Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

Seria poradników z przymrużeniem oka ;)

Jak nie dać się oszukać w internecie i chronić swoje pieniądze

Jak rozpoznawać oszustwa, zabezpieczyć konta i reagować, zanim znikną pieniądze



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

Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

Jak nie dać się oszukać w internecie i chronić swoje pieniądze

Jak rozpoznawać oszustwa, zabezpieczyć konta i reagować, zanim znikną pieniądze

Seria poradników z przymrużeniem oka ;)

Jak nie dać się oszukać w internecie i chronić swoje pieniądze

Max Paradox

Publikacja została przygotowana z wykorzystaniem narzędzi wspomagających proces twórczy, w tym rozwiązań opartych o sztuczną inteligencję. Ostateczna koncepcja, struktura i redakcja należą do autora.

Spis treści

INTRO.....5

Rozdział 1 - Dlaczego rozsądni ludzie dają się nabrać.....11

Rozdział 2 - Czerwone flagi, które wyglądają całkiem normalnie.....22

Rozdział 3 - Oszust najpierw sprzedaje ci zaufanie.....34

Rozdział 4 - „Mnie by nie oszukali”, czyli najdroższe zdanie w internecie.....46

Rozdział 5 - Nie oddawaj obcemu pilota do swojego telefonu 59

Rozdział 6 - Hasło123, czyli jeden klucz do całego życia.....70

Rozdział 7 - Sklep istnieje. Tylko towaru może nie być.....82

Rozdział 8 - Nie sprzedałeś kanapy. Właśnie prawie kupiłeś oszustowi wakacje.....94

Rozdział 9 - Procedura STOP, zanim palec zrobi coś głupiego 108

Rozdział 10 - Zrób z banku sejf, a nie automat do szybkiego tracenia pieniędzy.....123

Rozdział 11 - Wykres zarabia. Ty tylko ciągle dopłacasz.....138

Rozdział 12 - „Mamo, to ja”. A jeśli już nie wystarczy rozpoznać głosu?.....150

Rozdział 13 - Zastrzeż PESEL, zanim ktoś postanowi zostać tobą.....165

Rozdział 14 - Karta ma płacić. Nie rozdawać twoich pieniędzy po internecie.....178

Rozdział 15 - Kliknąłeś. Podałeś dane. Co teraz?.....192

Rozdział 16 - Zabezpieczenia dla ludzi, którzy czasem są ludźmi.....206

Rozdział 17 - Oszust może wrócić. Tym razem jako człowiek, który chce ci pomóc.....221

Rozdział 18 - Pół godziny co kilka miesięcy zamiast paniki raz na pięć lat.....234

Rozdział 19 - Po czym poznać, że znowu zaczynasz ryzykować 248

Rozdział 20 - Nie bój się internetu. Po prostu nie pomagaj oszustom.....262

INTRO

Telefon wibruje. Dostajesz SMS: „Twoja przesyłka została wstrzymana. Dopłać 1,47 zł, aby uniknąć zwrotu". Akurat czekasz na paczkę, więc wszystko wygląda logicznie. Kwota jest śmiesznie mała. Klikasz. Strona przypomina stronę firmy kurierskiej, logo się zgadza, kolory się zgadzają, nawet ten charakterystyczny korporacyjny smutek projektu graficznego wygląda znajomo. Wpisujesz dane karty, zatwierdzasz i wracasz do życia.

Przesyłka kosztowała 1,47 zł.

Lekcja może kosztować znacznie więcej.

Internetowi oszuści nie wygrywają dlatego, że wszyscy nagle staliśmy się idiotami. Gdyby ich metoda polegała na wysyłaniu wiadomości: „Dzień dobry, jestem przestępcą, proszę podać hasło do banku", branża cyberprzestępcza prawdopodobnie przeżywałaby lekki kryzys kadrowy. Problem polega na tym, że dobre oszustwo nie wygląda jak oszustwo. Wygląda jak bank. Kurier. Znajomy. Sklep. Pracownik działu bezpieczeństwa. Okazja inwestycyjna. Wiadomość od dziecka. Telefon z numeru, który wydaje się prawidłowy. Reklama czegoś, czego akurat szukasz.

