

Autor Max Paradox

SERIA BRUTALNA PRAWDA

Brutalna prawda o oszustwach internetowych

Nie dałeś się nabrać. Ktoś po prostu
lepiej znał twoje odruchy



SPIS TREŚCI

INTRO.....	3
Rozdział 1 - Masz pięć minut, żeby przestać myśleć.....	13
Rozdział 2 - Człowiek z banku brzmi jak człowiek z banku.	22
Rozdział 3 - To przecież wygląda normalnie.....	32
Rozdział 4 - Skoro już wpłaciłeś tysiąc, szkoda stracić wszystko.....	40
Rozdział 5 - Najpierw chciałeś, żeby to było prawdziwe.....	48
Rozdział 6 - Skoro oni wszyscy to robią.....	56
Rozdział 7 - Najbardziej podejrzany jest ten, kto niczego od ciebie nie chce.....	65
Rozdział 8 - Przecież powiedział coś, czego nikt obcy nie mógł wiedzieć.....	73
Rozdział 9 - Kliknąłeś, zanim zdążyłeś być ostrożny.....	81
Rozdział 10 - Teraz ktoś obiecuje odzyskać to, co ukradli. .	89
Rozdział 11 - Nie chciałeś wyjść na chama, więc podałeś dane.....	98
Rozdział 12 - Wstyd jest tańszym zabezpieczeniem niż hasło	106
Rozdział 13 - Najpierw ukradli ci pieniądze, potem nazwali cię idiotą.....	115
Rozdział 14 - Bałeś się stracić dostęp bardziej niż pieniądze	123
Rozdział 15 - Nie oszukali cię technologią, tylko tym, że chciałeś skończyć sprawę.....	131
Rozdział 16 - Uwierzyłeś, bo historia była o tobie.....	138

Rozdział 17 - Najpierw sprawili, że poczułeś się wybrany.	146
Rozdział 18 - Najłatwiej oszukać człowieka, który właśnie udowadnia, że nie jest naiwny.....	154
Rozdział 19 - Kiedy przestałeś ufać oszustomi, zacząłeś nie ufać wszystkim.....	162
Rozdział 20 - Nie dałeś się nabrać. Ktoś po prostu lepiej znał twoje odruchy.....	170

INTRO

Telefon zawibrował o 10:43, kiedy stałeś przy kasie w sklepie i próbowałeś jednocześnie zapłacić, schować kartę do portfela i nie przytrzasnąć reklamówką rękawa kurtki. Wiadomość wyglądała dokładnie tak, jak powinna wyglądać wiadomość, której nie masz ochoty czytać, ale której nie możesz zignorować. „Twoja przesyłka została wstrzymana. Dopłać 1,49 zł, aby uniknąć zwrotu.” Nie czekałeś przecież na żaden dramat, tylko na paczkę. Coś z Allegro, może kosmetyki, może kabel, może kolejny przedmiot, który dwa dni wcześniej wydawał się niezbędny do uporządkowania życia. Kwota była śmieszna, komunikat znajomy, pośpiech prawdziwy. Kliknięcie nie wyglądało jak decyzja finansowa. Wyglądało jak drobna czynność administracyjna pomiędzy terminalem płatniczym a pytaniem kasjerki, czy potrzebujesz paragon. I właśnie dlatego było tak skuteczne. Nikt nie próbował przekonać cię, że wygrałeś milion dolarów w loterii organizowanej przez księcia z egzotycznego kraju. Ktoś po prostu stworzył sytuację, w której przez kilkanaście sekund zachowywałeś się dokładnie tak, jak zachowujesz się każdego dnia.

Kilka godzin później historia wygląda już inaczej. Siedzisz przed ekranem bankowości elektronicznej, odświeżasz listę operacji i próbujesz ustalić moment, w którym człowiek rozsądny zamienił się w człowieka klikającego podejrzany link z SMS-a. Najłatwiej byłoby uznać, że wydarzyło się coś wyjątkowego, jakaś chwilowa utrata inteligencji, niedostatek koncentracji albo kompromitujący błąd, którego normalnie nigdy byś nie popełnił. Taka wersja jest bolesna, ale pocieszająca, ponieważ sugeruje jednorazową awarię systemu. Tymczasem oszustwo internetowe rzadko

potrzebuje awarii. Znacznie częściej potrzebuje twojej normalności. Potrzebuje tego, że spodziewasz się paczek, odbierasz telefony, logujesz się do banku, znasz ludzi, martwisz się o pieniądze, boisz się problemów i lubisz załatwiać drobne sprawy od razu, żeby nie wisały nad głową. Oszust nie musi stworzyć nowego człowieka. Wystarczy, że przez chwilę wykorzysta tego, którym już jesteś.

