

Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

Seria poradników z przymrużeniem oka ;)

Każda wiadomość wygląda jak oszustwo

Jak nie dać się nabrać w internecie,
ale też nie podejrzewać własnej babci



Mamy problem. Ale spokojnie.
Da się go rozwiązać i jeszcze będzie z czego się pośmiać.

SPIS TREŚCI

INTRO	1
Rozdział 1 - Oszust nie musi być genialny. Wystarczy, że ty masz zły moment.....	9
Rozdział 2 - „Natychmiast” to nie termin. To narzędzie	19
Rozdział 3 - Najgroźniejsza wiadomość wygląda znajomo.	29
Rozdział 4 - Zielona kłódka nie jest certyfikatem uczciwości	39
Rozdział 5 - Nie klikaj tylko dlatego, że przycisk jest niebieski.....	51
Rozdział 6 - „Sam sobie sprawdzę” też można przedawkować	61
Rozdział 7 - Fałszywy sklep nie musi wyglądać fałszywie..	73
Rozdział 8 - Najgorsza ochrona to przekonanie, że ty się nie nabierzesz	84
Rozdział 9 - Minuta, która może uratować ci kilka tysięcy..	97
Rozdział 10 - BLIK nie jest grą w „zgadnij, komu właśnie płacisz”	110
Rozdział 11 - Urząd, policjant i kurier też mogą poczekać trzydzieści sekund.....	123
Rozdział 12 - Jeśli mama mówi twoim głosem, nadal możesz do niej zadzwonić.....	136
Rozdział 13 - Hasło „Kotek123” nie potrzebuje hakera. Potrzebuje cierpliwości	149
Rozdział 14 - Zrób sobie bezpieczne skróty, zanim będziesz ich potrzebować	162

Rozdział 15 - Kliknąłeś. I co teraz?	175
Rozdział 16 - Kiedy metoda zawodzi, uprość ją jeszcze bardziej.....	190
Rozdział 17 - Nie wszystko musisz rozpoznać. Musisz wiedzieć, kiedy się zatrzymać.....	204
Rozdział 18 - Twoim celem nie jest wygrać z internetem...	217
Rozdział 19 - Jak tego znowu nie zepsuć po dwóch tygodniach.....	229
Rozdział 20 - Babcia może być babcią. I to jest dobra wiadomość	241

INTRO

Telefon wibruje. Patrzysz na ekran.

„Twoja paczka nie mogła zostać dostarczona. Dopłać 1,49 zł, aby ponowić dostawę.”

Pierwsza myśl: przecież rzeczywiście czekasz na paczkę.

Druga: ale czy kurier naprawdę potrzebuje ode mnie złotówki czterdzieści dziewięć, żeby odnaleźć drogę do mojego domu?

Trzecia: to oszustwo.

Czwarta: a jeśli nie?

Piąta pojawia się już trzy sekundy później i brzmi mniej więcej tak: może najlepiej nigdy więcej niczego nie zamawiać, nie odbierać telefonu, nie otwierać wiadomości i komunikować się wyłącznie listownie za pomocą gołębia. Gołąb przynajmniej nie prosi o kod BLIK.

Problem polega na tym, że internet rzeczywiście stał się miejscem, w którym warto zachować ostrożność. Fałszywe SMS-y, wiadomości podszywające się pod bank, telefony od „pracownika działu bezpieczeństwa”, lewe sklepy, spreparowane faktury, przejęte konta znajomych, fałszywe inwestycje i linki prowadzące do stron wyglądających niemal identycznie jak prawdziwe. Oszuści nie siedzą już w ciemnym pokoju w kapturze i nie piszą zielonych liter na czarnym ekranie. Czasem piszą poprawną polszczyznę, mają logo, stopkę, numer telefonu i bardzo profesjonalnie brzmiące „Z wyrazami szacunku”.

Brakuje tylko informacji: „Zespół ds. kradzieży pańskich pieniędzy”.

Nic dziwnego, że można przesunąć się za daleko w drugą stronę. Po kilku podejrzanych wiadomościach zaczynasz traktować każdą komunikację jak potencjalną operację wywiadowczą. Bank wysyła SMS? Podejrzane. Kurier? Podejrzany. Allegro? Podejrzane. Kolega pisze: „Hej, masz chwilę?” Jeszcze bardziej podejrzane, bo człowiek, który naprawdę chce tylko porozmawiać, powinien od razu napisać, czego chce. Babcia wysyła link do zdjęć z imieniem cioci Krysi? Babcia została przejęta przez międzynarodową grupę cyberprzestępczą. Nie ma innego wyjaśnienia.

Właśnie tutaj zaczyna się drugi problem. Bezpieczeństwo cyfrowe łatwo pomylić z permanentną paranoją.