Czyli wygląda jak wtorek.

CERT Polska ostrzega między innymi przed fałszywymi inwestycjami, sklepami, załącznikami, prośbami o szybki przelew, przejmowaniem danych logowania i podszywaniem się pod zaufane instytucje. KNF opisuje równie szeroki zestaw schematów: phishing, fałszywe SMS-y i e-maile, vishing,

oszustwa w serwisach ogłoszeniowych i mediach społecznościowych, złośliwe aplikacje czy reklamy prowadzące do fałszywych ofert inwestycyjnych.

Innymi słowy: przestępca internetowy nie ma jednego garnituru.

Ma całą garderobę.

Największy błąd polega na przekonaniu, że przed oszustwem chroni nas inteligencja. Oczywiście pomaga wiedza, doświadczenie i zdrowy rozsądek, ale człowiek posiada jeszcze kilka innych funkcji, z których oszuści korzystają wyjątkowo chętnie: strach, pośpiech, ciekawość, chciwość, zaufanie, zmęczenie i niechęć do komplikowania sobie życia. Wystarczy nacisnąć odpowiedni guzik.

„Wykryliśmy podejrzaną transakcję."

Strach.

„Oferta ważna jeszcze przez 10 minut."

Pośpiech.

„Zobacz, kto umieścił twoje zdjęcia tutaj."

Ciekawość.

„Zainwestuj 1000 zł i zarabiaj 400 zł dziennie."

Chciwość.

„Cześć mamo, zepsuł mi się telefon, to mój nowy numer."

Zaufanie.

I nagle rozsądny człowiek, który przez cztery dni porównuje w internecie ceny czajnika różniące się o dziewięć złotych, potrafi w trzy minuty przelać kilka tysięcy obcej osobie.

Ekonomia behawioralna w wersji premium.

To właśnie dlatego ta książka nie będzie próbowała zrobić z ciebie specjalisty od cyberbezpieczeństwa. Nie musisz wiedzieć, jak wygląda infrastruktura serwera przestępczej grupy działającej gdzieś na drugim końcu świata. Nie musisz analizować kodu strony internetowej. Nie musisz kupować czarnej bluzy z kapturem i siedzieć nocą przed trzema monitorami, żeby twoje konto bankowe było bezpieczniejsze.

Musisz przede wszystkim nauczyć się zatrzymywać w odpowiednich momentach.

Bo większość oszustw potrzebuje twojego działania.

Kliknij.

Podaj.

Zainstaluj.

Potwierdź.

Przelej.

Zeskanuj.

Zaloguj się.

Powiedz kod.

Oszuści mogą przygotować scenografię, historię, presję i fałszywą stronę, ale w wielu przypadkach potrzebują jeszcze jednego elementu: ciebie, który wykonasz ostatni krok. Phishing właśnie na tym często polega - oszust podszywa się pod zaufany podmiot i próbuje skłonić ofiarę do ujawnienia danych albo przekazania pieniędzy.

To dobra wiadomość.

Bo skoro ostatni ruch należy do ciebie, można nauczyć się go nie wykonywać.

Nie oznacza to życia w paranoi. Nie musisz odbierać telefonu od własnej matki słowami: „Najpierw uwierzytelnianie wieloskładnikowe". Nie musisz podejrzewać sprzedawcy marchewki na targu o próbę przejęcia bankowości elektronicznej. Chodzi o coś znacznie prostszego: stworzenie kilku nawyków, które uruchamiają się zanim emocje zdążą przejąć sterowanie.

To szczególnie ważne dlatego, że oszuści bardzo lubią sytuacje, w których nie masz czasu myśleć.

Bank dzwoni „natychmiast".

Kurier potrzebuje dopłaty „dzisiaj".