Lubimy wyobrażać sobie oszusta internetowego jako cyfrowego drapieżnika siedzącego w ciemnym pokoju, otoczonego monitorami, kodem i technologią, której przeciętny użytkownik nie rozumie. Taki obraz jest wygodny, bo ustawia konflikt w prosty sposób: po jednej stronie zwykły człowiek, po drugiej stronie ekspert posiadający niemal nadprzyrodzoną wiedzę techniczną. Tyle że wiele skutecznych oszustw nie wymaga szczególnie wyrafinowanej technologii. Wymagają znacznie starszego wynalazku: człowieka przewidywalnego. Formularz może być prymitywny, strona niedoskonała, język momentami podejrzany, a mimo to mechanizm działa, ponieważ nie sprzedaje ci technologicznej iluzji. Sprzedaje ci znajomą sytuację. Kurier potrzebuje dopłaty. Bank wykrył podejrzaną aktywność. Syn stracił telefon. Koleżanka prosi o kod. Urząd musi potwierdzić dane. Pracownik działu bezpieczeństwa chce zabezpieczyć konto. Każda z tych historii brzmi banalnie. I właśnie banalność jest jej najdroższym elementem.

Nie klikamy dlatego, że wierzymy we wszystko. Klikamy dlatego, że większości drobnych komunikatów w ciągu dnia nie analizujemy jak śledczy. Gdybyś przed każdym SMS-em zatrzymywał się na dziesięć minut, sprawdzał domenę, konsultował treść z trzema źródłami i wykonywał analizę ryzyka, prawdopodobnie nie zostałbyś oszukany, ale również nie zdążyłbyś zrobić niczego poza sprawdzaniem

wiadomości. Codziennosc działa dzięki automatyzmom. Wiesz, gdzie kliknac „zaplac”. Wiesz, jak wyglada przycisk „zaloguj”. Wiesz, ze czerwony komunikat oznacza klopot, zielony potwierdzenie, a zegar odliczajacy czas sugeruje, ze nalezy sie pospieszyc. Nie zastanawiasz sie nad kazdym z tych elementow, poniewaz wlasnie po to nauczyles sie obslugiwac internet, zeby nie zastanawiac sie nad kazdym z nich. Paradoks jest wyjatkowo elegancki: im sprawniej poruszasz sie po cyfrowym swiecie, tym wiecej czynnosci wykonujesz automatycznie. A automatyzm, ktory normalnie oszczedza czas, w odpowiednio skonstruowanej sytuacji moze zaczac oszczedzac czas rowniez czlowiekowi, ktory wlasnie cie okrada.

- Oszustwo zaczyna sie czesto wtedy, kiedy komunikat nie wydaje sie wyjatkowy, lecz przeciwnie, jest wystarczajaco zwyczajny, zeby przelizgnac sie przez uwage bez uruchamiania pelnej kontroli.

- Najbardziej uzyteczna informacja o tobie nie musi byc numer dokumentu ani haslo, lecz wiedza, ze boisz sie utraty pieniedzy, reagujesz szybko na wiadomosci od bliskich albo nie znosisz niedokonczonych spraw.

- Skuteczna manipulacja nie zawsze polega na zmuszeniu cie do zrobienia czegoś nienaturalnego. Znacznie czesciej polega na ustawieniu sytuacji tak, zebyś zrobil cos calkowicie naturalnego w niewlasciwym miejscu.

Po oszustwie pojawia sie jednak potrzeba prostego wyjasnienia, poniewaz czlowiek wyjatkowo zle znosi historie, w ktorych jego wlasne zachowanie nie pasuje do obrazu siebie. „Przeciez ja nie jestem naiwny” brzmi wtedy bardziej jak obrona tozsamosci niz opis sytuacji. Mozesz miec wyzsze wyksztalcenie, zarzadzac zespolem, inwestowac pieniedze, konfigurowac router, rozpoznawac falszywe reklamy i od lat

tłumaczyć rodzicom, żeby nie klikali w dziwne linki. Możesz być nawet osobą, która kilka tygodni wcześniej z pobłażaniem opowiadała znajomym, że trzeba naprawdę nie uważać, żeby podać komuś kod BLIK. Potem telefon przychodzi w złym momencie, rozmówca zna twoje imię, numer wygląda znajomo, ton jest profesjonalny, a problem wymaga szybkiej decyzji. Nagle cała pewność siebie nie znika. Ona właśnie zostaje użyta. Człowiek przekonany, że dobrze rozpoznaje zagrożenia, nie analizuje każdej sytuacji od początku. Korzysta z własnego przekonania, że wie, jak wygląda oszustwo. Wystarczy więc przygotować takie, które wygląda trochę inaczej.