Celem nie jest nauczenie się, że nikomu nie wolno ufać. Celem jest nauczenie się, kiedy ufać, kiedy sprawdzić i kiedy bez dyskusji zamknąć wiadomość. To ogromna różnica. Jeśli każdą wiadomość uznasz za prawdziwą, prędzej czy później ktoś wykorzysta twoje zaufanie. Jeśli każdą uznasz za oszustwo, będziesz funkcjonować jak człowiek, który w trosce o bezpieczeństwo przed kradzieżą samochodu sprzedał samochód.

Technicznie skuteczne.

Życiowo umiarkowane wygodne.

Najważniejszą rzeczą, którą trzeba zrozumieć, jest to, że współczesne oszustwa rzadko polegają przede wszystkim na „hakowaniu komputera”. Znacznie częściej ktoś próbuje zhakować ciebie. Twoją uwagę, pośpiech, strach, ciekawość, chciwość, poczucie obowiązku albo naturalną potrzebę pomocy komuś bliskiemu. To dlatego wiadomość brzmi „Twoje konto zostanie zablokowane”, a nie „Proszę spokojnie przeanalizować sytuację w dogodnym terminie”. Oszust potrzebuje, żebyś działał szybciej, niż myślisz.

Masz dwie minuty.

Kliknij teraz.

Potwierdź natychmiast.

Ostatnia szansa.

Bank oczywiście nie wybuchnie za siedemdziesiąt sekund. Ale twój mózg niekoniecznie chce przeprowadzać analizę ryzyka, kiedy właśnie przeczytał, że ktoś wypłaca pieniądze z twojego konta.

I tu pojawia się dobra wiadomość: nie musisz stać się ekspertem od cyberbezpieczeństwa, znać budowy adresów IP ani mieć piwnicy pełnej monitorów pokazujących mapę świata. Większość prób oszustwa można odśiać przy pomocy kilku prostych nawyków. Najważniejszym z nich jest stworzenie niewielkiej przerwy między wiadomością a reakcją.

Przychodzi SMS z banku? Nie klikaj od razu.

Ktoś informuje o problemie z kontem? Otwórz aplikację banku samodzielnie.

Kurier chce dopłaty? Wejdź ręcznie do aplikacji przewoźnika albo sklepu.

Znajomy prosi o pieniądze? Skontaktuj się z nim innym kanałem.

Firma dzwoni z pilną sprawą? Możesz się rozłączyć i oddzwonić na numer znaleziony na jej oficjalnej stronie.

Ta kilkudziesięciosekundowa przerwa jest dla oszusta wyjątkowo niewygodna. Jego scenariusz działa najlepiej wtedy, gdy pozostajesz wewnątrz scenariusza. On dzwoni, on tłumaczy, on podaje numer, on wysyła link, on mówi, co masz zrobić.

Nie dawaj jednej osobie kontroli nad całą rozmową.

To trochę jak kupowanie używanego samochodu od człowieka, który jednocześnie jest sprzedawcą, mechanikiem, rzeczoznawcą i twoim doradcą finansowym. Być może wszystko jest w porządku.

Ale jednak warto zapytać kogoś jeszcze.

W tej książce nie będziemy więc budować listy czterystu siedemnastu możliwych oszustw, ponieważ zanim dotarlibyśmy do pozycji 418, powstałoby sześć nowych. Zamiast tego nauczysz się rozpoznawać mechanizmy, które powtarzają się niezależnie od tego, czy wiadomość dotyczy banku, paczki, dopłaty do prądu, inwestycji w kryptowaluty czy kuzyna, który nagle potrzebuje pięciu tysięcy złotych, mimo że ostatni raz odzywał się na twoim weselu.

Zobaczysz, dlaczego pośpiech jest jednym z ulubionych narzędzi oszustów, jak sprawdzać nadawcę bez prowadzenia cyfrowego śledztwa trwającego do północy, jak reagować na podejrzane telefony, co robić z linkami, jak rozpoznawać fałszywe sklepy i jak weryfikować prośby o pieniądze od znajomych. Będzie też o sytuacjach trudniejszych: wiadomości wyglądającej całkowicie wiarygodnie, przejętym koncie prawdziwej osoby, fałszywym numerze telefonu czy wykorzystaniu sztucznej inteligencji do tworzenia coraz bardziej przekonujących treści.

Ale równie ważne będzie coś jeszcze: nauczysz się nie wpadać w pułapkę sprawdzania wszystkiego siedem razy.

Bo bezpieczeństwo, które wymaga dwudziestu minut analizy każdego SMS-a, szybko staje się nie do utrzymania. Potrzebujesz systemu prostego enough, żeby działał także wtedy, kiedy wracasz zmęczony z pracy, gotujesz obiad, ktoś

pyta cię, gdzie są klucze, a telefon właśnie informuje, że „Twoje konto wymaga natychmiastowej weryfikacji”.

