Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-sec-phishing

BEZPIECZEŃSTWO IT

Phishing, czyli list od banku, który banku nigdy nie widział

W poniedziałek o 8:03 pani Agnieszka otworzyła firmową pocztę. Bank właśnie poinformował ją, że konto zostanie zablokowane za dziewięć minut, chyba że natychmiast potwierdzi tożsamość. Załączono wielki czerwony przycisk. Pan Kierownik, który przechodził obok, zobaczył słowo „PILNE” i natychmiast podniósł rangę wydarzenia do katastrofy narodowej.

— AGNIESZKO! KLIKAMY!

— A pan wie, dokąd prowadzi ten przycisk?

— DO BANKU! PRZECIEŻ JEST LOGO!

— To ja panu wydrukuję logo policji. Będzie pan mógł wystawiać mandaty — odezwał się Grzesiu zza monitora.

Pan Kierownik przystanął.

— GRZESIU, BEZ GŁUPICH ŻARTÓW. MAMY DZIEWIĘĆ MINUT!

— Osiem. Ale złodziejowi też kończy się cierpliwość, więc może poczekać razem z nami.

Wiadomość od banku, który niczego nie wysyłał

Agnieszka otworzyła szczegóły wiadomości. Nadawca nazywał się „Dział Bezpieczeństwa Banku”, a adres wyglądał jak nazwa banku po zderzeniu z klawiaturą.

— Widzi pan? Nazwa wyświetlana to nie dowód, że wiadomość pochodzi z banku — powiedziała.

— ALE MA LOGO!

— Logo można skopiować ze strony banku. Tak samo jak kolor przycisku, podpis prezesa i zdjęcie uśmiechniętej konsultantki.

Grzesiu przysunął krzesło.

— To jest **phishing**: próba nakłonienia człowieka, żeby oddał dane, pieniądze lub dostęp, podszywając się pod kogoś godnego zaufania. Przynęta może przyjść mailem, ale nie musi. Ważniejsze jest oszustwo niż medium.

— Czyli „łowienie” ludzi? — zapytała Agnieszka.

— Dokładnie. Tylko ryba nie dostaje SMS-a z informacją, że jej płetwy wymagają aktualizacji.

— I co robię?

— Nie klikamy. Nie odpisujemy. Otwieramy bank znaną drogą: przez własną zakładkę, aplikację albo ręcznie wpisany, wcześniej zweryfikowany adres. Jeśli naprawdę coś się dzieje, sprawdzimy to tam.

— A ja mogę zadzwonić do banku? — zainteresował się Kierownik.

— Może pan. Ale pod numer, który zna pan z oficjalnej strony lub dokumentów. Nie pod ten dopisany w podejrzanym mailu.

Dziewięć minut do końca świata

Na ściennym zegarze minęły trzy minuty. Pan Kierownik patrzył na nie jak na odliczanie startu rakiety.

— Może to jednak prawdziwy alarm? Dlaczego mieliby kłamać, że zablokują konto?

— Bo **presja czasu** utrudnia spokojne sprawdzanie — odpowiedziała Agnieszka. — Człowiek widzi „ostatnia szansa”, „pilna dopłata”, „nieautoryzowane logowanie” i chce natychmiast coś zrobić.

— A jeśli napiszą „wygrał pan milion”?

— Wtedy też chcą, żeby pan nie myślał, tylko działał. Strach i chciwość mają ten sam guzik.

Grzesiu otworzył prawdziwą aplikację bankową. Żadnego alarmu. Żadnej blokady. Rachunek spokojnie istniał, jakby nie wiedział o zbliżającym się końcu świata.

— No proszę. W banku cisza — powiedział.

— CZYLI MOŻEMY JUŻ ODWOŁAĆ SZTAB KRYZYSOWY?

— Możemy. Tylko proszę wcześniej odwołać zamówione przez pana trzy pizze dla sztabu.

— TEGO NIE ODWOŁUJEMY.

Adres wygląda znajomo. I właśnie o to chodzi

Grzesiu pokazał Agnieszce adres przycisku. Wyglądał przekonująco do momentu, gdy ktoś zaczął czytać całość.

— Proszę spojrzeć: nazwa prawdziwego banku może pojawić się na początku ścieżki, w subdomenie albo jako kawałek zupełnie innej domeny. O tym, do jakiej witryny trafiamy, decyduje rzeczywista nazwa hosta, a nie znajome słowo gdziekolwiek w adresie.

— Czyli napis „bank” nie wystarczy?

— Tak samo jak restauracja „Ambasada Kotleta” nie jest ambasadą.

