Jak nie dać się oszukać

Praktyczne porady jak rozpoznać scam, phishing i inne cyberoszustwa

Konrad Mach

Spis treści

Rozdział 1. Dlaczego dajemy się nabrać 4

1.1. Psychologia oszustwa 4

1.2. Presja czasu i strach 14

1.3. Zaufanie do autorytetów 21

1.4. Każdy może być ofiarą 29

Rozdział 2. Fałszywe SMS-y i maile... **Błąd! Nie zdefiniowano zakładki.**

2.1. Jak działa phishing..... **Błąd! Nie zdefiniowano zakładki.**

2.2. Dopłata do paczki ..... **Błąd! Nie zdefiniowano zakładki.**

2.3. Niedopłata za prąd, mandat, zwrot podatku**Błąd! Nie zdefiniowano zakładki.**

2.4. Fałszywe komunikaty z banku.. **Błąd! Nie zdefiniowano zakładki.**

2.5. Jak sprawdzić link i nadawcę ... **Błąd! Nie zdefiniowano zakładki.**

Rozdział 3. Fałszywy pracownik banku**Błąd! Nie zdefiniowano zakładki.**

3.1. Spoofing, czyli fałszywy numer **Błąd! Nie zdefiniowano zakładki.**

3.2. Bezpieczne konto, którego nie ma**Błąd! Nie zdefiniowano zakładki.**

3.3. Zdalny pulpit i fałszywe aplikacje**Błąd! Nie zdefiniowano zakładki.**

3.4. Fałszywy policjant i inne służby**Błąd! Nie zdefiniowano zakładki.**

3.5. Jak zweryfikować rozmówcę.... **Błąd! Nie zdefiniowano zakładki.**

Rozdział 4. Pułapki BLIK ..... **Błąd! Nie zdefiniowano zakładki.**

4.1. Kod dla znajomego z Facebooka**Błąd! Nie zdefiniowano zakładki.**

4.2. Przelew przez pomyłkę..... **Błąd! Nie zdefiniowano zakładki.**

4.3. Fałszywe strony i SMS-y o BLIK **Błąd! Nie zdefiniowano zakładki.**

4.4. Bezpieczne zasady korzystania z BLIK **Błąd! Nie zdefiniowano zakładki.**

Rozdział 5. Zakupy w sieci ..... **Błąd! Nie zdefiniowano zakładki.**

5.1. Oszustwo na kupującego ..... **Błąd! Nie zdefiniowano zakładki.**

5.2. Fałszywe sklepy internetowe .... **Błąd! Nie zdefiniowano zakładki.**

5.3. Podrobione bramki płatności .... **Błąd! Nie zdefiniowano zakładki.**

5.4. Pułapki wynajmu i wakacji ..... **Błąd! Nie zdefiniowano zakładki.**

5.5. Jak sprawdzić sprzedawcę ..... **Błąd! Nie zdefiniowano zakładki.**

Rozdział 6. Fałszywe inwestycje ..... **Błąd! Nie zdefiniowano zakładki.**

6.1. Reklamy ze znanymi twarzami. **Błąd! Nie zdefiniowano zakładki.**

6.2. Fałszywy doradca inwestycyjny **Błąd! Nie zdefiniowano zakładki.**

6.3. Kryptowaluty i platformy widmo **Błąd! Nie zdefiniowano zakładki.**

6.4. Praca za zadania ..... **Błąd! Nie zdefiniowano zakładki.**

6.5. Sygnały ostrzegawcze ..... **Błąd! Nie zdefiniowano zakładki.**

Rozdział 7. Gra na emocjach ..... **Błąd! Nie zdefiniowano zakładki.**

7.1. Na wnuczka i na wypadek ..... **Błąd! Nie zdefiniowano zakładki.**

7.2. Oszustwa romantyczne ..... **Błąd! Nie zdefiniowano zakładki.**

7.3. Przejęte konta bliskich ..... **Błąd! Nie zdefiniowano zakładki.**

7.4. Deepfake i klonowanie głosu ... **Błąd! Nie zdefiniowano zakładki.**

7.5. Rodzinne hasło bezpieczeństwa **Błąd! Nie zdefiniowano zakładki.**

Rozdział 8. Jak się chronić ..... **Błąd! Nie zdefiniowano zakładki.**

8.1. Zasady codziennej higieny ..... **Błąd! Nie zdefiniowano zakładki.**

8.2. Hasła i weryfikacja dwuetapowa **Błąd! Nie zdefiniowano zakładki.**

8.3. Zastrzeżenie numeru PESEL .... **Błąd! Nie zdefiniowano zakładki.**

8.4. Co zrobić po oszustwie..... **Błąd! Nie zdefiniowano zakładki.**

8.5. Gdzie zgłaszać: bank, policja, CERT, 8080**Błąd! Nie zdefiniowano zakładki.**

Rozdział 1. Dlaczego dajemy się nabrać

1.1. Psychologia oszustwa

Socjotechnika zamiast włamania. Kiedy myślimy o przestępcach internetowych, przed oczami pojawia się zwykle obraz człowieka w ciemnym pokoju, który wpisuje setki linijek kodu i przełamuje kolejne zabezpieczenia banku. Przez lata zajmowania się oszustwami spotkałem się z takimi przypadkami bardzo rzadko. Ogromna większość spraw, które trafiają do zgłoszeń, wygląda zupełnie inaczej. Nikt nie łamie haseł, nikt nie włamuje się do systemów bankowych, nikt nie przejmuje serwerów. Przestępca robi coś znacznie prostszego: przekonuje człowieka, żeby sam wykonał przelew, sam podał dane karty albo sam zainstalował program, który odda telefon w obce ręce.

Taką metodę nazywa się socjotechniką. Polega ona na wpływaniu na decyzje drugiej osoby tak, żeby działała na własną szkodę, a przy tym miała poczucie, że postępuje rozsądnie. Bank może mieć najlepsze zabezpieczenia na świecie, ale jeśli właściciel konta sam zaloguje się do aplikacji, sam wpisze kwotę i sam potwierdzi operację, system widzi zwykłą, prawidłową transakcję. Z technicznego punktu widzenia nic złego się nie wydarzyło. Złe rzeczy wydarzyły się wcześniej, w rozmowie albo w wiadomości, która skłoniła do tego działania.

Dlatego większość oszustw nie wymaga od sprawcy żadnej wiedzy hakerskiej. Wystarczy mu telefon, kilka gotowych zdań, tania strona internetowa postawiona w kwadrans i trochę cierpliwości. Bardzo wiele narzędzi da się kupić gotowych, łącznie z szablonami stron udających banki i firmy kurierskie. Wiedza, której oszust naprawdę potrzebuje, dotyczy ludzi, a nie komputerów. Musi wiedzieć, co nas niepokoi, czemu ufamy, kiedy jesteśmy zmęczeni i jakie słowa sprawiają, że przestajemy myśleć krytycznie.

To ważne spostrzeżenie, bo zmienia sposób, w jaki warto patrzeć na własne bezpieczeństwo. Program antywirusowy, silne hasło i aktualny system są potrzebne i wrócę do nich w ostatnim rozdziale. Jednak żadne z nich nie zadziała, jeśli przestępca skłoni Cię do tego, żeby własnoręcznie otworzyć mu drzwi. Najskuteczniejszą ochroną jest zrozumienie

mechanizmów, które wykorzystuje. Gdy je poznasz, zaczniesz je zauważać w wiadomościach i rozmowach, a zauważony mechanizm traci większość swojej siły.

Warto przy tym zauważyć, że socjotechnika nie jest wynalazkiem epoki internetu. Oszuści matrymonialni, fałszywi inkasenci i domokrążcy sprzedający cudowne garnki stosowali te same metody kilkadziesiąt lat temu. Zmieniła się skala i narzędzia. Dawniej jeden naciągacz mógł w ciągu dnia odwiedzić kilka mieszkań. Dziś jeden człowiek z laptopem może w tym samym czasie wysłać wiadomości do setek tysięcy osób, a zorganizowana grupa prowadzi jednocześnie dziesiątki rozmów telefonicznych.

Kiedy analizuję opisy oszustw publikowane przez banki i policję, zawsze zadaję sobie jedno pytanie: kto nacisnął przycisk? W przytłaczającej większości przypadków odpowiedź brzmi: ofiara. To ona wpisała dane karty, to ona przepisała kod, to ona zatwierdziła przelew. Ta obserwacja nie służy obwinianiu kogokolwiek. Pokazuje natomiast, gdzie leży pole walki. Przestępca potrzebuje Twojego działania, a każde działanie poprzedza decyzja, nad którą masz kontrolę.

Dwa tryby myślenia. Psychologowie od dawna opisują dwa sposoby, w jakie przetwarzamy informacje. Pierwszy jest szybki, automatyczny i niewymagający wysiłku. Dzięki niemu rozpoznajemy twarze, czytamy proste słowa, prowadzimy samochód znaną trasą i odruchowo odpowiadamy na pytanie „co słychać". Drugi jest wolny, analityczny i męczący. Uruchamiamy go, kiedy liczymy w pamięci, porównujemy oferty, czytamy umowę albo zastanawiamy się nad trudną decyzją.

Na co dzień korzystamy głównie z pierwszego trybu i to jest rozsądne. Gdybyśmy każdą drobną czynność analizowali krok po kroku, nie zdążylibyśmy zrobić niczego. Mózg oszczędza energię, opierając się na nawykach i skojarzeniach. Problem polega na tym, że ten sam mechanizm, który pozwala sprawnie funkcjonować, otwiera drogę do manipulacji. Szybki tryb myślenia nie pyta, czy coś jest prawdziwe. Reaguje na znajome sygnały: logo, kolor, ton wiadomości, słowo „pilne".

Oszuści doskonale o tym wiedzą i celowo tworzą sytuacje, w których człowiek działa odruchowo. Wiadomość ma przyjść wtedy, kiedy masz mnóstwo zajęć, ma być krótka, ma wyglądać znajomo i ma zawierać jedno proste polecenie. Nie chodzi o to, żeby ją dokładnie przeczytać i ocenić.

Chodzi o to, żeby kliknięcie nastąpiło, zanim w ogóle zaczniesz się zastanawiać.

Najprostszy przykład znam z własnego doświadczenia. Czekałem kiedyś na paczkę z kilkoma rzeczami zamówionymi do domu. W ciągu dnia dostałem SMS z informacją, że przesyłka czeka na doręczenie i wymaga potwierdzenia adresu. Kciuk już był nad linkiem, kiedy zorientowałem się, że zamówienie miało przyjść inną firmą, a ja nigdy nie podawałem tej firmie swojego numeru. Gdybym był odrobinę bardziej zmęczony albo bardziej zajęty, kliknąłbym bez zastanowienia. Nie dlatego, że uwierzyłem w treść wiadomości, tylko dlatego, że kliknięcie w link od kuriera stało się nawykiem. Właśnie takie kliknięcia „z przyzwyczajenia" są paliwem większości kampanii phishingowych.

Z tego wynika praktyczna wskazówka, którą będę powtarzał w różnych miejscach książki. Kiedy wiadomość lub rozmowa dotyczy pieniędzy, danych albo instalacji czegokolwiek, warto świadomie przełączyć się na wolny tryb myślenia. Wystarczy zatrzymać się na kilka sekund i zadać sobie pytanie: skąd ta wiadomość naprawdę pochodzi i czy na nią czekam? Ta chwila wysiłku często wystarcza, żeby zobaczyć coś, czego w trybie automatycznym nie widać.