Wtedy nie przypomnisz sobie siedemnastopunktowej procedury z tabelą ryzyka.

Przypomnisz sobie trzy rzeczy.

Nie działaj pod presją.

Nie korzystaj z danych kontaktowych dostarczonych przez podejrzanego nadawcę.

Zweryfikuj sprawę niezależnym kanałem.

To wystarczy zaskakująco często.

A jeśli mimo wszystko coś pójdzie nie tak, również nie będziemy urządzać pogrzebu cyfrowej godności. Kliknięcie podejrzanego linku nie oznacza automatycznie katastrofy. Podanie danych nie oznacza, że niczego nie da się zrobić. Liczy się szybka, spokojna reakcja: zabezpieczenie kont, kontakt z bankiem lub usługodawcą, zmiana hasła tam, gdzie to potrzebne, i ocena tego, jakie informacje faktycznie zostały ujawnione.

Panikowanie jest bardzo widowiskowe.

Procedura jest skuteczniejsza.

Ta książka ma doprowadzić cię do punktu, w którym podejrzana wiadomość nie wywołuje ani automatycznego kliknięcia, ani natychmiastowej wizji człowieka w kominiarce siedzącego gdzieś pod Mińskiem i przejmującego właśnie twoją lodówkę.

Masz ją zobaczyć i pomyśleć:

„Dobra. Sprawdzę.”

Czasem okaże się oszustwem.

Czasem prawdziwą wiadomością.

A czasem naprawdę będzie to babcia.
Babcia też może wysłać dziwny link.
Tylko zwykle bez kodu BLIK.

Rozdział 1 - Oszust nie musi być genialny. Wystarczy, że ty masz zły moment

Jest 17:42. Wracasz z pracy, stoisz w kolejce, ktoś przed tobą próbuje zapłacić kuponem zapisanym na telefonie, który właśnie postanowił zaktualizować system. W jednej ręce trzymasz zakupy, drugą sprawdzasz wiadomości.

SMS.

„Nie udało się dostarczyć przesyłki. Zaktualizuj dane adresowe, aby uniknąć zwrotu.”

Czekasz na trzy paczki.

Oczywiście, że czekasz. Współczesny człowiek niemal zawsze czeka na jakąś paczkę. To już nie stan przejściowy. To styl życia.

Klikasz?

Jeśli odpowiedź brzmi „nigdy”, bardzo dobrze. Tylko nie przywiązuj się za mocno do własnej nieomyślności. Większość osób, które dały się oszukać, również nie rozpoczynała dnia od myśli: „Dzisiaj chętnie podam dane karty przestępcy”.

Oszustwa internetowe rzadko działają dlatego, że ich autor stworzył genialny plan godny międzynarodowego thrillera. Znacznie częściej działają dlatego, że wiadomość trafiła do właściwej osoby w niewłaściwym momencie.

Jesteś zmęczony.

Spieszysz się.

Naprawdę czekasz na paczkę.

Naprawdę masz konto w tym banku.

Naprawdę twoje dziecko jest poza domem.

Naprawdę kupowałeś coś wczoraj przez internet.

Oszust nie musi znać całego twojego życia. Czasem wystarczy mu statystyka.

Jeżeli wyśle wiadomość o paczce do dziesięciu tysięcy osób, spora część rzeczywiście będzie czekała na przesyłkę. Jeśli wyśle informację o problemie z bankiem, część odbiorców będzie klientami tego banku. Jeżeli napisze: „Mamo, zepsuł mi się telefon, to mój nowy numer”, w wystarczająco dużej grupie znajdzie się ktoś, kto ma dziecko w wieku, w którym zepsuty telefon nie brzmi szczególnie egzotycznie.

Nie trzeba wiedzieć, że pani Krystyna ma syna Pawła.

Wystarczy wysłać wiadomość do odpowiednio wielu Krystyn.

To pierwsza ważna rzecz: trafność wiadomości nie jest dowodem jej autentyczności.

„Ale oni wiedzieli, że mam konto w tym banku.”

Być może.

A być może po prostu zgadli.

„Wiedzieli, że czekam na przesyłkę.”

A kto dziś nie czeka?

„Napisali dokładnie w dniu, kiedy miał przyjść kurier.”

To robi wrażenie. Nadal jednak nie jest dowodem.

Nasz mózg ma dużą słabość do zbiegów okoliczności, które pasują do aktualnej sytuacji. Gdy dostajesz fałszywą wiadomość o paczce dwa tygodnie po ostatnich zakupach, odrzucasz ją bez zastanowienia. Gdy przychodzi