— A kłódka obok adresu? — zapytał Kierownik. — PRZECIEŻ KŁÓDKA OZNACZA BEZPIECZEŃSTWO!

— **HTTPS** zazwyczaj oznacza szyfrowane połączenie z określonym serwerem. Nie potwierdza uczciwości jego właściciela. Oszust też może mieć poprawny certyfikat TLS.

— To po co ta kłódka?

— Żeby nikt po drodze łatwo nie podsłuchiwał połączenia. Nie żeby sprawdzać, czy człowiek po drugiej stronie jest porządny.

— Jak zamknięta koperta od oszusta?

— Właśnie. O kopertach i pocztówkach opowiadaliśmy przy **HTTP i HTTPS**.

Grzesiu dodał, że samo najechanie kursorem na link bywa pomocne przy ocenie adresu na komputerze, ale na telefonie wygląda to inaczej, a podglądy i skrócone linki nie zawsze wszystko zdradzają. Bezpieczniej nie korzystać z podejrzanego odnośnika w ogóle.

Kurier z paczką, której nikt nie zamawiał

O 8:19 zadzwonił telefon Agnieszki. Wiadomość SMS: „Dopłać 1,49 zł do przesyłki”.

— Nie zamawiałam niczego — zdziwiła się.

— ALE KWOTA MAŁA! — zauważył Kierownik. — MOŻNA ZAPŁACIĆ DLA ŚWIĘTEGO SPOKOJU!

— Właśnie na to liczą. Link może prowadzić do fałszywej bramki płatności. Mała dopłata jest tylko pretekstem do poznania danych karty albo wyłudzenia zgody na operację.

— To też phishing?

— Gdy przynęta przychodzi SMS-em, często mówimy **smishing**. Kiedy oszust dzwoni i udaje konsultanta banku lub pracownika technicznego, mamy **vishing** — od voice phishing.

— Czyli phishing ma tyle odmian co zamówienia naszego Kierownika?

— Więcej. Kierownik zawsze zamawia trzy pizze.

— ZMIENIAM NA CZTERY!

Bank dzwoni i każe ratować pieniądze

Jak na zamówienie odezwał się kolejny telefon. Mężczyzna przedstawił się jako specjalista do spraw bezpieczeństwa banku.

— Wykryliśmy próbę kradzieży. Musi pani natychmiast przenieść środki na rachunek techniczny — oznajmił.

Agnieszka spojrzała na Grzesia, który bezgłośnie pokazał kartkę: „NIE”.

— Proszę podać imię i numer służbowy — odpowiedziała spokojnie.

— Nie mamy czasu! Proszę tylko potwierdzić kod z SMS-a!

— Nie podaję kodów podczas niezamówionych rozmów. Rozłączam się i sama zadzwonię do banku.

Połączenie się urwało. Kierownik wyglądał na urażonego.

— ALE PRZECIEŻ NUMER NA EKRANIE WYGLĄDAŁ JAK BANK!

— Numer prezentowany przy połączeniu również można podrobić — wyjaśnił Grzesiu. — Nazywa się to **spoofingiem identyfikacji dzwoniącego**. Nie zawsze wyświetlany numer mówi prawdę o źródle rozmowy.

— Czyli nie mogę wierzyć własnemu telefonowi?

— Można z niego korzystać. Trzeba tylko pamiętać, że ekran pokazuje informację o połączeniu, nie policyjny dowód tożsamości.

Bank nie potrzebuje Twojego hasła, kodu jednorazowego ani przelewu na „bezpieczny rachunek", żeby uratować pieniądze. Podejrzaną rozmowę najlepiej zakończyć i skontaktować się z instytucją niezależnym, sprawdzonym kanałem.

Jedna faktura, jedna księgowa i bardzo osobisty oszust

Po południu przyszła wiadomość od rzekomego dostawcy. Tym razem nadawca znał nazwę firmy, nazwisko Kierownika i fakt, że pani Agnieszka zatwierdza przelewy.

— To już brzmi poważniej — przyznała.

— Bo to może być **spear phishing**, czyli atak przygotowany pod konkretną osobę lub organizację — odpowiedział Grzesiu. — Oszust może wykorzystać informacje z internetu, korespondencji albo wycieku danych.

— A jeśli pisze do samego prezesa? — zapytał Kierownik, prostując krawat.

— Ataki celowane w osoby na wysokich stanowiskach bywają nazywane **whalingiem**.

— WRESZCIE COŚ DLA KIEROWNICTWA!

