Bitdefender

Australijskie małżeństwo dzieli się swoją historią utraty ponad 2,5 miliona dolarów w wyniku oszustwa inwestycyjnego

12.02.2024

Sawyerowie chcieli bezpieczniejszego sposobu inwestowania pieniędzy z funduszu emerytalnego. Stali się jednak ofiarami oszustwa inwestycyjnego nie otrzymali wsparcia od ich banku, gdy najbardziej tego potrzebowali. Australijska para ma nadzieję, że upublicznienie ich sprawy zwróci uwagę na niedociągnięcia w obecnych przepisach i skłoni ustawodawców do wprowadzenia reform, które będą lepiej chronić klientów banków przed oszustwami. W Australii ciężar strat wynikających z oszustw w przeważającej mierze spada na ofiary, a banki zazwyczaj zwracają jedynie niewielką część strat swoich klientów, średnio od 2% do 5%.

W jaki sposób małżeństwo padło ofiarą oszustów inwestycyjnych?

Oszustwo inwestycyjne zaczęło się od reklamy w Google obiecującej możliwości inwestycyjne za pośrednictwem „St George Capital", czyli placówki, która twierdziła, że jest powiązana ze znanym St. George Bank.

Kim Sawyer i jego żona kliknęli ogłoszenie, pozostawili dane kontaktowe i odebrali telefon od mężczyzny, który podszywał się pod prawdziwego pracownika St. George Bank.

Między lipcem a wrześniem 2023 r. oszust zbudował relacje z parą, dzieląc się danymi osobowymi i zachowując się bardzo przyjaźnie, pomagając im w dokonywaniu przelewów na konta w Westpac, ANZ, Commonwealth Bank i Bendigo Bank.

„Zawsze mówił: no wiesz, miłego weekendu albo dobrej nocy" – mówi Kim Sawyer. „Wspomniał, że jego żona jest w ciąży. Wierzyliśmy, że mamy do czynienia z prawdziwym pracownikiem St.George Bank".

Za jego radą Kim i jego żona dokonali aż 26 przelewów na kwotę 100 000 dolarów na konta kontrolowane przez oszustów. Oszust przekonał ich nawet do zainwestowania w obligacje korporacyjne Commonwealth Bank rzekomo oferujące 9% zwrotu. Jednak obligacje, które otrzymali e-mailem, za które zapłacili ponad 1 milion dolarów, okazały się fałszywe.

Jak Sawyerowie dowiedzieli się, że stracili pieniądze?

Sawyerowie odkryli, że stracili wszystko, gdy trzy miesiące po oszustwie

skontaktował się z nimi Macquarie Bank, aby poinformować ich, że ich pieniądze są w rękach oszusta. Był to jedyny z zaangażowanych banków, który się odezwał, ale było już za późno, aby zapobiec stratom, a Macquarie Bank odmówił zwrotu jakiejkolwiek z utraconych 850 000 dolarów.

Kiedy para zwróciła się do innych zaangażowanych banków – Westpac, ANZ, Commonwealth Bank i Bendigo Bank – o informacje na temat kont kontrolowanych przez oszustów, nie otrzymali żadnej pomocy. Banki odpowiedziały, że wszystkie środki zostały pobrane i nie mogą powiązać kont z konkretnymi osobami.

Ostatecznie żaden z ośmiu zaangażowanych banków nie zgodził się na zwrot utraconych środków.

Oferta zbyt piękna, aby mogła być prawdziwa i inne sygnały ostrzegawcze

Zwykle oszuści wabią ofiary ofertami, które wydają się zbyt piękne, aby mogły być prawdziwe, ale w tym przypadku obietnica była bardziej realistyczna: ochrona kapitału, ochrona przed wahaniami na rynku i gwarantowany zwrot do 6,5%.

Oszuści często wykorzystują „konta mułowe” do przesyłania środków, co polega na korzystaniu z legalnych kont bankowych osób niezaangażowanych bezpośrednio w oszustwo, zwanych mułami pieniężnymi i rekompensowaniu im części wpływów.

Jednak w tym wypadku Sawyerowie rozpoznali kilka znaków ostrzegawczych dopiero po fakcie. Poniżej wymieniamy najgroźniejsze z nich:

- E-maile wysyłane na ogólne adresy St.George często wracały.