Szybki tryb myślenia ma jeszcze jedną cechę, która ułatwia pracę oszustom. Uzupełnia brakujące informacje na podstawie oczekiwań. Jeśli czekasz na zwrot pieniędzy ze sklepu, wiadomość o „zwrocie środków" od razu połączysz z tym zamówieniem, choć nie ma w niej nazwy sklepu ani numeru zamówienia. Mózg sam dopowie resztę historii i uzna ją za spójną. Oszust nie musi znać szczegółów Twojego życia, wystarczy, że poda ogólną treść, a dopasowanie jej do Twojej sytuacji nastąpi samo.

Ten mechanizm działa szczególnie silnie wtedy, gdy wykonujemy kilka czynności jednocześnie. Odpisywanie na wiadomości podczas jazdy tramwajem, sprawdzanie poczty w przerwie między spotkaniami, przeglądanie telefonu przy gotowaniu obiadu to sytuacje, w których umysł nie ma zasobów na dokładną analizę. Dlatego dobrym nawykiem jest odkładanie wiadomości dotyczących pieniędzy i kont na chwilę, w której można się nimi zająć w spokoju.

Reguła wzajemności. Jedną z najsilniejszych norm społecznych jest potrzeba odwzajemniania. Kiedy ktoś coś dla nas zrobi, czujemy się zobowiązani, żeby zrobić coś w zamian. Ta reguła jest obecna we wszystkich

kulturach i ma głęboki sens, bo pozwala ludziom współpracować i budować relacje. Kiedy sąsiad pomoże nam wnieść meble, chętnie podlejemy mu kwiaty podczas jego urlopu. Kiedy ktoś nas poczęstuje, mamy ochotę się zrewanżować.

Oszuści bardzo często zaczynają od tego, że coś dają. Najczęściej jest to pomoc albo ostrzeżenie. Dzwoni rzekomy pracownik banku i mówi, że wykrył podejrzaną transakcję na Twoim koncie i chce ją zablokować. Rozmówca nie prosi o nic, tylko oferuje ochronę. W ten sposób buduje w Tobie poczucie wdzięczności i zobowiązania. Kiedy po kilku minutach poprosi o potwierdzenie danych albo wykonanie jakiejś czynności, trudniej będzie odmówić komuś, kto właśnie stara się Ci pomóc.

Czasem prezent ma postać drobnej kwoty. W oszustwach inwestycyjnych i w schematach „pracy za zadania" ofiara na początku dostaje kilka, kilkanaście albo kilkadziesiąt złotych prawdziwego zysku. Pieniądze naprawdę wpływają na konto. To nie tylko uwiarygadnia całe przedsięwzięcie, ale też uruchamia poczucie, że druga strona dotrzymuje słowa, więc wypada odpowiedzieć tym samym. Innym razem prezentem jest porada, darmowe szkolenie, e-book albo dostęp do „zamkniętej grupy".

Rozpoznanie tej reguły nie oznacza, że trzeba podejrzliwie traktować każdą życzliwość. Chodzi o coś innego: kiedy nieznana osoba najpierw oferuje pomoc, a potem prosi o pieniądze, dane lub działanie na Twoim urządzeniu, warto zauważyć, że pierwsza część rozmowy mogła być tylko przygotowaniem do drugiej. Prawdziwa pomoc nie wymaga od Ciebie spłacania długu wdzięczności w postaci kodów, haseł i przelewów.

Bardzo charakterystyczną formą wykorzystania tej reguły jest rzekome ustępstwo. Oszust najpierw prosi o coś dużego, na przykład o przelanie wszystkich oszczędności na bezpieczne konto. Kiedy ofiara się waha, rozmówca „idzie na rękę" i mówi, że wystarczy przelać połowę albo tylko środki z jednego rachunku. Ofiara ma poczucie, że druga strona zrobiła krok w jej stronę, więc sama też powinna ustąpić. W rzeczywistości mniejsza prośba od początku była celem oszusta, a duża służyła jedynie temu, żeby ta druga wydała się rozsądna.

Reguła wzajemności działa też w kontaktach długotrwałych. W oszustwach, które trwają tygodniami, przestępcy pamiętają o urodzinach ofiary, pytają o zdrowie jej bliskich, wysyłają drobne prezenty w postaci kart

podarunkowych albo kodów do gier. Każdy taki gest buduje dług wdzięczności, który zostanie wykorzystany w odpowiednim momencie.

Metoda małych kroków. Mało kto zgodziłby się na przelanie oszczędności życia na nieznane konto, gdyby ktoś zaproponował to w pierwszym zdaniu rozmowy. Oszuści o tym wiedzą, dlatego nigdy nie zaczynają od dużej prośby. Zaczynają od bardzo małych, z pozoru niewinnych kroków. Najpierw rozmówca prosi o potwierdzenie imienia. Potem o datę urodzenia. Potem o to, z jakiego banku korzystasz. Potem o kod, który przyszedł SMS-em „w celu weryfikacji". Na końcu prosi o zalogowanie się do aplikacji i wykonanie przelewu.

Każdy z tych kroków osobno wydaje się drobny. Potwierdzenie imienia nie wymaga namysłu, przecież rozmówca je zna. Podanie daty urodzenia wygląda na standardową procedurę. Przepisanie kodu z SMS-a sprawia wrażenie zwykłej formalności. Problem polega na tym, że każda kolejna zgoda przychodzi łatwiej niż poprzednia. Ludzie mają silną potrzebę bycia konsekwentnymi. Jeśli raz zgodziliśmy się na współpracę, odmowa w kolejnym kroku wydaje się niespójna z tym, co zrobiliśmy przed chwilą. Mówiąc wprost: skoro już się zaczęło, głupio teraz przerywać.

Ten mechanizm jest dobrze opisany w psychologii społecznej i wykorzystywany nie tylko przez przestępców, ale też przez sprzedawców i marketingowców. W przypadku oszustw ma jednak szczególnie groźne skutki, bo każdy krok przybliża przestępcę do celu, a ofiara nie widzi całej drogi. Widzi tylko najbliższą prośbę, która nie różni się wiele od poprzedniej.

Najlepszą obroną jest patrzenie na rozmowę jako całość, a nie na pojedynczy krok. Jeśli w pewnym momencie zauważysz, że rozmowa zaczęła się od niewinnego pytania, a teraz dotyczy kodów, haseł albo pieniędzy, masz pełne prawo przerwać. Wcześniejsza zgoda na kilka pytań nie zobowiązuje Cię do niczego. Przerwanie w połowie nie jest niekonsekwencją, tylko rozsądną reakcją na zmianę sytuacji.

Przestępcy stosują tę metodę także w kanałach pisemnych. Fałszywy formularz rzadko prosi od razu o wszystkie dane. Najpierw pojawia się pole z imieniem i nazwiskiem, potem adres, potem numer telefonu, a dopiero na kolejnej stronie numer karty i kod CVV. Osoba, która wypełniła już trzy strony formularza, czuje, że zainwestowała w niego wysiłek, i chce

doprowadzić sprawę do końca. Gdyby pierwsza strona zawierała pole na kod CVV, wiele osób zamknęłoby ją bez zastanowienia.

Ten sam mechanizm widać w oszustwach na kupującego i w pracy za zadania. Pierwsza prośba jest tak drobna, że odmowa wydaje się przesadą. Kolejne prośby rosną stopniowo, a różnica między nimi jest za każdym razem niewielka. Po kilku dniach ofiara robi rzeczy, których na początku nie wzięłaby pod uwagę, i nie potrafi wskazać momentu, w którym przekroczyła granicę.

Społeczny dowód słuszności. Kiedy nie jesteśmy pewni, jak postąpić, patrzymy na innych. W nieznanym mieście wybieramy restaurację, w której siedzi dużo ludzi. W sklepie internetowym sprawdzamy, ile osób kupiło produkt i jakie wystawiło oceny. To naturalny odruch, który zwykle dobrze nam służy, bo doświadczenie wielu osób bywa cenniejsze od naszej pojedynczej oceny.

Oszuści fabrykują ten dowód na masową skalę. Pod fałszywymi reklamami inwestycji pojawiają się dziesiątki komentarzy zachwyconych użytkowników, którzy rzekomo zarobili tysiące złotych w kilka tygodni. Na stronach nieistniejących sklepów widnieją setki pięciogwiazdkowych opinii. W komunikatorach działają grupy, w których „wszyscy już skorzystali", regularnie publikują zrzuty ekranu z wypłatami i dziękują opiekunowi za pomoc. Ofiara, która trafia do takiej grupy, widzi wokół siebie zadowolonych ludzi i trudno jej uwierzyć, że coś może być nie tak.

Tymczasem wszystkie te elementy da się wyprodukować tanio i szybko. Fałszywe konta w mediach społecznościowych kupuje się hurtowo. Komentarze można wygenerować automatycznie. Zrzut ekranu z aplikacji bankowej albo platformy inwestycyjnej spreparuje każdy, kto potrafi obsłużyć prosty program graficzny. W grupach w komunikatorach często tylko jedna osoba jest prawdziwa, a reszta uczestników to wspólnicy lub konta prowadzone przez tych samych ludzi.

Dlatego liczba pozytywnych reakcji nie świadczy o wiarygodności. Świadczy co najwyżej o tym, że ktoś zadbał o ich liczbę. Warto zwracać uwagę na szczegóły: czy profile komentujących mają historię starszą niż kilka tygodni, czy opinie nie są do siebie podobne w treści i stylu, czy pod postem da się w ogóle dodać krytyczny komentarz, czy może takie wpisy szybko znikają. Bardziej wartościowe od setki entuzjastycznych głosów są informacje z niezależnych źródeł, o których piszę w dalszych rozdziałach.

Społeczny dowód słuszności bywa wykorzystywany także w rozmowach telefonicznych. Fałszywy konsultant mówi na przykład: „Dziś dzwonimy do wszystkich klientów z Pani regionu, bo atak dotyczy wielu osób" albo „Większość klientów już przeniosła środki, zostało tylko kilka osób". Takie zdania mają sprawić, że ofiara poczuje się częścią większej grupy, która postępuje w określony sposób. Skoro inni już to zrobili, wydaje się to normalne i bezpieczne.

Siła tego mechanizmu rośnie, kiedy dowód pochodzi od osób podobnych do nas. Komentarz od kogoś w tym samym wieku, z tej samej miejscowości albo o podobnym zawodzie przekonuje bardziej niż anonimowa opinia. Oszuści o tym wiedzą i dopasowują fałszywe profile do grupy docelowej reklamy. Do seniorów piszą rzekomi emeryci, do młodych rodziców rzekome matki, do przedsiębiorców rzekomi właściciele firm.

Sympatia i zaufanie. Łatwiej zgadzamy się z ludźmi, których lubimy. Lubimy zaś tych, którzy są dla nas mili, okazują zainteresowanie, podzielają nasze poglądy i rozumieją nasze kłopoty. To kolejny mechanizm, który przestępcy wykorzystują świadomie i z dużą wprawą.

W rozmowach z ofiarami oszustw słyszę często podobne zdanie: „On był taki uprzejmy". Oszuści zwracają się po imieniu, są cierpliwi, nie przerywają, okazują zrozumienie. Przepraszają za kłopot. Chwalą rozmówcę za czujność. Jeśli ofiara mówi wolniej, oni też zwalniają. Jeśli używa prostego języka, unikają specjalistycznych słów. Jeśli jest zdenerwowana, uspokajają. Dopasowanie się do rozmówcy sprawia, że w krótkim czasie powstaje poczucie bliskości i porozumienia.