Wstyd po internetowym oszustwie jest szczególnym rodzajem wstydu, bo rzadko dotyczy wyłącznie straty pieniędzy. Uderza w obraz własnej kompetencji. Sto złotych można odrobić, tysiąc złotych można przeżyć, nawet większa strata po pewnym czasie staje się liczbą w historii rodzinnych katastrof finansowych. Znacznie trudniej przetrwać myśl, że ktoś obcy przewidział twoją reakcję lepiej, niż ty sam potrafiłeś ją skontrolować. Dlatego ofiary mówią czasem o szczegółach z obsesyjną precyzją. „Strona wyglądała identycznie.” „Numer naprawdę był podobny.” „On znał nazwę banku.” „Wiadomość przyszła akurat wtedy, kiedy czekałem na kuriera.” Każdy szczegół pełni funkcję obronną. Ma udowodnić, że sytuacja była niezwykle przekonująca, ponieważ alternatywa brzmi zbyt nieprzyjemnie: może nie trzeba było stworzyć idealnej pułapki, tylko wystarczająco dobrze trafić w moment, w którym działałeś szybciej, niż myślałeś.

Internet dodatkowo komplikuje sprawę, ponieważ nauczył nas traktować autentyczność jako zestaw znaków wizualnych. Logo wygląda znajomo. Kolory się zgadzają.

Formularz przypomina bank. Wiadomość ma stopkę. Profil posiada zdjęcie. Konto istnieje od kilku miesięcy. Strona ma opinie. Człowiek po drugiej stronie zna fachowe słowa. W cyfrowym środowisku większość relacji zaczyna się przecież od powierzchni, więc powierzchnia musiała zostać uznana za wystarczający dowód, żeby codzienność w ogóle działała. Nie możesz osobiście odwiedzać siedziby każdej firmy, której płacisz przez internet. Nie możesz weryfikować dowodu osobistego każdego sprzedawcy. Nie możesz przeprowadzać przesłuchania człowieka, który pisze do ciebie z konta znajomego. Zaufanie zostało skompresowane do kilku sygnałów, a oszustwa internetowe rozwijają się właśnie w przestrzeni pomiędzy sygnałem a rzeczywistością. Człowiek widzi znajome elementy i dopowiada resztę, ponieważ mózg bardzo lubi kończyć historie, których początek już rozpoznaje.

- Logo nie musi udowadniać autentyczności, żeby zadziałać. Wystarczy, że przez sekundę przesunie twoją uwagę z pytania „czy to prawdziwe?” na pytanie „co mam teraz zrobić?”.

- Profesjonalny ton rozmowy nie musi być perfekcyjny. Musi jedynie pasować do twojego wyobrażenia o tym, jak brzmi pracownik banku, konsultant operatora albo osoba z działu bezpieczeństwa.

- Znajoma historia daje przewagę, ponieważ mózg nie analizuje jej od zera. Uzupełnia brakujące elementy na podstawie wcześniejszych doświadczeń, a właśnie w tych brakujących miejscach może zostać ukryta manipulacja.

Najbardziej spektakularne oszustwa przyciągają uwagę, ale najbardziej interesujące bywają te małe. Pięćdziesiąt złotych za przedmiot, którego nigdy nie dostaniesz. Fałszywa zbiórka. Sklep, który znika tydzień po promocji. Oferta

inwestycyjna wyglądająca jak artykuł finansowy. Wiadomość od człowieka poznanego na portalu, który przez kilka tygodni nie prosi o nic, aż pewnego dnia pojawia się niewielki problem wymagający niewielkiej pomocy. To właśnie niewielkość pierwszego kroku jest psychologicznie wygodna. Duża prośba uruchamia opór. Mała prośba wygląda rozsądnie. Kiedy wykonasz pierwszy ruch, następny nie zaczyna się już od zera, ponieważ powstała historia, którą sam współtworzysz. Zapłaciłeś. Odpisałeś. Zaufałeś. Potwierdziłeś. Przyznałeś, że sytuacja wydaje ci się wiarygodna. Od tej chwili wycofanie nie oznacza jedynie przerwania kontaktu. Oznacza również przyznanie przed sobą, że wcześniejsza decyzja mogła być błędna. Oszust otrzymuje więc coś więcej niż pieniądze. Otrzymuje twoją potrzebę konsekwencji.