- Podane przez oszusta dane logowania do „internetowego portalu klienta", na którym Sawyerowie mogli rzekomo monitorować swoje inwestycje, wielokrotnie kończyły się niepowodzeniem.

- Adresy e-mail używane do wysyłania potwierdzeń przelewów pieniężnych były fałszywymi adresami St. George Bank, takimi jak info@stgeorge-capital.com lub client@stgeorge-capital.com.

Osiem wskazówek od zespołu Bitdefender, jak uchronić się przed oszustwami inwestycyjnymi

- Sprawdź, z kim masz do czynienia. Zbadaj każdą możliwość inwestycyjną i zweryfikuj legalność firmy lub osoby oferującej ją, kontaktując się z firmą za pośrednictwem jej oficjalnych kanałów (strona internetowa, aplikacja).

- Zrozum inwestycję. Poświęć trochę czasu na zrozumienie oferowanego produktu, w tym związanych z nim zagrożeń, warunków i potencjalnych zysków. Przelewaj pieniądze dopiero po potwierdzeniu uprawnień doradcy i szczegółów inwestycji.

- Uważaj na taktykę nacisku. Uważaj na osoby wywierające na Ciebie presję, abyś podjął szybką decyzję lub namawiające do zachowania poufności inwestycji. Uzasadnione inwestycje dają czas na rozważenie dostępnych opcji.

- Bezpieczne konta internetowe. Jeśli inwestujesz online, upewnij się, że Twoje konta mają silne hasła. Włącz uwierzytelnianie dwuskładnikowe dla większego bezpieczeństwa. Unikaj udostępniania poufnych informacji za pośrednictwem niezabezpieczonych kanałów.

- Bądź na bieżąco. Bądź na bieżąco z typowymi oszustwami inwestycyjnymi i taktykami stosowanymi przez oszustów. Możesz na przykład sprawdzić najnowsze oszustwa i alerty na stronie internetowej instytucji finansowej. Niektóre z nich przedstawiają ostatnie zgłoszone im przykłady oszustw.

- Zasięgnij porady i drugiej opinii. Przed podjęciem jakichkolwiek decyzji inwestycyjnych rozważ konsultację z niezależnym, licencjonowanym doradcą finansowym lub specjalistą ds. inwestycji. Porozmawiaj ze znajomymi i rodziną, mogą oni udzielić cennych wskazówek i pomóc Ci uniknąć oszustw.

- Sprawdzaj reklamy, wiadomości, e-maile i kody QR poprzez Bitdefender Scamio. Bitdefender Scamio to wykrywacz oszustw AI nowej generacji, który pomaga w ciągu kilku sekund sprawdzić każdą wiadomość e-mail phishingową, podstępną wiadomość lub

fałszywą reklamę. Możesz skopiować i wkleić wiadomość, przesłać obraz, wysłać link lub opisać swoją sytuację. Scamio analizuje to i informuje Cię, czy jest to bezpieczne, czy nie.

- Zgłoś podejrzenie oszustwa. Jeśli uważasz, że zetknąłeś się z oszustwem inwestycyjnym lub padłeś ofiarą oszustwa, zgłoś to odpowiednim władzom, takim jak organ nadzoru finansowego w Twoim kraju, CERT Polska, Policja lub agencja ochrony konsumentów, i rozważ zasięgnięcie porady prawnej. Zgłaszanie oszustw może pomóc zapobiec ofiarom innych osób i pomóc w odzyskaniu utraconych środków.

„Oszustwa inwestycyjne to w ostatnich latach coraz częstsza taktyka wykorzystywana przez cyberprzestępców. Warto pamiętać o tym, aby zawsze być sceptycznie nastawionym do ofert zbyt pięknych, aby mogły być prawdziwe i zawsze korzystać z systemu antywirusowego wyposażonego w skuteczny moduł antyphishingowy oraz dedykowane zabezpieczenie do wykonywania płatności online, np. SafePay” - mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/australijskie-malzenstwo-dzieli-sie-swoja-historia-utraty-ponad-25-miliona-dolarow-w-wyniku-oszustwa-inwestycyjnego/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 12.02.2024

Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.