W wielu przypadkach ta uprzejmość wypada lepiej niż kontakt z prawdziwą infolinią, na której trzeba czekać, przechodzić przez menu i rozmawiać z konsultantem, który ma ograniczony czas. Paradoksalnie właśnie to może uśpić czujność. Przestępca ma czas, bo każda minuta rozmowy przybliża go do celu. Prawdziwa instytucja ma setki innych klientów.

Miła rozmowa nie jest dowodem dobrych intencji. To zdanie warto zapamiętać. Uprzejmość jest narzędziem, które każdy może wykorzystać, i nie mówi nic o tym, kim naprawdę jest rozmówca. Ocena, czy rozmowa jest bezpieczna, powinna opierać się na tym, o co ktoś prosi, a nie na tym, jak sympatycznie to robi.

Budowanie sympatii obejmuje też szukanie podobieństw. Rozmówca może wspomnieć, że pochodzi z tego samego miasta, że też ma dzieci w podobnym wieku, że kibicuje tej samej drużynie albo że jego matka też miała problem z bankiem. Takie wtrącenia wydają się przypadkowe, ale są przemyślanym elementem rozmowy. Ludzie ufają bardziej tym, z którymi coś ich łączy.

Warto zwrócić uwagę na jeszcze jeden element. Oszuści bardzo często chwalą swoje ofiary. „Świetnie, że Pan tak szybko zareagował", „Widać, że Pani zna się na bankowości", „Rzadko trafiam na tak rozsądnego klienta". Komplement sprawia przyjemność i jednocześnie utrudnia późniejsze wycofanie się. Trudno przyznać się do wątpliwości komuś, kto przed chwilą pochwalił nasz rozsądek.

Scenariusze i legendy. Wiele osób wyobraża sobie oszusta jako samotnego naciągacza, który improwizuje w trakcie rozmowy. W rzeczywistości duża część oszustw, zwłaszcza telefonicznych i inwestycyjnych, jest prowadzona przez zorganizowane grupy działające według gotowych scenariuszy. W środowisku policyjnym i bankowym nazywa się je legendami.

Legenda to przemyślana opowieść z rolami, kwestiami i przygotowanymi odpowiedziami. Określa, kto dzwoni pierwszy, co mówi, jakie dane podaje dla uwiarygodnienia i w którym momencie przekazuje rozmowę dalej. W zorganizowanych grupach role są podzielone na kolejnych rozmówców. Pierwszy może udawać konsultanta infolinii, drugi pracownika działu bezpieczeństwa, trzeci policjanta albo prokuratora. Każdy z nich ma swoją część historii do opowiedzenia i swoje zadanie do wykonania.

Najbardziej zaskakuje ofiary to, że oszuści mają gotowe odpowiedzi na typowe pytania i wątpliwości. Kiedy ktoś mówi „zadzwonię do banku i sprawdzę", słyszy, że właśnie rozmawia z bankiem, a połączenie przez infolinię może zostać przechwycone przez przestępców. Kiedy pyta, skąd rozmówca ma jego dane, słyszy, że to dane z systemu bankowego. Kiedy waha się przed przelewem, słyszy, że zwłoka oznacza utratę wszystkich pieniędzy. Te odpowiedzi są przećwiczone setki razy i dopracowane na podstawie wcześniejszych rozmów.

Świadomość istnienia legend pomaga zrozumieć jedną ważną rzecz: jeśli rozmówca ma odpowiedź na każde Twoje pytanie, nie oznacza to, że mówi prawdę. Oznacza tylko, że jest dobrze przygotowany. Gładka, spójna

opowieść bywa właśnie sygnałem, że masz do czynienia z wyćwiczonym scenariuszem, a nie z prawdziwą sytuacją, w której pracownik często musi coś sprawdzić, zapytać przełożonego albo oddzwonić.

Z ustaleń policji wynika, że zorganizowane grupy prowadzą centra telefoniczne, w których pracuje wiele osób jednocześnie. Mają one przygotowane skrypty rozmów, listy numerów do wybrania i zestawy odpowiedzi na typowe zastrzeżenia. Zdarza się, że po zatrzymaniu członków takich grup śledczy znajdują wydrukowane instrukcje opisujące krok po kroku, co mówić przy każdym etapie rozmowy.

Legenda jest też stale doskonalona. Kiedy banki i media zaczynają ostrzegać przed konkretnym scenariuszem, przestępcy modyfikują go tak, żeby ostrzeżenia przestały pasować. Jeśli wszyscy wiedzą, że bank nie dzwoni w sprawie bezpiecznego konta, zaczyna dzwonić „policja". Jeśli wszyscy wiedzą, że nie podaje się kodów BLIK, pojawia się prośba o „zwrot" przez wpłatomat. Dlatego bardziej niż pojedyncze historie warto zapamiętać mechanizmy, które się za nimi kryją.

Izolowanie ofiary. Każde oszustwo ma słaby punkt: może je przerwać ktoś z zewnątrz. Członek rodziny, który zapyta, co się dzieje. Przyjaciel, który powie „to wygląda podejrzanie". Pracownik banku, który zauważy nietypową transakcję i zadzwoni z pytaniem. Kasjer w oddziale, który zwróci uwagę na zdenerwowanie klienta wypłacającego dużą kwotę. Dlatego jednym z najważniejszych zadań oszusta jest odcięcie ofiary od wszystkich tych osób.

Izolacja przybiera kilka form. Pierwsza to prośba o nierozłączanie się. Rozmówca tłumaczy, że przerwanie połączenia uniemożliwi zablokowanie przestępców albo że trzeba pozostać na linii, aż operacja zostanie zakończona. W praktyce chodzi o to, żeby nie dało się do nikogo zadzwonić i żeby nikt nie mógł zadzwonić do Ciebie. Druga forma to żądanie zachowania tajemnicy. Słyszysz, że sprawa jest objęta poufnym postępowaniem, że w banku może pracować wspólnik przestępców albo że rozmowa z bliskimi zaszkodzi śledztwu. Trzecia forma to wprost zakaz kontaktu z bankiem lub rodziną, czasem połączony z instrukcją, co powiedzieć, gdyby ktoś zadawał pytania.

Wszystkie te zabiegi mają jeden cel: odciąć Cię od osób, które mogłyby przerwać oszustwo. Dlatego zasada jest prosta i nie ma od niej wyjątków. Prawdziwa instytucja nigdy nie zabrania rozmowy z rodziną ani kontaktu z

własnym bankiem. Jeśli ktokolwiek każe Ci utrzymać coś w tajemnicy przed najbliższymi, to właśnie jest moment, w którym trzeba do nich zadzwonić.

Izolacja bywa też fizyczna. W niektórych oszustwach przestępcy każą ofierze pojechać do innego oddziału banku niż zwykle, bo „w Pani oddziale pracuje podejrzany". W innych proszą o wyjście z domu i rozmowę z dala od domowników albo o przejście do innego pokoju. Każdy taki zabieg zmniejsza szansę, że ktoś przypadkiem usłyszy rozmowę i zareaguje.

Z drugiej strony izolacja jest najsłabszym punktem całego scenariusza. Wystarczy jedna rozmowa z kimś spoza historii, żeby oszustwo się rozpadło. Policja i banki opisują wiele przypadków, w których kasjerka, sąsiad, taksówkarz albo wnuk przerwali oszustwo jednym pytaniem. Dlatego warto pamiętać, że prośba o tajemnicę jest dokładnie tym sygnałem, który powinien skłonić do złamania tajemnicy.

Efekt utopionych kosztów. Ostatni mechanizm, który chcę tu opisać, jest szczególnie bolesny, bo działa już po tym, jak ofiara poniosła pierwszą stratę. W psychologii nazywa się go efektem utopionych kosztów. Polega na tym, że im więcej zainwestowaliśmy w jakieś przedsięwzięcie, tym trudniej nam z niego zrezygnować, nawet jeśli rozsądek podpowiada, że należy przestać. Nie chcemy pogodzić się z tym, że wcześniejsze pieniądze, czas i wysiłek przepadły.

Oszuści świadomie wykorzystują tę skłonność. Osoba, która wpłaciła kilka tysięcy złotych na fałszywą platformę inwestycyjną i widzi na ekranie rzekomy zysk, w pewnym momencie chce wypłacić pieniądze. Wtedy słyszy, że najpierw musi uiścić „opłatę za wypłatę", „podatek od zysku", „prowizję za przewalutowanie" albo „depozyt zabezpieczający". Ponieważ stawką są już nie tylko nowe pieniądze, ale też wszystkie poprzednie, ofiara płaci. Po chwili pojawia się kolejna opłata, potem następna. Każda wpłata jest uzasadniana tym, że to już ostatni krok przed odzyskaniem całości.

Ten sam mechanizm działa w oszustwach romantycznych, w schematach pracy za zadania i w fałszywych zakupach, w których „dopłata do przesyłki" zamienia się w ciąg kolejnych opłat. Bywa też wykorzystywany przez drugą falę oszustów, którzy kontaktują się z ofiarami i oferują pomoc w odzyskaniu utraconych środków. Oczywiście za opłatą z góry.

Rozpoznanie tego efektu pozwala podjąć trudną, ale rozsądną decyzję. Jeśli, żeby odzyskać pieniądze, musisz najpierw zapłacić kolejne, niemal na pewno masz do czynienia z oszustwem. Prawdziwa platforma inwestycyjna

potrąca podatki i prowizje z wypłacanej kwoty, a nie żąda dodatkowych przelewów. Prawdziwa firma kurierska nie wymyśla nowych opłat co kilka godzin. Każda kolejna wpłata nie przybliża do odzyskania poprzednich, tylko powiększa stratę. Zatrzymanie się w tym miejscu nie jest porażką, tylko przerwaniem schematu, który bez Twojego udziału nie może trwać dalej.

Efekt utopionych kosztów dotyczy nie tylko pieniędzy, ale też czasu i emocji. Osoba, która przez kilka godzin rozmawiała z rzekomym pracownikiem banku, wykonała dziesiątki poleceń i przeżyła ogromny stres, nie chce uwierzyć, że wszystko to było na nic. Łatwiej jej zaakceptować kolejną prośbę rozmówcy niż przyznać, że od początku była oszukiwana. Im dłużej trwa oszustwo, tym trudniej je przerwać.

Pomocne może być zadanie sobie prostego pytania: czy ta propozycja, usłyszana dziś po raz pierwszy, wydałaby się do przyjęcia? Jeśli odpowiedź jest przecząca, to wcześniejsze wpłaty nie są powodem, żeby się zgodzić teraz. Pieniądze już wpłacone są niezależne od decyzji, którą podejmujesz w tej chwili.

1.2. Presja czasu i strach

Dlaczego oszustowi tak bardzo się spieszy. Jeśli miałbym wskazać jeden element, który łączy niemal wszystkie oszustwa, z jakimi się zetknąłem, byłby to pośpiech. Fałszywy kurier chce dopłaty natychmiast. Fałszywy bank wymaga reakcji w ciągu kilku minut. Fałszywy doradca inwestycyjny przekonuje, że okazja zniknie jeszcze dziś. Nawet w oszustwach romantycznych, które rozwijają się tygodniami, przychodzi moment nagłej, dramatycznej prośby, której nie da się odłożyć do jutra.

Ten pośpiech nie jest przypadkowy. Dla przestępcy czas jest największym wrogiem. Każda minuta zwłoki daje Ci szansę na sprawdzenie informacji. Możesz wejść na stronę firmy, zadzwonić na infolinię banku, zapytać kogoś bliskiego albo po prostu ochłonąć i spojrzeć na sytuację spokojniej. Wystarczy jedna z tych czynności, żeby cała misternie przygotowana historia się rozpadła. Oszust doskonale zdaje sobie sprawę, że jego opowieść nie wytrzyma konfrontacji z rzeczywistością, dlatego robi wszystko, żeby do tej konfrontacji nie doszło.