— Panie Kierowniku, to nie jest program lojalnościowy.

W mailu proszono o zmianę numeru rachunku na fakturze. Kwota była prawdziwa, nazwa kontrahenta również. Zmieniony był tylko numer konta.

— I właśnie dlatego nie sprawdzamy takich próśb przez „Odpowiedz" — zauważyła Agnieszka. — Gdy ktoś przejął skrzynkę dostawcy, odpowiadamy temu samemu oszustowi.

Grzesiu przytaknął.

— Zmiany danych do płatności potwierdzamy osobnym kanałem, pod wcześniej znanym numerem. To przykład oszustwa na korespondencję biznesową, często określanego jako **BEC — Business Email Compromise**.

Kierownik chwycił telefon.

— TO JA DO NICH ZADZWONIĘ!

— Doskonale. Tylko nie pod numer z tej faktury.

— CORAZ TRUDNIEJ BYĆ BOHATEREM.

Załącznik „faktura”, który bardzo chce być programem

Grzesiu wskazał drugi mail. Załącznik miał nazwę podobną do faktury, ale jego rozszerzenie nie przypominało zwykłego dokumentu.

— Co się stanie, jeśli otworzę? — zapytała Agnieszka.

— Zależy od pliku i zabezpieczeń. Może to być zwykły dokument, ale może też wykorzystywać lukę albo próbować uruchomić szkodliwy kod. Czasem niebezpieczny jest nie sam załącznik, tylko link do strony, która wyłudza logowanie.

— A PDF jest zawsze bezpieczny?

— Nie. Format pliku sam w sobie nie gwarantuje bezpieczeństwa, podobnie jak nazwa „faktura”.

— A przecież mamy antywirusa! — zawołał Kierownik.

— Mamy. Ale antywirus to ochroniarz, nie jasnowidz. Nie zwalnia z myślenia, aktualizacji i ograniczania uprawnień. O ochronie warstwowej mówiliśmy przy **podstawach bezpieczeństwa**.

Agnieszka przeniosła podejrzaną wiadomość do firmowego procesu zgłoszeń, zamiast przesyłać ją całemu działowi z dopiskiem „KLIKNIJCIE I SPRAWDŹCIE”.

Drugi ochroniarz też może dać się oszukać

— Włączymy MFA i po problemie! — ogłosił Pan Kierownik.

— Włączymy, bo to bardzo pomaga — odpowiedział Grzesiu. — Ale nie każdy rodzaj **uwierzytelniania wieloskładnikowego** jest równie odporny na phishing.

— Przecież do hasła dochodzi kod!

— Oszust może próbować wyłudzić również kod, nakłonić do zatwierdzenia powiadomienia albo przechwycić sesję przez stronę pośredniczącą w logowaniu. Są ataki, w których użytkownik loguje się pozornie poprawnie, ale trafia do witryny kontrolowanej przez napastnika.

— Czyli dwa zamki nie wystarczą?

— Dwa zamki są lepsze niż jeden. Ale jeśli sam wpuszcza pan złodzieja do środka, liczba zamków przestaje być najważniejsza.

Klucze bezpieczeństwa i passkeys korzystające z mechanizmów powiązanych z prawdziwą domeną mogą znacząco ograniczać ryzyko typowego phishingu logowania. To inna ochrona niż przepisanie kodu SMS na obcą stronę. Nie oznacza jednak odporności na każdy rodzaj oszustwa.

— To już rozumiem, czemu nie mam klikać „Zatwierdź”, gdy sam się nie loguję — powiedziała Agnieszka.

— Dokładnie. A o hasłach i drugim ochroniarzu będzie osobna opowieść: „Hasła i MFA”.

QR kod prowadzi do tego samego oszusta, tylko okrężną drogą

Na recepcji ktoś zostawił wydruk: „Nowa sieć Wi-Fi dla gości — zeskanuj kod QR, by potwierdzić konto”.

— WRESZCIE COŚ BEZ LINKU! — ucieszył się Kierownik.

— Kod QR może właśnie zawierać link — westchnęła Agnieszka.

— Czyli oszust wydrukował link w kwadracikach?

— Może tak zrobić. **Quishing** to określenie oszustwa phishingowego wykorzystującego kod QR. Telefon po zeskanowaniu może otworzyć fałszywą witrynę.

Grzesiu odwrócił kartkę.

— I proszę nie zakładać, że naklejka na plakacie jest oficjalna tylko dlatego, że plakat wisi w naszym budynku. Ktoś mógł ją przykleić później.