Kupujący z portalu ogłoszeniowego już wysłał pieniądze i wystarczy „odebrać je przez link".

Fantastyczna inwestycja zaraz zniknie.

Ktoś bliski pilnie potrzebuje przelewu.

Pracownik banku każe przenieść środki na „bezpieczne konto".

CERT Polska opisuje właśnie taki wariant podszywania się pod konsultanta banku: rozmówca może przekonywać, że pieniądze są zagrożone i trzeba przelać je na rzekomo bezpieczny rachunek.

Zauważ wspólny element.

Nigdy nie ma czasu zrobić herbaty.

A herbata bywa bardzo skutecznym narzędziem cyberbezpieczeństwa, bo oznacza pięć minut, podczas

których możesz odłożyć telefon, wejść do banku własną drogą, zadzwonić na oficjalny numer, sprawdzić wiadomość albo zapytać bliską osobę, czy rzeczywiście potrzebuje pieniędzy.

Oszuści uwielbiają szybkość.

Ty polubisz opóźnienie.

W tej książce zajmiemy się więc nie tylko oczywistym „nie klikaj podejrzanych linków", bo ta rada jest mniej więcej tak użyteczna jak „nie podejmuj złych decyzji". Problem polega przecież na tym, że link w chwili kliknięcia zazwyczaj nie wygląda podejrzanie. Gdyby obok znajdowała się animowana czaszka oraz napis „UWAGA, ZA CHWILĘ STRACISZ PIENIĄDZE", współczynnik skuteczności phishingu zapewne delikatnie by spadł.

Nauczysz się rozpoznawać presję stosowaną przez oszustów, sprawdzać wiadomości i strony bez doktoratu z informatyki, zabezpieczać najważniejsze konta, rozsądniej korzystać z bankowości, zakupów internetowych i portali ogłoszeniowych oraz reagować, gdy ktoś próbuje podszyć się pod bank, firmę kurierską, urząd, znajomego albo członka rodziny. Przyjrzymy się także fałszywym inwestycjom, cudownym okazjom, przejmowaniu kont, kodom autoryzacyjnym, kartom płatniczym i temu niezwykłemu momentowi, w którym człowiek zaczyna wierzyć, że nieznajomy z internetu naprawdę chce uczynić go bogatym.

Spoiler: zazwyczaj chce uczynić bogatszym siebie.

Będzie też plan awaryjny, bo nawet ostrożny człowiek może się pomylić. Możesz kliknąć. Możesz podać dane. Możesz coś

zatwierdzić, zanim zorientujesz się, że historia się nie zgadza. Wtedy najgorszą strategią jest siedzenie przez dwie godziny i analizowanie, jak mogłeś być tak głupi. W sytuacji zagrożenia liczy się szybka reakcja. Policja zaleca między innymi pilny kontakt z bankiem, gdy konto lub środki mogły zostać przejęte lub wykorzystane; podejrzane SMS-y z linkami można również przekazywać do CERT Polska na numer 8080.

Wstyd nie blokuje przelewu.

Bank czasem może.

Najważniejsze jednak będzie coś innego: nie zamierzamy budować bezpieczeństwa na ciągłym strachu. Internet ma pozostać miejscem, w którym kupujesz, płacisz, rozmawiasz, sprzedajesz, inwestujesz i załatwiasz sprawy. Tylko zamiast ufać każdej wiadomości wyglądającej wystarczająco profesjonalnie, zaczniesz stosować prostą zasadę:

Im bardziej ktoś chce, żebyś działał natychmiast, tym bardziej warto zwolnić.

Oszuści liczą na reakcję.

My zbudujemy procedurę.

A jeżeli dzięki niej choć raz spojrzysz na SMS „Twoja paczka została zatrzymana", odłożysz telefon i pomyślisz: „No dobrze, Sherlocku z firmy kurierskiej, najpierw cię sprawdzimy", ta książka zacznie zarabiać na siebie.

Tym razem twoimi pieniędzmi.

Nie cudzymi.