Celem presji czasu jest więc uniemożliwienie weryfikacji. Nie chodzi o to, żeby Cię przekonać do prawdziwości wiadomości. Chodzi o to, żeby

zabrakło chwili na sprawdzenie tej prawdziwości. To zasadnicza różnica. Wiele osób zakłada, że jeśli wiadomość wydaje się wiarygodna, to musi być prawdziwa. Tymczasem oszust nie potrzebuje stuprocentowej wiarygodności. Wystarczy mu, że przez kilka minut historia wyda się na tyle przekonująca, żeby wykonać polecenie.

Zauważyłem też, że pośpiech działa na nas silniej niż sama treść wiadomości. Nawet osoba, która ma pewne wątpliwości, często decyduje się działać, bo koszt pomyłki w jej oczach wydaje się większy od kosztu zwłoki. Myśli: lepiej zapłacić te kilka złotych, niż ryzykować, że paczka wróci do nadawcy. Lepiej przelać pieniądze na bezpieczne konto, niż stracić wszystko. Ten rachunek jest fałszywy, bo opiera się na informacjach podanych przez oszusta, ale w chwili stresu trudno to dostrzec.

Pośpiech ma też wymiar techniczny. Fałszywe strony działają krótko, bo szybko trafiają na listy ostrzeżeń. Kod BLIK jest ważny dwie minuty. Kod SMS z banku wygasa po kilku minutach. Przelew natychmiastowy może zostać zatrzymany, jeśli bank zorientuje się wystarczająco szybko. Oszust działa więc pod presją własnego zegara i przenosi ją na ofiarę.

Warto zauważyć, że w prawdziwych sytuacjach awaryjnych instytucje działają same. Jeśli bank wykryje włamanie na konto, zablokuje je bez Twojego udziału. Jeśli dostawca energii ma problem z siecią, wysyła ekipę techniczną, a nie prośbę o przelew. Pośpiech, który wymaga Twojego natychmiastowego działania finansowego, prawie zawsze jest pośpiechem oszusta.

Słowa, które wyznaczają termin. Presja czasu ma swój charakterystyczny język. Kiedy zacząłem zwracać na niego uwagę, okazało się, że w fałszywych wiadomościach powtarzają się te same sformułowania. Warto je znać, bo pełnią funkcję sygnału ostrzegawczego niezależnie od tego, pod kogo podszywa się nadawca.

Najczęściej pojawiają się zwroty takie jak „w ciągu 24 godzin”, „do końca dnia”, „najpóźniej dziś do godziny 20:00”, „ostatnie wezwanie”, „pozostało 15 minut”, „termin mija dziś”, „natychmiast”, „pilne” i „bez dalszych powiadomień”. Na fałszywych stronach często widnieje odliczający zegar, który pokazuje, ile czasu zostało na opłacenie przesyłki albo potwierdzenie danych. W rozmowach telefonicznych podobną funkcję pełnią zdania w rodzaju „mamy bardzo mało czasu” czy „przestępcy właśnie próbują wykonać przelew”.

Warto zestawić to z tym, jak naprawdę działają instytucje. Banki, urzędy, dostawcy energii i firmy kurierskie rzadko wymagają reakcji w ciągu minut lub godzin. Terminy na zapłatę rachunku liczy się w dniach albo tygodniach. Wezwania urzędowe przychodzą listownie lub przez oficjalne skrzynki i dają czas na odpowiedź. Przesyłka, której nie da się doręczyć, czeka w punkcie odbioru kilka dni. Nawet jeśli bank zablokuje kartę z powodu podejrzanej transakcji, robi to sam i informuje o tym klienta, zamiast żądać od niego natychmiastowych działań.

Prawdziwy pośpiech zdarza się oczywiście w życiu, ale prawie nigdy nie przybiera formy SMS-a z linkiem albo telefonu od nieznanej osoby, która domaga się działania w ciągu kwadransa. Jeśli wiadomość wyznacza bardzo krótki termin i jednocześnie dotyczy pieniędzy lub danych, to połączenie jest silną przesłanką, że masz do czynienia z oszustwem.

Presja czasu pojawia się także w formie wizualnej. Wiadomości zawierają wykrzykniki, wielkie litery, czerwone ikony ostrzegawcze i słowa takie jak „UWAGA” czy „OSTATECZNE”. Na fałszywych stronach pojawiają się paski postępu, które pokazują, że „rezerwacja wygasa”, albo komunikaty o tym, że „sesja zostanie zamknięta za 3 minuty”. Wszystkie te elementy mają przyspieszyć decyzję.

Prosty test polega na tym, żeby w myślach usunąć z wiadomości wszystkie słowa dotyczące terminu i sprawdzić, co zostaje. Bardzo często okazuje się, że bez nich wiadomość traci sens, bo nie ma w niej żadnej konkretnej informacji: numeru faktury, numeru zamówienia, nazwiska, kwoty wynikającej z umowy. Prawdziwe wezwania zawierają szczegóły, które można sprawdzić. Fałszywe zawierają głównie presję.

Groźby, które mają wywołać panikę. Drugim narzędziem presji jest strach. Oszuści sięgają po groźby, które dotyczą rzeczy dla nas ważnych i których utrata byłaby bolesna lub kłopotliwa. Przez lata obserwowania kolejnych kampanii widziałem ich bardzo wiele, ale da się je pogrupować w kilka powtarzalnych kategorii.

Pierwsza to blokada konta bankowego. Wiadomość informuje, że dostęp do bankowości zostanie ograniczony, karta zablokowana, a środki zamrożone, jeśli nie potwierdzisz danych. Druga to odcięcie usług domowych: prądu, gazu, internetu albo telefonu, często jeszcze tego samego dnia. Trzecia to mandat lub kara administracyjna, na przykład za przekroczenie prędkości albo nieopłacony przejazd. Czwarta to egzekucja

komornicza i zajęcie wynagrodzenia lub rachunku. Piąta to sprawa karna, w której odbiorca rzekomo jest podejrzanym albo świadkiem i musi pilnie współpracować z policją lub prokuraturą. Szósta, najsilniejsza, to utrata oszczędności, bo ktoś właśnie próbuje je ukraść.

Każda z tych gróźb ma ten sam cel: wywołać chęć natychmiastowego „załatwienia sprawy". Kiedy słyszymy, że coś złego zaraz się wydarzy, nasza uwaga skupia się na tym, jak tego uniknąć. Nie zastanawiamy się, czy zagrożenie jest prawdziwe, tylko co zrobić, żeby je usunąć. Oszust od razu podsuwa rozwiązanie: kliknij w link, zapłać niewielką kwotę, podaj kod, przelej pieniądze. To rozwiązanie wydaje się w tej sytuacji ulgą, a nie ryzykiem.

Warto zapamiętać, że groźba połączona z gotowym, prostym sposobem jej uniknięcia jest typowym schematem manipulacji. Prawdziwe problemy prawne i finansowe rzadko rozwiązuje się jednym kliknięciem w link z SMS-a.

Groźba bywa też połączona z poczuciem winy. Wiadomość może sugerować, że odbiorca czegoś zaniedbał: nie zapłacił rachunku, nie zaktualizował danych, przekroczył prędkość, nie odebrał przesyłki. Wiele osób, które nie pamiętają dokładnie wszystkich swoich płatności, zaczyna się zastanawiać, czy rzeczywiście o czymś nie zapomniały. Ta niepewność wystarcza, żeby kliknąć w link „dla pewności".

W rozmowach telefonicznych groźba jest często stopniowana. Najpierw pojawia się informacja o niewielkim problemie, potem o coraz poważniejszych konsekwencjach. Na początku chodzi o zablokowanie karty, po kilku minutach o utratę wszystkich środków, a na końcu o odpowiedzialność karną za rzekomy udział w praniu pieniędzy. Każdy kolejny poziom zagrożenia sprawia, że ofiara jest gotowa na coraz bardziej radykalne działania.

Strach przed utratą okazji. Presja nie zawsze opiera się na groźbie. Równie skutecznie działa obietnica, która zaraz przepadnie. W języku marketingu mówi się o strachu przed przegapieniem okazji. Oszuści korzystają z niego w sklepach internetowych, w ofertach wynajmu, w reklamach inwestycyjnych i w ogłoszeniach o pracy.

Typowe sformułowania to „tylko dziś", „ostatnie sztuki", „promocja kończy się o północy", „limitowany dostęp do inwestycji", „zostały trzy miejsca w programie", „cena obowiązuje tylko dla pierwszych stu osób". Na

stronach fałszywych sklepów można zobaczyć licznik osób, które w tej chwili oglądają produkt, albo powiadomienia o tym, że ktoś z sąsiedniego miasta właśnie dokonał zakupu. Wszystkie te elementy mają sprawić, że zwłoka wyda się kosztowna.

Obietnica zysku działa na tej samej zasadzie co groźba straty. W obu przypadkach ofiara czuje, że musi zdecydować szybko, bo inaczej coś straci: w pierwszym przypadku pieniądze, które ma, w drugim pieniądze, które mogłaby zarobić. Psychologowie zwracają uwagę, że ludzie silniej odczuwają stratę niż równoważny zysk, dlatego oszuści często łączą oba mechanizmy. Wiadomość obiecuje wysoki zwrot z inwestycji, a jednocześnie zaznacza, że kto nie dołączy dziś, straci jedyną taką szansę.

Prawdziwe okazje rzadko zależą od tego, czy zdecydujesz w ciągu kwadransa. Nawet jeśli promocja faktycznie się kończy, jej utrata jest drobną niedogodnością w porównaniu z ryzykiem utraty pieniędzy w fałszywym sklepie. W przypadku inwestycji zasada jest jeszcze prostsza: oferta, która wymaga natychmiastowej decyzji, nie jest inwestycją, tylko presją.

Strach przed utratą okazji wykorzystuje też porównanie z innymi. Reklamy fałszywych inwestycji często mówią: „Twoi sąsiedzi już zarabiają", „Tysiące Polaków skorzystały, a Ty wciąż czekasz". Taka narracja wywołuje poczucie, że ktoś inny korzysta z czegoś, z czego my nie korzystamy, i że zwłoka oznacza pozostawanie w tyle.

Dobrym sposobem obrony jest odwrócenie pytania. Zamiast zastanawiać się, co stracisz, jeśli nie skorzystasz z oferty, zastanów się, co stracisz, jeśli oferta okaże się fałszywa. Przegapiona promocja kosztuje kilkadziesiąt złotych różnicy w cenie. Utracone dane karty albo oszczędności kosztują znacznie więcej.

Co stres robi z ciałem i umysłem. Wiele osób, które padły ofiarą oszustwa, mówi mi potem: „Nie wiem, jak mogłem to zrobić, przecież normalnie nigdy bym tak nie postąpił". Albo: „Nie poznaję siebie w tym, co zrobiłam". To bardzo częsta reakcja i ma ona solidne wyjaśnienie fizjologiczne.

Kiedy czujemy zagrożenie, organizm uruchamia reakcję stresową. Wydzielają się hormony, które przygotowują ciało do szybkiego działania. Przyspiesza tętno, oddech staje się płytszy, mięśnie się napinają. Jednocześnie zmienia się sposób działania mózgu. Uwaga zawęża się do źródła zagrożenia i do najbliższego rozwiązania. Części mózgu

odpowiedzialne za planowanie, analizowanie i ocenę konsekwencji pracują słabiej. Człowiek widzi mniej szczegółów, gorzej zapamiętuje informacje i trudniej mu logicznie myśleć.