Tu zaczyna się jeden z najbardziej niewygodnych aspektów całego zjawiska: inteligencja nie usuwa podstawowych odruchów psychicznych. Może wręcz dostarczyć im bardziej eleganckiego uzasadnienia. Człowiek rozsądny potrafi wymyślić więcej powodów, dla których dziwna sytuacja jednak ma sens. Literówka? Pewnie automat. Nietypowy numer? Centrale mają różne numery. Presja czasu? Procedury bezpieczeństwa. Prośba o dodatkową płatność? System mógł źle naliczyć koszt. Brak możliwości oddzwonienia? Dział techniczny działa inaczej. Każda drobna niezgodność otrzymuje wyjaśnienie, ponieważ człowiek nie zawsze używa rozumu po to, żeby odkrywać prawdę. Czasem używa go po to, żeby utrzymać spójność historii, w którą już zaczął inwestować. To wyjątkowo obraźliwa cecha ludzkiego myślenia, bo pozwala być jednocześnie inteligentnym i konsekwentnie zmierzać w złą stronę.

Oszustwa internetowe korzystają też z emocji, których nie lubimy uważać za podatność. Strach jest oczywisty, więc chętnie o nim mówimy. Znacznie mniej wygodne są chciwość, próżność, samotność, potrzeba uznania, poczucie wyjątkowości i przekonanie, że tym razem udało się znaleźć okazję niedostępną dla innych. Kiedy ktoś traci pieniądze w fałszywej inwestycji, łatwo zredukować historię do zachłanności. Tyle że rzadko zaczyna się ona od myśli „chcę się szybko wzbogacić, niezależnie od ryzyka”. Częściej zaczyna się od znacznie przyzwoitszej opowieści: inflacja zjada oszczędności, pieniądze powinny pracować, inni inwestują, trzeba być odpowiedzialnym, może warto wreszcie zrobić coś rozsądnego z kapitałem. Oszust nie musi więc karmić cię obietnicą bogactwa. Może pozwolić ci poczuć się finansowo dojrzałe. To znacznie bardziej elegancka przynęta, ponieważ człowiek broni wtedy nie tylko potencjalnego zysku, ale również obrazu siebie jako osoby, która wreszcie podejmuje mądre decyzje.

Podobnie działa oszustwo romantyczne, choć na pierwszy rzut oka wydaje się zupełnie innym światem niż fałszywa strona banku. Tam nie ma czerwonego przycisku ani trzyminutowego zegara. Jest cierpliwość. Wiadomości rano. Pytania o dzień. Zapamiętane szczegóły. Zdjęcia. Historie o pracy, rodzinie, planach i samotności. Zanim pojawi się prośba o pieniądze, powstaje relacja wystarczająco realna emocjonalnie, żeby jej cyfrowy charakter przestał mieć znaczenie. Człowiek po drugiej stronie nie sprzedaje inwestycji ani produktu. Sprzedaje poczucie, że ktoś wreszcie słucha dokładnie. Koszt emocjonalny pojawia się długo przed stratą finansową, ponieważ ofiara zaczyna inwestować uwagę, nadzieję i przyszłość. Kiedy później pojawia się katastrofa wymagająca przelewu, odmowa oznaczałaby nie tylko ryzyko utraty pieniędzy, ale ryzyko

utrąty całej historii. Wtedy kalkulator w głowie nie liczy już złotych. Liczy więź.

- Presja nie zawsze ma formę „musisz zrobić to natychmiast”. Może mieć formę miesięcy budowania sytuacji, w której odmowa zaczyna być emocjonalnie droższa niż zgoda.

- Oszust nie musi wiedzieć wszystkiego o twoim życiu. Czasem wystarczy, że daje ci przestrzeń do opowiadania, a ty sam dostarczasz informacji o tym, czego się boisz, czego potrzebujesz i czego najbardziej nie chcesz stracić.

- Najbardziej skuteczna historia nie zawsze brzmi niewiarygodnie atrakcyjnie. Często brzmi dokładnie tak dobrze, jak twoim zdaniem życie mogłoby wyglądać, gdyby wreszcie coś ułożyło się po twojej myśli.

Potem dochodzi do zderzenia z otoczeniem. Rodzina pyta, dlaczego nie zadzwoniłeś. Partner mówi, że od początku coś mu nie pasowało. Znajomy zapewnia, że on nigdy nie podałyby kodu. Kolega z pracy opowiada, że takie wiadomości kasuje bez czytania. Każdy nagle staje się ekspertem od sytuacji, w której nie uczestniczył. To wyjątkowo komfortowa pozycja, ponieważ po fakcie każda pułapka wygląda na widoczną. Link jest podejrzany, kiedy już wiadomo, że prowadził do fałszywej strony. Rozmówca brzmi dziwnie, kiedy już wiadomo, że nie był pracownikiem banku. Oferta wydaje się nierealna, kiedy pieniądze zniknęły. Wiedza o zakończeniu zmienia sposób oceniania początku, dlatego późniejsza analiza tak łatwo produkuje pogardę zamiast zrozumienia. Ofiara zostaje wtedy z podwójną stratą: najpierw ktoś wykorzystał jej zachowanie, a później otoczenie wykorzystuje rezultat jako dowód jej naiwności.