfort komunikacji, jednak znaczenie tej umiejętności jest o wiele większe: socjotechnika stanowi nieodzowny element działania hakerów, przestępców czy służb specjalnych. Korzystanie z wiedzy socjotechnicznej i jej zdobyczy pozwala zachować kontrolę w każdej sytuacji, gdy mamy do czynienia z komunikowaniem się ludzi ze sobą.

Dzięki tej książce udoskonalisz swoje umiejętności komunikacyjne: nauczysz się odczytywać niewerbalne wskazówki i samemu prezentować niewerbalne wzmocnienia. Z jednej strony zaczniesz lepiej rozumieć przekaz innych ludzi, z drugiej — sprawisz, że rozmówcy zaczną cenić komunikowanie się z Tobą. Szybko zauważysz, jaka to cenna umiejętność: jako specjalista do spraw bezpieczeństwa będziesz skuteczniej edukować współpracowników i zwalczać cyberataki. Jako osoba działająca publicznie łatwiej przekonasz ludzi do swoich idei. Dowiesz się, jak naukowe zdobycze socjotechniki mogą być wykorzystywane do różnych celów: dobrych, złych czy po prostu brzydkich. Wiedza zdobyta dzięki tej lekturze oraz odrobina krytycznego myślenia staną się Twoim najlepszym zabezpieczeniem.

W tej książce między innymi:

- prawdziwa wiedza o mowie ciała i ekspresji mimicznej człowieka
- metody zdobywania zaufania wykorzystywane do nieetycznych celów
- tajniki warsztatu „hakera umysłów”
- czynnik ludzki jako zagrożenie bezpieczeństwa systemu informatycznego
- neutralizowanie zagrożenia ze strony nieetycznych socjotechników

Christopher Hadnagy jest zawodowym socjotechnikiem i prezesem firmy Social Engineer LLC. Współtworzył pierwszy serwis poświęcony inżynierii społecznej (*www.social-engineer.org*). Jest cenionym mówcą i trenerem, często występuje jako prelegent na konferencjach, takich jak RSA, Black Hat i DEF CON. Autor bestsellera *Socjotechnika. Sztuka zdobywania władzy nad umysłami*.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
Sprawdź nasze szkolenia!
SZKOLENIA
AKADEMIA IT & BUSINESS
HELIONSZKOLENIA.PL
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-6948-1
9 788328 369481
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 49,00 zł
onepress