Ta reakcja była przydatna, kiedy zagrożenie miało postać drapieżnika i wymagało ucieczki albo walki. Nie sprawdza się w sytuacji, w której trzeba ocenić wiarygodność rozmówcy, przeczytać treść powiadomienia w aplikacji i zdecydować, czy przelać pieniądze. W stanie silnego stresu wykonujemy polecenia, zamiast je analizować. Słuchamy osoby, która wydaje się panować nad sytuacją, i robimy to, co nam każe.

Dlatego pod wpływem silnych emocji nawet osoby ostrożne wykonują polecenia, których normalnie by nie wykonały. To nie jest kwestia inteligencji ani wykształcenia. To kwestia biologii. Wiedza o tym mechanizmie ma dwie korzyści. Po pierwsze, pozwala zrozumieć, że ofiara oszustwa nie jest naiwna, tylko została doprowadzona do stanu, w którym rozsądne myślenie jest bardzo utrudnione. Po drugie, podpowiada, co robić: jeśli zauważasz u siebie przyspieszone tętno, napięcie i poczucie, że musisz natychmiast coś zrobić, to jest najlepszy moment, żeby się zatrzymać.

Stres wpływa także na pamięć. Osoby, które przeżyły oszustwo telefoniczne, często nie potrafią później dokładnie odtworzyć przebiegu rozmowy. Pamiętają pojedyncze zdania i emocje, ale nie kolejność zdarzeń. To jeszcze jeden powód, żeby po zakończeniu podejrzanej rozmowy jak najszybciej zapisać jej szczegóły.

Istnieją proste sposoby, żeby obniżyć poziom stresu w krytycznej chwili. Kilka spokojnych, głębokich oddechów, wydłużenie wydechu, świadome rozluźnienie ramion i dłoni. Pomaga też powiedzenie na głos, co się dzieje: „Ktoś mnie pogania, chcę to sprawdzić". Nazwanie sytuacji uruchamia myślenie analityczne i pozwala odzyskać choć część kontroli nad decyzją.

Presja rozciągnięta na godziny. W prostych oszustwach SMS-owych presja trwa kilka minut, od przeczytania wiadomości do wypełnienia formularza. W bardziej złożonych schematach przestępcy potrafią utrzymywać ją przez wiele godzin, a nawet dni. W relacjach ofiar fałszywych pracowników banku i fałszywych policjantów powtarzają się opisy rozmów trwających trzy, cztery, a nawet siedem godzin bez przerwy.

Taka długa presja ma swoje charakterystyczne elementy. Pierwszym są wielogodzinne rozmowy, w których oszust nie pozwala się rozłączyć, prowadzi ofiarę krok po kroku i zajmuje jej uwagę, nawet kiedy niczego

konkretnego nie trzeba robić. Drugim są kolejne telefony od „różnych osób": konsultanta, przełożonego, pracownika działu bezpieczeństwa, policjanta. Każda z nich potwierdza historię poprzedniej i dodaje nowe szczegóły. Trzecim są wiadomości na kilku kanałach jednocześnie. Ofiara rozmawia przez telefon, a w tym samym czasie dostaje SMS-y, e-maile i wiadomości w komunikatorze, które mają potwierdzać prawdziwość sytuacji. Czwartym jest wymaganie, żeby rozmowa trwała podczas wykonywania przelewu, wypłaty w bankomacie albo wizyty w oddziale banku. Oszust słucha wtedy wszystkiego, co mówi ofiara i osoby wokół niej, i może natychmiast zareagować, jeśli ktoś zacznie zadawać pytania.

Celem takiego działania jest wyczerpanie ofiary i odebranie jej choćby chwili do namysłu. Po kilku godzinach w stresie człowiek jest zmęczony, zdezorientowany i coraz bardziej skłonny zgodzić się na wszystko, byle sytuacja się skończyła. Oszuści to wiedzą i często zostawiają najważniejszą prośbę na koniec, kiedy opór jest najmniejszy.

Jeśli kiedykolwiek znajdziesz się w rozmowie, która trwa długo, a rozmówca nie pozwala jej przerwać, potraktuj to jako jeden z najsilniejszych sygnałów ostrzegawczych. Żadna prawdziwa procedura bankowa ani policyjna nie wymaga wielogodzinnego trzymania klienta na linii.

W relacjach ofiar powtarza się też motyw zmęczenia, które w pewnym momencie zamienia się w obojętność. Po kilku godzinach rozmowy ofiara przestaje się zastanawiać, czy to wszystko ma sens, i po prostu wykonuje kolejne polecenia, żeby sytuacja się skończyła. Oszuści potrafią rozpoznać ten moment i wykorzystują go do najważniejszych operacji, takich jak zaciągnięcie kredytu czy przelanie całych oszczędności.

Jeśli kiedykolwiek przyłapiesz się na myśli „byle to się już skończyło", potraktuj ją jako sygnał alarmowy. To właśnie wtedy rozsądne myślenie jest najsłabsze, a ryzyko największe. Przerwanie rozmowy, nawet w połowie zdania rozmówcy, jest w takiej chwili najlepszą decyzją.

Pośpiech plus pieniądze równa się alarm. Wszystko, co opisałem w tym podrozdziale, można sprowadzić do jednej zasady, którą warto mieć zawsze w pamięci. Każda prośba połączona z pośpiechem i dotycząca pieniędzy, danych lub instalacji aplikacji jest sygnałem alarmowym, niezależnie od tego, kto się kontaktuje. Nie ma znaczenia, czy wiadomość wygląda na wysłaną przez bank, kuriera, urząd, policję czy członka rodziny. Nie ma znaczenia, czy rozmówca jest uprzejmy, czy zna Twoje dane, czy ma na

wszystko odpowiedź. Jeśli pojawiają się jednocześnie dwa elementy, pośpiech i prośba o pieniądze, dane albo instalację, należy się zatrzymać.

Ta zasada jest prosta, ale bardzo skuteczna, bo nie wymaga rozpoznawania konkretnego schematu. Oszuści stale wymyślają nowe historie i podszywają się pod coraz to inne instytucje. Trudno nadążyć za wszystkimi wariantami. Natomiast połączenie presji czasu z prośbą o coś wartościowego występuje niemal zawsze, bo bez niego oszustwo po prostu nie działa.

Najbardziej optymistyczna obserwacja, jaką mogę tu przekazać, jest taka: samo przerwanie kontaktu na kilka minut najczęściej wystarcza, żeby oszustwo się nie udało. Odłożenie telefonu, zamknięcie wiadomości, wyjście z pokoju, wypicie szklanki wody, telefon do kogoś zaufanego. Te kilka minut pozwala stresowi opaść i daje szansę na uruchomienie spokojnego, analitycznego myślenia. Kiedy wracasz do sprawy, często od razu widzisz rzeczy, które wcześniej umknęły Twojej uwadze. A jeśli wiadomość była prawdziwa, nic złego się nie stanie. Prawdziwy bank, kurier czy urząd poczeka na Twoją reakcję znacznie dłużej niż kilka minut.

Warto tę zasadę przekazać bliskim w możliwie prostej formie. Dla dzieci może brzmieć: „Jeśli ktoś każe Ci się spieszyć i chce czegoś z telefonu mamy, najpierw zapytaj mamę". Dla seniorów: „Jeśli ktoś dzwoni w sprawie pieniędzy i mówi, że to pilne, odkładam słuchawkę i dzwonię do syna". Prosta reguła działa lepiej niż długa lista schematów, bo łatwo ją przywołać w stresie.

Można też umówić się z samym sobą na stały odruch. Na przykład taki, że każdą prośbę o pieniądze, która przychodzi niespodziewanie, odkładam co najmniej na dziesięć minut. Ten czas wystarcza, żeby zadzwonić na infolinię, sprawdzić status w aplikacji albo zapytać kogoś o zdanie.

1.3. Zaufanie do autorytetów

Skąd się bierze posłuszeństwo. Od dziecka uczymy się, że niektórym osobom należy się posłuch. Najpierw rodzicom, potem nauczycielom, później przełożonym w pracy, lekarzom, policjantom i urzędnikom. Ta nauka ma sens, bo społeczeństwo nie mogłoby funkcjonować, gdyby każde polecenie trzeba było negocjować od nowa. Kiedy policjant kieruje ruchem na skrzyżowaniu, jedziemy tam, gdzie wskazuje. Kiedy lekarz zleca badanie,

zazwyczaj je wykonujemy. Kiedy bank informuje o zmianie regulaminu, przyjmujemy to do wiadomości.

Siłę tego mechanizmu pokazał w latach sześćdziesiątych ubiegłego wieku amerykański psycholog Stanley Milgram. W jego słynnym eksperymencie uczestnicy mieli wymierzać rzekome kary elektryczne innej osobie, która myliła się w prostym zadaniu pamięciowym. W rzeczywistości nikt nie był rażony prądem, a osoba „karana" była aktorem. Uczestnicy o tym nie wiedzieli. Słyszeli krzyki i prośby o przerwanie, a mimo to duża część z nich, zachęcana spokojnymi poleceniami prowadzącego w fartuchu, doszła do najwyższego poziomu napięcia na skali. Nie robili tego z okrucieństwa. Robili to, bo osoba, którą uznali za autorytet, mówiła im, że tak trzeba i że bierze odpowiedzialność na siebie.

Wnioski z tego eksperymentu bywają dyskutowane, a jego metody budzą dziś zastrzeżenia etyczne. Jedno pozostaje jednak niepodważalne: posłuszeństwo wobec instytucji jest wyuczoną normą społeczną i działa bardzo silnie, często silniej niż własne wątpliwości. Kiedy ktoś przedstawia się jako przedstawiciel banku, policji czy prokuratury, automatycznie przyjmujemy wobec niego postawę współpracy. Zakładamy, że wie więcej od nas, że działa w naszym interesie i że jego polecenia mają uzasadnienie, nawet jeśli go nie rozumiemy.

Oszuści korzystają z tego mechanizmu w sposób bardzo przemyślany. Nie muszą nikogo przekonywać do posłuszeństwa, bo ono już istnieje. Wystarczy, że przekonają Cię, że należą do instytucji, której ufasz.

Posłuszeństwo wobec autorytetów wzmacnia też poczucie przeniesienia odpowiedzialności. Kiedy wykonujemy polecenie urzędnika, policjanta czy pracownika banku, mamy wrażenie, że to on odpowiada za skutki. Skoro bank każe przelać pieniądze, to bank wie, co robi. Ta myśl przynosi ulgę w trudnej sytuacji, bo zdejmuje z nas ciężar decyzji. Oszuści chętnie podsycają to wrażenie, zapewniając, że „bierzemy pełną odpowiedzialność" albo że „wszystko jest objęte procedurą".

Badania nad posłuszeństwem pokazują też, że ludzie łatwiej się sprzeciwiają, kiedy widzą, że ktoś inny się sprzeciwił. W wariantach eksperymentu Milgrama, w których obok uczestnika siedziała osoba odmawiająca wykonania poleceń, posłuszeństwo wyraźnie spadało. To kolejny argument za tym, żeby w podejrzanych sytuacjach jak najszybciej porozmawiać z kimś z zewnątrz.

Instytucje, pod które podszywają się oszuści. Kiedy przeglądam ostrzeżenia publikowane przez CERT Polska, banki i policję, widzę, że lista instytucji wykorzystywanych przez oszustów jest długa, ale powtarzalna. Najczęściej pojawiają się banki, zarówno te największe, jak i mniejsze, regionalne. Zaraz za nimi plasuje się policja, w tym Centralne Biuro Zwalczania Cyberprzestępczości, prokuratura i Komisja Nadzoru Finansowego. Często spotyka się też podszywanie pod Urząd Skarbowy i Krajową Administrację Skarbową, Zakład Ubezpieczeń Społecznych, firmy kurierskie, operatorów telekomunikacyjnych i dostawców energii. Oszuści nie wahają się nawet podszywać pod sam CERT Polska, czyli zespół, który zajmuje się ich zwalczaniem.