— TO MOŻE ZAKAZAĆ KWADRATÓW?

— Zacznijmy od sprawdzania celu skanowania.

Jeśli jednak ktoś kliknął

O 15:40 Agnieszka weszła do pokoju Grzesia.

— Mam hipotetyczne pytanie.

— O nie. „Hipotetyczne” zawsze oznacza, że ktoś już kliknął.

— Kierownik.

— W CO?! — krzyknął Grzesiu.

— W link do promocji na bezpłatną pizzę dla sztabu kryzysowego.

Pan Kierownik pojawił się w drzwiach.

— TO BYŁA PROMOCJA LIMITOWANA!

— Czy podał pan hasło, kod, dane karty? Pobrał coś? Zatwierdził logowanie? — zapytał Grzesiu.

— TYLKO IMIĘ, MAIL I HASŁO DO KONTA FIRMOWEGO.

Zapadła cisza. Nawet drukarka przestała udawać, że pracuje.

— W takim razie nie zamiatamy sprawy pod dywan — powiedział Grzesiu. — Natychmiast zgłaszamy incydent, z bezpiecznego urządzenia zmieniamy przejęte hasło, wylogowujemy aktywne sesje tam, gdzie można, sprawdzamy ustawienia konta i dostęp. Jeśli hasło było użyte gdzie indziej, zmieniamy je także tam.

— A jeśli ktoś podał dane płatnicze albo zrobił przelew? — zapytała Agnieszka.

— Od razu kontaktuje się z bankiem przez oficjalny kanał, żeby zablokować instrument płatniczy lub spróbować zatrzymać transakcję. Jeśli podejrzewamy szkodliwe oprogramowanie, urządzenie trzeba odpowiednio zabezpieczyć i przekazać do analizy, a nie używać dalej do logowania.

— Czyli nie mam usuwać wiadomości, żeby nikt nie zobaczył? — zapytał Kierownik.

— Właśnie nie. Zachowujemy informacje o zdarzeniu zgodnie z procedurą, żeby ustalić zakres i skutki. Szybkie zgłoszenie jest ważniejsze niż udawanie, że nic się nie stało.

— A jeśli to była tylko strona z pizzą?

— Tym lepiej. Wolę sprawdzić fałszywy alarm niż nie zauważyć prawdziwego włamania.

Po kliknięciu liczy się to, co wydarzyło się dalej. Samo otwarcie odnośnika, wpisanie hasła, uruchomienie pliku i zatwierdzenie płatności to różne sytuacje i mogą wymagać różnych działań. Nie ma jednej magicznej procedury dla wszystkich przypadków.

Raport końcowy z połowu

Następnego dnia Kierownik zwołał konferencję.

— OGŁASZAM NOWĄ POLITYKĘ! NIE WIERZYMY W ŻADNE MAILE!

— To utrudni fakturowanie — zauważyła Agnieszka.

— W ŻADNE TELEFONY!

— To utrudni rozmowy z klientami.

— W ŻADNE KODY QR!

— To utrudni odczytanie menu w restauracji.

Grzesiu stanął przy tablicy.

— Nie chodzi o to, żeby bać się całego Internetu. Chodzi o to, żeby **oddzielać wiadomość od potwierdzenia jej wiarygodności**. Gdy ktoś żąda pośpiechu, hasła, kodu, przelewu, zmiany rachunku albo instalacji programu, sprawdzamy prośbę niezależną drogą.

— Czyli mamy nie ufać każdej wiadomości bez sprawdzenia?

— Szczególnie takiej, która wywiera presję albo prosi o coś wrażliwego.

Agnieszka odłożyła telefon.

— Właśnie dzwonili z pizzerii. Pan Kierownik zamówił wczoraj cztery pizze. Wszystkie prawdziwe.

— A WIĘC JEDNA DOBRA WIADOMOŚĆ!

— Nie do końca. Każda ma dopisek „płatność przy odbiorze”.

— GRZESIU! SPRAWDŹ, CZY TO NIE PHISHING!

— Sprawdzę. Ale najpierw proszę przestać podawać hasło firmowe w zamian za pepperoni.

Komisja do spraw Bezpiecznego Połowu informuje: fałszywy bank nie otrzymał przelewu, fikcyjny kurier nadal czeka na 1,49 zł, a dostawca faktur odzyskał prawidłowy numer rachunku. Pan Kierownik otrzymał nowe hasło i instrukcję, by nie wpisywać go na stronach z pizzą. Na wszelki wypadek odwołano mu dostęp do zamawiania cateringu. 🍕🎣🤣❤️