Ta lista jest efektem świadomego wyboru. Przestępcy nie podszywają się pod przypadkowe firmy. Wybierają instytucje, którym ludzie ufają, i z którymi mają regularny kontakt. Bank to miejsce, gdzie trzymamy pieniądze, więc wiadomość o zagrożeniu konta natychmiast przykuwa uwagę. Policja i prokuratura budzą respekt i lęk przed konsekwencjami. Urząd skarbowy i ZUS kojarzą się z obowiązkami, których zaniedbanie może skończyć się karą. Kurierzy i operatorzy wysyłają nam wiadomości tak często, że kolejna nie wzbudza zdziwienia.

Każda z tych instytucji ma inną funkcję w scenariuszu oszustwa. Bank służy do wywołania strachu o pieniądze. Policja i prokuratura do wymuszenia posłuszeństwa i tajemnicy. KNF do uwiarygodnienia „bezpiecznych" rozwiązań finansowych. Kurier i dostawca energii do wyłudzenia niewielkich płatności i danych karty. Kiedy zrozumiesz, dlaczego oszust wybrał konkretną instytucję, łatwiej przewidzisz, o co za chwilę poprosi.

Lista instytucji zmienia się też w zależności od pory roku i bieżących wydarzeń. W okresie rozliczeń podatkowych rośnie liczba wiadomości podszywających się pod urząd skarbowy. Przed świętami dominują firmy kurierskie. W czasie powodzi albo innych katastrof pojawiają się fałszywe zbiórki i wiadomości od rzekomych służb kryzysowych. Po głośnych wyciekach danych oszuści podszywają się pod firmę, z której wyciekły dane, i informują o konieczności „zabezpieczenia konta".

Warto więc zwracać uwagę na to, czy wiadomość nie wpisuje się zbyt dokładnie w aktualne wiadomości z mediów. Oszuści śledzą te same serwisy

informacyjne co my i błyskawicznie wykorzystują każdy temat, który budzi emocje.

Siła znanej marki. Zaufanie do autorytetów nie dotyczy wyłącznie instytucji publicznych. Równie silnie działa zaufanie do znanych marek: serwisów zakupowych, firm kurierskich, systemów płatności, operatorów komórkowych czy popularnych sklepów. Kiedy widzimy znane logo i znajomą kolorystykę, mózg automatycznie przypisuje wiadomości wiarygodność, którą zbudowała prawdziwa firma.

Ten proces zachodzi szybciej, niż zdążymy przeczytać treść. Żółte tło i charakterystyczny krój pisma kojarzą się z konkretnym przewoźnikiem paczek. Zielony przycisk z nazwą banku kojarzy się z bankowością elektroniczną. Ikonka systemu płatności kojarzy się z bezpieczną transakcją. Zanim przeczytamy, czego wiadomość od nas chce, już jesteśmy nastawieni na to, że pochodzi od kogoś, kogo znamy.

Oszuści kopiują wygląd prawdziwych firm z dużą starannością. Pobierają logotypy z oficjalnych stron, odtwarzają układ graficzny, a czasem wręcz kopiują całe podstrony wraz z regulaminami i stopkami. Fałszywa strona może być nieodróżnialna od prawdziwej, jeśli patrzy się tylko na to, co widać na ekranie. Różnice kryją się w adresie internetowym, w nadawcy wiadomości i w tym, o co strona prosi. Do tych szczegółów wrócę w rozdziale drugim.

Wniosek jest prosty: wygląd nie jest dowodem autentyczności. Znane logo i kolory to tylko obrazki, które każdy może skopiować. Oceniając wiadomość, warto świadomie odsunąć na bok pierwsze wrażenie i zadać pytanie, czy prawdziwa firma rzeczywiście prosiłaby o to, o co prosi ta wiadomość.

Zaufanie do marki działa także w drugą stronę. Kiedy mamy złe doświadczenia z jakąś firmą, na przykład opóźnioną przesyłkę albo pomyłkę w rachunku, łatwiej uwierzymy w wiadomość o kolejnym problemie z jej strony. Oszuści korzystają więc nie tylko z dobrej reputacji firm, ale również z frustracji klientów, którzy spodziewają się kłopotów.

Szczególnie podatne na podrabianie są marki, których komunikacja z klientem jest bardzo częsta i automatyczna. Firma, która wysyła kilka SMS-ów przy każdej przesyłce, przyzwyczaja klientów do tego, że jej wiadomości są normalne i nie wymagają zastanowienia. Paradoksalnie im lepiej firma informuje klientów, tym łatwiej oszustom podszyć się pod jej komunikaty.

Rekwizyty, które mają uwiarygodnić historię. Kiedy sam wizerunek instytucji nie wystarcza, oszuści sięgają po rekwizyty. Mają one wzmocnić wrażenie, że rozmowa jest oficjalna i że stoi za nią prawdziwa procedura. Spotykam się z nimi w niemal każdej relacji ofiar oszustw telefonicznych.

Pierwszym rekwizytem jest oficjalny język. Rozmówca mówi o „weryfikacji tożsamości", „zabezpieczeniu środków", „procedurze ochronnej", „postępowaniu przygotowawczym" czy „czynnościach operacyjnych". Używa słów, które brzmią poważnie i urzędowo, a jednocześnie są na tyle mgliste, że trudno je zweryfikować. Drugim rekwizytem są numery spraw i sygnatury akt. Ofiara słyszy, że jej zgłoszenie ma numer, który powinna zapisać, albo że toczy się postępowanie o określonej sygnaturze. Trzecim są nazwiska i stopnie służbowe. Rozmówca przedstawia się z imienia i nazwiska, podaje stopień, wydział i numer legitymacji, a czasem prosi, żeby je zanotować. Czwartym są pieczątki, podpisy i loga na dokumentach. Piątym, coraz popularniejszym, są zdjęcia „dokumentów" przesyłane przez komunikator: legitymacji służbowej, nakazu, postanowienia prokuratora albo pisma z bankowym nagłówkiem.

Wszystkie te elementy można łatwo podrobić. Numer sprawy to po prostu ciąg cyfr i liter wymyślony przez oszusta. Nazwisko i stopień służbowy mogą należeć do prawdziwego funkcjonariusza, którego dane znaleziono w internecie, albo być całkowicie zmyślone. Pieczątkę i nagłówek odtworzy każdy edytor graficzny. Zdjęcie legitymacji można spreparować w kilka minut, a w czasach narzędzi sztucznej inteligencji jest to jeszcze prostsze.

Co więcej, prawdziwe instytucje nie przesyłają dokumentów przez komunikatory. Policja nie wysyła zdjęć legitymacji w wiadomościach. Prokurator nie przekazuje postanowień jako plików graficznych w czacie. Bank nie przesyła pism z pieczątkami w aplikacjach do rozmów. Sam fakt, że ktoś próbuje udowodnić swoją tożsamość w taki sposób, powinien wzbudzić czujność.

Coraz częściej rekwizytem jest też dźwięk. W tle rozmowy słychać gwar biura, odgłosy klawiatury, rozmowy innych konsultantów albo komunikaty radiowe typowe dla policji. Takie tło można odtworzyć z nagrania i ma ono jeden cel: przekonać ofiarę, że rozmówca naprawdę siedzi w centrum obsługi klienta albo na komisariacie.

Innym rekwizytem bywa procedura. Rozmówca prosi o zanotowanie numeru zgłoszenia, każe powtórzyć dane, informuje, że rozmowa jest

nagrywana „dla bezpieczeństwa klienta", zadaje pytania kontrolne. Wszystko to sprawia wrażenie profesjonalnego procesu. Prawdziwe procedury rzeczywiście tak wyglądają, dlatego ich naśladowanie jest tak skuteczne. Różnica tkwi w celu, do którego procedura prowadzi.

Dane, które oszust już zna. Jednym z najbardziej mylących elementów rozmów z oszustami jest to, że często znają oni wiele informacji o swoich ofiarach. Rozmówca zwraca się po imieniu i nazwisku, zna adres, numer PESEL, nazwę banku, a czasem nawet ostatnie cyfry karty płatniczej albo informację o niedawnej transakcji. Ofiara myśli wtedy: skoro ten człowiek ma moje dane, musi dzwonić z banku. Kto inny mógłby je znać?

Odpowiedź jest niestety prosta: bardzo wiele osób. W ostatnich latach doszło do licznych wycieków danych z firm, sklepów internetowych, przychodni, szkół i instytucji. Dane z tych wycieków są gromadzone, łączone i sprzedawane w przestępczym obiegu. Do tego dochodzą informacje, które sami udostępniamy w mediach społecznościowych: imię, nazwisko, miejsce pracy, miejscowość, imiona członków rodziny, a nawet zdjęcia z urodzin, które pozwalają odgadnąć datę urodzenia. Ostatnie cyfry karty pojawiają się na paragonach i potwierdzeniach zamówień. Nazwę banku można odgadnąć z dużym prawdopodobieństwem, bo kilka instytucji obsługuje większość klientów w Polsce.

Oszuści często stosują też prosty trik: podają informację ogólną i czekają, aż ofiara ją uzupełni. Mówią na przykład: „Dzwonię w sprawie Pana rachunku w naszym banku", a rozmówca odpowiada: „W PKO?". Od tej chwili oszust wie, z jakim bankiem ma do czynienia, a ofiara pamięta, że to on wiedział, gdzie ma konto.

Dlatego znajomość Twoich danych przez rozmówcę nie potwierdza, że dzwoni z prawdziwej instytucji. Potwierdza tylko, że te dane są dostępne. Prawdziwy pracownik banku rzeczywiście zna Twoje dane, ale znają je również przestępcy, którzy zdobyli je z wycieku. Tożsamość rozmówcy trzeba sprawdzić w inny sposób, o czym piszę w rozdziale trzecim.

Warto też pamiętać, że część danych oszust może zdobyć w trakcie samej rozmowy. Pytania zadawane pod pozorem weryfikacji tożsamości, takie jak „Proszę potwierdzić datę urodzenia" albo „Proszę podać ostatnie cztery cyfry numeru dowodu", mogą służyć do zbierania informacji, których przestępcy jeszcze nie mają. Po zakończeniu rozmowy oszust wie więcej, niż wiedział na jej początku, nawet jeśli ofiara nie straciła pieniędzy.

Dlatego dobrą zasadą jest niepodawanie żadnych danych osobowych w rozmowie, której nie zainicjowało się samodzielnie. Jeśli ktoś dzwoni i prosi o potwierdzenie danych, możesz odpowiedzieć, że oddzwonisz na oficjalny numer instytucji i tam je potwierdzisz.

Łańcuch autorytetów. Jedną z technik, które szczególnie skutecznie wzmacniają wiarygodność oszustwa, jest przekazywanie rozmowy kolejnym, coraz „ważniejszym" osobom. Zaczyna się od konsultanta infolinii, który informuje o problemie. Po chwili konsultant mówi, że sprawa jest poważna i musi przełączyć rozmowę do przełożonego. Przełożony potwierdza zagrożenie i przekazuje sprawę do działu bezpieczeństwa. Pracownik działu bezpieczeństwa informuje, że w sprawę zaangażowana jest policja, i łączy z policjantem prowadzącym sprawę. Policjant mówi, że konieczna jest współpraca z prokuraturą.

Każda kolejna osoba wnosi do rozmowy nowy autorytet. Ofiara słyszy, że jej sprawą zajmuje się już nie jedna osoba, ale cały zespół, a nawet kilka instytucji. Historia staje się coraz poważniejsza i coraz bardziej przekonująca. Trudno uwierzyć, że ktoś zadałby sobie tyle trudu, żeby wymyślić tak rozbudowaną opowieść. A jednak dokładnie tak działają zorganizowane grupy oszustów, w których role są podzielone, a każdy członek grupy ma przygotowaną swoją kwestię.

Łańcuch autorytetów ma też inną funkcję. Każde przekazanie rozmowy to sygnał dla ofiary, że problem jest pilny i rośnie. Jednocześnie każda kolejna osoba jest „wyżej" w hierarchii, więc kwestionowanie jej słów wydaje się jeszcze trudniejsze. Jeśli zwykły konsultant mógłby się mylić, to czy może mylić się również jego przełożony, dział bezpieczeństwa i policjant?

Warto pamiętać, że w prawdziwych instytucjach takie przekazywanie rozmów zdarza się rzadko, a jeszcze rzadziej prowadzi do połączenia z policją lub prokuraturą. Bank nie przełącza klientów do policjantów. Policjant nie dzwoni do obywatela, żeby wspólnie z nim zabezpieczać pieniądze na rachunku. Jeśli rozmowa w ciągu kilkunastu minut przeszła przez kilka coraz ważniejszych osób, to właśnie ta dynamika jest sygnałem, że coś jest nie tak.

Przekazanie rozmowy ma też funkcję praktyczną dla przestępców. Pozwala zmienić ton rozmowy bez utraty wiarygodności. Pierwszy rozmówca może być uprzejmy i spokojny, a kolejny stanowczy i wymagający. Ofiara, która opierała się prośbom miłego konsultanta, może

ulec naciskom surowego „funkcjonariusza”. Każda osoba w łańcuchu odgrywa inną rolę psychologiczną.

Łańcuch autorytetów pojawia się również w formie pisemnej. Ofiara dostaje kolejno e-mail z banku, pismo z rzekomej prokuratury, dokument z logo KNF i wiadomość od „kancelarii prawnej”. Każdy dokument potwierdza poprzedni i dodaje kolejną instytucję do historii. Prawdziwe instytucje nie tworzą takich łańcuchów korespondencji z jednym obywatelem w ciągu kilku godzin.

Czego prawdziwe instytucje nie robią. Zamykając ten podrozdział, chcę zebrać w jednym miejscu kilka zasad, które pozwalają odróżnić prawdziwą instytucję od oszusta niezależnie od tego, jak przekonujący jest rozmówca i jakimi rekwizytami się posługuje. Zasady te dotyczą banków, policji, prokuratury, urzędów, KNF i wszystkich innych instytucji, pod które podszywają się przestępcy.

Prawdziwe instytucje nie proszą o przelew na „bezpieczne konto”, „konto techniczne” ani „rachunek zabezpieczający”. Takie konta nie istnieją. Prawdziwe instytucje nie odbierają pieniędzy w gotówce, ani osobiście, ani przez kuriera, ani przez wpłatomat. Nie zlecają instalacji aplikacji na telefonie lub komputerze, zwłaszcza programów do zdalnego dostępu. Nie proszą o kody z SMS-ów, kody autoryzacyjne, hasła do bankowości ani kody BLIK. Nie żądają zachowania tajemnicy przed bliskimi ani przed własnym bankiem.

Te pięć zasad warto zapamiętać tak dokładnie, żeby przypominały się automatycznie w każdej podejrzanej sytuacji. Jeśli rozmówca prosi o którąkolwiek z tych rzeczy, nie ma znaczenia, kim się przedstawia, jak brzmi, co wie i jakie dokumenty pokazuje. Prośba o którąkolwiek z tych rzeczy wystarcza, żeby zakończyć rozmowę. Nie trzeba niczego tłumaczyć, nie trzeba być uprzejmym, nie trzeba czekać, aż rozmówca skończy. Wystarczy się rozłączyć.

Warto mieć tę listę zapisaną w widocznym miejscu, na przykład na kartce przy telefonie stacjonarnym albo w notatce w portfelu. W stresie trudno przypomnieć sobie nawet proste zasady, a kartka z pięcioma punktami może przypomnieć o nich w odpowiednim momencie. Dobrze sprawdza się też przekazanie takiej kartki starszym członkom rodziny.

Prawdziwe instytucje robią natomiast kilka rzeczy, które warto znać. Zachęcają do samodzielnego oddzwonienia na oficjalny numer. Pozwalają

przerwać rozmowę i wrócić do sprawy później. Przesyłają ważne informacje oficjalnymi kanałami, takimi jak bankowość internetowa, list polecony albo skrzynka w serwisie urzędowym. Jeśli rozmówca utrudnia którąkolwiek z tych rzeczy, nie działa w imieniu prawdziwej instytucji.

1.4. Każdy może być ofiarą

Skala zjawiska w liczbach. Kiedy rozmawiam ze znajomymi o oszustwach internetowych, często słyszę, że to problem marginalny, który dotyczy nielicznych pechowców. Liczby pokazują coś zupełnie innego. W chwili, gdy piszę tę książkę, najnowszy raport roczny CERT Polska, zespołu reagowania na incydenty bezpieczeństwa działającego w NASK, dotyczy 2025 roku. Zespół przyjął w tym czasie ponad 658 tysięcy zgłoszeń, czyli o około 10% więcej niż rok wcześniej. Po ich przeanalizowaniu obsłużono 260,8 tysiąca incydentów, a więc przypadków, w których rzeczywiście doszło do zagrożenia lub próby ataku. To ponad dwa i pół raza więcej niż w roku 2024.

Jeszcze bardziej wymowna jest struktura tych incydentów. Aż 97% stanowiły oszustwa komputerowe, czyli przypadki, w których przestępcy próbowali wyłudzić pieniądze lub dane. Dominował phishing i fałszywe inwestycje. Klasyczne ataki techniczne, takie jak złośliwe oprogramowanie czy włamania do systemów, stanowiły niewielki ułamek. Statystyka ta potwierdza to, o czym pisałem na początku rozdziału: współczesna przestępczość internetowa to przede wszystkim manipulowanie ludźmi.

Przy takiej skali każdego dnia do CERT Polska trafiało średnio około 1800 zgłoszeń, z czego ponad 700 okazywało się prawdziwymi incydentami. Na listę ostrzeżeń przed niebezpiecznymi stronami trafiło w 2025 roku około 250 tysięcy domen, co oznacza średnio kilkaset nowych fałszywych stron dziennie. Dzięki tej liście zablokowano około 140 milionów prób wejścia na niebezpieczne witryny. Te liczby obejmują wyłącznie przypadki, które zostały zgłoszone lub wykryte. Rzeczywista skala jest większa, o czym napiszę pod koniec tego podrozdziału.

Dane z kolejnych lat będą się oczywiście zmieniać. Raporty CERT Polska są publikowane co roku i warto do nich zaglądać, żeby wiedzieć, jakie schematy są w danym momencie najpopularniejsze. Trend od kilku lat

pozostaje jednak niezmienny: oszustw przybywa, a przestępcy stają się coraz sprawniejsi.

Za statystykami kryją się konkretne ludzkie historie. Siedemset prawdziwych incydentów dziennie oznacza, że każdego dnia setki osób w Polsce trafiają na fałszywą stronę, odbierają telefon od oszusta albo tracą pieniądze. Wiele z nich to nasi sąsiedzi, współpracownicy i członkowie rodzin, choć rzadko o tym mówią.

Raporty CERT Polska pokazują też, jak zmienia się struktura zagrożeń. Rośnie udział oszustw inwestycyjnych, pojawiają się nowe formy wykorzystania sztucznej inteligencji, a przestępcy coraz sprawniej łączą różne kanały kontaktu. Te zmiany warto śledzić, bo wiedza sprzed dwóch lat może dziś nie wystarczać.

Mit seniora jako jedynej ofiary. Jednym z najbardziej rozpowszechnionych przekonań na temat oszustw jest to, że ulegają im głównie osoby starsze. W mediach najczęściej pojawiają się historie emerytów, którzy przekazali oszczędności fałszywemu wnuczkowi albo fałszywemu policjantowi. Takie przypadki rzeczywiście się zdarzają i są szczególnie bolesne, bo dotyczą osób, które często tracą dorobek całego życia. Wizerunek ofiary oszustwa jako starszej, nieobeznanej z technologią osoby jest jednak bardzo niepełny.

Osoby młode i w średnim wieku również padają ofiarą oszustw, tylko innych schematów. Ich straty rzadziej trafiają na pierwsze strony gazet, bo pojedyncze kwoty bywają mniejsze, a same ofiary rzadziej o nich mówią. W wielu kategoriach oszustw to właśnie młodsze osoby stanowią większość poszkodowanych. Dotyczy to zakupów w internecie, sprzedaży na portalach ogłoszeniowych, ofert pracy i oszustw związanych z grami komputerowymi.

Przekonanie, że oszustwa dotyczą tylko seniorów, jest groźne z dwóch powodów. Po pierwsze, usypia czujność osób młodszych, które uważają się za odporne. Po drugie, utrwala krzywdzący stereotyp, w którym ofiara oszustwa to ktoś mniej sprawny, mniej rozgarnięty albo zbyt ufny. Tymczasem, jak pokażę dalej, podatność na oszustwo ma niewiele wspólnego z wiekiem czy sprawnością.

Stereotyp ma też inną szkodliwą stronę. Kiedy młodsza osoba padnie ofiarą oszustwa, często wstydzi się bardziej, niż wstydziłby się senior, bo przecież „to się zdarza tylko starszym”. Ten wstyd sprawia, że rzadziej

zgłasza sprawę i rzadziej szuka pomocy. W efekcie statystyki jeszcze bardziej zaniżają liczbę młodszych ofiar, a stereotyp się utrwala.

W rzeczywistości różnice dotyczą raczej rodzaju strat niż samego ryzyka. Seniorzy częściej tracą duże kwoty jednorazowo, w oszustwach telefonicznych. Młodsze osoby częściej tracą mniejsze kwoty, ale wielokrotnie, w różnych schematach internetowych. Łączna skala strat w obu grupach jest bardzo poważna.

Kto jest celem jakich oszustw. Różne grupy wiekowe i zawodowe trafiają na różne rodzaje oszustw, bo przestępcy dopasowują scenariusze do tego, z czym dana osoba ma do czynienia na co dzień. Nie będę tu opisywał mechanizmów działania poszczególnych schematów, bo poświęcam im kolejne rozdziały. Chcę jedynie pokazać, jak szeroko rozkłada się ryzyko.

Seniorzy są najczęściej celem oszustw telefonicznych: na wnuczka, na policjanta, na fałszywego pracownika banku. Wynika to z tego, że wiele starszych osób chętnie odbiera telefony, ma oszczędności zgromadzone na koncie lub w gotówce i jest wychowanych w przekonaniu, że instytucjom należy się posłuch.

Osoby młode najczęściej padają ofiarą oszustw zakupowych, fałszywych ogłoszeń o pracy i oszustw w grach. Robią dużo zakupów w internecie, sprzedają używane rzeczy na portalach ogłoszeniowych, szukają dorywczej pracy i spędzają czas w grach, w których handluje się wirtualnymi przedmiotami.

Osoby w średnim wieku są szczególnie często celem fałszywych inwestycji. Mają już pewne oszczędności, myślą o zabezpieczeniu przyszłości, a przy tym korzystają z mediów społecznościowych, w których pojawiają się reklamy obiecujące wysokie zyski.

Przedsiębiorcy najczęściej trafiają na fałszywe faktury i fałszywe zamówienia. Codziennie otrzymują dużo korespondencji, regularnie płacą kontrahentom i często działają w pośpiechu.

Ten podział jest oczywiście uproszczony. Każdy z nas może trafić na każdy rodzaj oszustwa. Warto jednak wiedzieć, na co najbardziej uważać w swojej sytuacji życiowej, i pomyśleć też o tym, na co narażeni są nasi rodzice, dzieci czy współpracownicy.

Wiedza nie zapewnia odporności. Często słyszę zdanie: „Mnie by się to nie zdarzyło, przecież znam się na komputerach”. Rozumiem tę pewność, ale doświadczenie pokazuje, że jest ona złudna. Wykształcenie, wiek i

kompetencje cyfrowe nie chronią przed oszustwem. Ofiarami bywają informatycy, prawnicy, lekarze, nauczyciele, a nawet pracownicy banków, którzy na co dzień zajmują się bezpieczeństwem transakcji.

Jak to możliwe? Odpowiedź tkwi w tym, że oszustwo trafia w moment, a nie w poziom wiedzy. Ekspert od bezpieczeństwa, który na szkoleniu bez trudu rozpozna fałszywą wiadomość, w innym kontekście może zachować się zupełnie inaczej. Wystarczy, że wiadomość przyjdzie w chwili, gdy czeka na przesyłkę, jest zmęczony po całym dniu pracy, prowadzi samochód, rozmawia z dzieckiem i jednocześnie odpisuje na maila. Wystarczy, że historia opowiedziana przez rozmówcę trafi w jego aktualne zmartwienie. Wiedza nie znika w takich chwilach, ale nie zostaje uruchomiona, bo szybki, automatyczny tryb myślenia działa szybciej niż ten analityczny.

Co więcej, osoby, które uważają się za dobrze przygotowane, bywają szczególnie narażone na bardziej wyrafinowane schematy. Oszuści wiedzą, że do różnych grup trzeba trafiać różnymi metodami. Dla osób obeznanych z technologią przygotowują wiadomości bez błędów, strony bez śladów podróbki i scenariusze dopasowane do ich pracy. Przykładem jest atak na firmę, w którym przestępca podszywa się pod kontrahenta i prosi o zmianę numeru konta do płatności. Mało kto spodziewa się w takiej sytuacji oszustwa, bo wszystko wygląda na rutynową korespondencję.

Dlatego najlepszą postawą nie jest przekonanie o własnej odporności, tylko świadomość, że każdy może zostać oszukany i że czujność trzeba zachować niezależnie od wiedzy i doświadczenia.

Paradoksalnie wiedza może czasem zwiększać ryzyko. Osoba, która dobrze zna zagrożenia, bywa przekonana, że od razu rozpozna oszustwo, i dlatego nie stosuje prostych zasad ostrożności, takich jak samodzielne oddzwanianie do banku. Uważa, że skoro zna mechanizmy, nie musi niczego sprawdzać. Tymczasem nawyki chronią skuteczniej niż wiedza, bo działają także wtedy, gdy uwaga jest osłabiona.

Dlatego w tej książce, oprócz opisów schematów, przedstawiam proste reguły postępowania. Ich zaletą jest to, że nie wymagają oceny, czy dana sytuacja jest oszustwem. Wystarczy je stosować zawsze, niezależnie od tego, jak wiarygodna wydaje się wiadomość.

Sytuacje, które zwiększają podatność. Skoro oszustwo trafia w moment, warto wiedzieć, jakie momenty są szczególnie niebezpieczne. Z rozmów z

poszkodowanymi i z analiz publikowanych przez specjalistów wynika, że pewne sytuacje życiowe wyraźnie zwiększają ryzyko.

Pierwszą jest zmęczenie. Po długim dniu pracy, po nieprzespanej nocy albo w okresie przewlekłego stresu nasz umysł częściej korzysta z automatycznych reakcji. Drugą jest pośpiech w pracy, kiedy trzeba załatwić wiele spraw naraz i każda wiadomość jest kolejną rzeczą do odhaczenia. Trzecią jest choroba, zwłaszcza połączona z gorączką, bólem lub przyjmowaniem leków, które wpływają na koncentrację.

Czwartą sytuacją jest samotność. Osoby, które mają niewiele kontaktów z innymi ludźmi, są bardziej podatne na oszustwa oparte na relacji, a także na rozmowy telefoniczne z kimś, kto okazuje zainteresowanie i życzliwość. Piątą jest żałoba. Po stracie bliskiej osoby człowiek jest emocjonalnie wyczerpany, często musi załatwiać wiele formalności i łatwiej ulega presji. Szóstą są problemy finansowe, które zwiększają podatność na obietnice szybkiego zarobku, pożyczki bez weryfikacji i oferty pracy z wysokim wynagrodzeniem.

Siódmą sytuacją jest przeprowadzka, w czasie której zmienia się wiele umów, adresów i dostawców, a wiadomości o niedopłatach i zmianach danych wydają się naturalne. Ósmą jest oczekiwanie na przesyłkę, które sprawia, że SMS od kuriera trafia w realną potrzebę. Dziewiątą jest sprzedaż czegoś w internecie, kiedy czekamy na kontakt od kupującego i jesteśmy nastawieni na szybkie sfinalizowanie transakcji.

Nie chodzi o to, żeby w takich okresach unikać internetu czy telefonu. Chodzi o świadomość, że w tych chwilach warto zachować szczególną ostrożność i dać sobie więcej czasu na decyzje dotyczące pieniędzy i danych.

Masowość i automatyzacja. Wielu osobom wydaje się, że oszuści wybierają swoje ofiary starannie i że trzeba czymś zwrócić ich uwagę, żeby stać się celem. W rzeczywistości większość oszustw działa na zasadzie masowej wysyłki. Przestępcy wysyłają tysiące, dziesiątki tysięcy, a nawet miliony wiadomości. Wykonują setki połączeń dziennie, często z pomocą automatów, które wybierają numery i przełączają rozmowę do człowieka dopiero wtedy, gdy ktoś odbierze.

Przy takiej skali działania przestępcom wystarcza skuteczność rzędu ułamka procenta. Jeśli z dziesięciu tysięcy wysłanych SMS-ów tylko kilka osób kliknie w link i poda dane karty, kampania już się opłaca. Koszt wysłania wiadomości jest niewielki, a zysk z jednej udanej próby może

wynosić setki lub tysiące złotych. Skalę zjawiska dobrze widać w danych CERT Polska: tylko w 2025 roku zespół zidentyfikował prawie 800 wzorców fałszywych wiadomości SMS i dzięki ich blokowaniu zatrzymał około 1,9 miliona wiadomości.

Z tego wynika ważny wniosek. Wiadomość od oszusta rzadko jest wymierzona w konkretną osobę. Trafia do każdego, kogo numer telefonu lub adres e-mail znalazł się w bazie przestępców. Nie dostajesz fałszywego SMS-a dlatego, że ktoś uznał Cię za łatwy cel. Dostajesz go, bo Twój numer jest jednym z milionów. To samo dotyczy telefonów od fałszywych konsultantów. Oszust nie wie, z kim będzie rozmawiał, dopóki ktoś nie odbierze.

Automatyzacja dotyczy też samych rozmów. Coraz częściej pierwsze minuty kontaktu prowadzi program, który zadaje pytania, odtwarza nagrane komunikaty i przekazuje rozmowę człowiekowi dopiero wtedy, gdy rozmówca wykaże zainteresowanie. Narzędzia sztucznej inteligencji pozwalają też tworzyć tysiące wersji tej samej wiadomości, żeby utrudnić ich automatyczne blokowanie.

Z perspektywy przestępcy oszustwo jest więc biznesem opartym na liczbach. Im więcej wiadomości wyśle, tym więcej zarobi. Z perspektywy odbiorcy oznacza to, że fałszywa wiadomość jest zjawiskiem codziennym, a nie wyjątkowym. Jej otrzymanie nie świadczy o żadnym błędzie z Twojej strony. Oznacza tylko, że Twój numer krąży w obiegu razem z numerami milionów innych osób.

Złudzenie „mnie to nie dotyczy”. Psychologowie opisują zjawisko nazywane złudzeniem optymizmu. Polega ono na tym, że ludzie oceniają swoje szanse na doświadczenie przykrych zdarzeń jako mniejsze niż szanse innych osób. Uważamy, że to inni częściej chorują, częściej mają wypadki, częściej padają ofiarą przestępstw. My sami jesteśmy bardziej ostrożni, mądrzejsi albo po prostu mamy więcej szczęścia.

W przypadku oszustw to złudzenie jest szczególnie silne. Kiedy czytamy historię kogoś, kto przelał pieniądze fałszywemu pracownikowi banku, myślimy: jak można było się na to nabrać? Przecież to oczywiste. Ta reakcja jest zrozumiała, bo czytamy tę historię na spokojnie, bez stresu, znając zakończenie. Ofiara przeżywała ją w zupełnie innych warunkach.

Przekonanie, że jesteśmy mniej narażeni niż inni, samo w sobie zwiększa ryzyko, bo obniża czujność. Osoba, która uważa, że jej to nie dotyczy, nie

zastanawia się nad wiadomościami, nie sprawdza nadawców i nie przygotowuje się na trudne sytuacje. Kiedy oszustwo w końcu do niej trafia, jest zaskoczona i bezbronna. Znacznie bezpieczniejsza jest postawa, która zakłada, że każdy może zostać celem, a pytanie nie brzmi „czy", tylko „kiedy".

Wstyd i milczenie ofiar. Na koniec tego rozdziału chcę poruszyć temat, który jest dla mnie szczególnie ważny. Wiele osób, które padły ofiarą oszustwa, nikomu o tym nie mówi. Nie zgłasza sprawy na policję, nie informuje banku, nie rozmawia z rodziną. Powodem jest najczęściej wstyd. Ofiary obawiają się, że zostaną uznane za naiwne, że usłyszą „jak mogłeś", „jak mogłaś", że stracą szacunek w oczach bliskich albo współpracowników.

To milczenie ma poważne konsekwencje. Oficjalne statystyki zaniżają skalę zjawiska, bo nie obejmują przypadków, które nigdy nie zostały zgłoszone. Przestępcy pozostają bezkarni i mogą kontynuować działalność. Same ofiary tracą szansę na odzyskanie przynajmniej części pieniędzy, bo w wielu przypadkach liczy się każda godzina od momentu oszustwa. A przede wszystkim zostają same z poczuciem krzywdy, które bywa bardzo trudne do udźwignięcia.

Dlatego chcę jasno powiedzieć coś, co będzie obowiązywać w całej tej książce: winny jest zawsze sprawca, nie osoba oszukana. Oszust to przestępca, który świadomie i z premedytacją przygotował scenariusz, by wyrządzić krzywdę. Osoba oszukana to ofiara przestępstwa, niezależnie od tego, czy sama kliknęła w link, podała kod czy wykonała przelew. Odpowiedzialność za przestępstwo spoczywa na tym, kto je popełnił, a nie na tym, kto mu zaufał.

Kiedy w kolejnych rozdziałach będę opisywał schematy oszustw i sposoby obrony, nie będę tego robił po to, żeby wskazywać, kto popełnił błąd. Będę to robił po to, żeby przestępcom było trudniej. Jeśli kiedyś ktoś z Twoich bliskich powie Ci, że padł ofiarą oszustwa, najważniejsze, co możesz zrobić, to wysłuchać go bez oceniania i pomóc w podjęciu dalszych kroków.