HSBCnet

Inżynieria społeczna

Ryzyko dla firmy:

- Utrata danych
- Straty finansowe
- Fałszywe przekierowania w bankowości internetowej

Czy wiedzą Państwo z kim tak naprawdę rozmawiają przez telefon? Czy email lub wiadomość tekstowa wyglądają na autentyczne? Należy zachować czujność. Złodzieje stosują teraz różne sprytne sposoby kradzieży informacji w celu dokonywania oszustw.

Na czym polega inżyniera społeczna

How Social Engineering works

Phishing
Wiadomości email

Treść wiadomości email może wywoływać poczucie zagrożenia, wrażenie pilności lub zachęcać odbiorcę do kliknięcia łącza lub otworzenia załącznika, w wyniku czego urządzenie zostanie zainfekowane przez wirusa lub złośliwe oprogramowanie.

W ten sposób przestępcy mogą wykraść informacje lub środki pieniężne, lub zakłócić działanie systemu informatycznego.

Chociaż wielu oszustów działa losowo, niektórzy koncentrują się na konkretnych grupach pracowników lub klientów. Takie działania to tzw. phishing profilowany (spear phishing). Jednym z przykładów jest „oszustwo na prezesa". Przestępcy podszywają się pod przedstawicieli wyższej kadry kierowniczej i wydają swoim współpracownikom polecenie przelewu środków na ich konto.

Inną taktyką jest oszustwo polegające na przekierowaniu płatności. Przestępcy wysyłają wiadomość email, w której podają się za przedstawiciela dostawcy. Wiadomość zawiera informację o zmianie danych bankowych i prośbę o dokonanie przelewu na inne konto.

Nie należy odpowiadać na takie wiadomości email.

Vishing
Rozmowy telefoniczne

Oszuści często starają się wzbudzić panikę, aby zmusić rozmówcę do szybkiej reakcji. Oszuści wybierający za swój cel firmy, mogą podszywać się pod członka kadry kierowniczej lub klienta potrzebującego pilnej pomocy.

Oszuści mogą także dzwonić, podając się za pracownika HSBC. Mogą podejmować próby nakłonienia rozmówcy do podjęcia działań, które umożliwią wysłanie nieautoryzowanych płatności do przestępcy. Mogą żądać na przykład podania kodów wygenerowanych przez token.

Wiele kampanii vishingowych jest prowadzonych na dużą skalę, z wykorzystaniem automatycznego wybierania numerów i połączeń za pomocą łączy szerokopasmowych, co umożliwia kontakt z tysiącami potencjalnych ofiar na godzinę.

W przypadku odebrania podejrzanego połączenia nie należy udzielać żadnych informacji.

Smishing
Wiadomości tekstowe

W wiadomościach „smishingowych" oszuści próbują nakłonić odbiorcę do kliknięcia złośliwych łączy aktywujących trojany, które wykradają hasła i inne wartościowe dane.

Wiadomości tekstowe mogą informować o rzekomych podejrzeniach banku jakoby na rachunku ofiary wykonywane były podejrzane transakcje lub że ma ona problemy z urzędem skarbowym lub że wygrała ona nagrodę pieniężną.

Wiadomości smishingowe zazwyczaj wymagają podjęcia pilnych działań, które często wiążą się z koniecznością kliknięcia złośliwego łącza umożliwiającego kradzież danych. Filtry antyspamowe blokują wiele wiadomości phishingowych, ale nie opracowano jeszcze ogólnego rozwiązania, które uniemożliwiałoby dostarczanie wiadomości tekstowych do potencjalnych ofiar.

Nie należy odpowiadać na takie wiadomości tekstowe, ani klikać żadnych łączy w nich zamieszczonych.

Jeżeli którekolwiek z rozmów telefonicznych, wiadomości tekstowych lub wiadomości elektronicznych otrzymanych rzekomo od HSBC wydają się podejrzane, prosimy o kontakt z przedstawicielem HSBC w celu ich zweryfikowania.

HSBC

Sygnały ostrzegawcze	Zalecane działania
Odbierasz połączenie międzymiastowe od nieznanego numeru lub połączenie zostaje przekierowane przez operatora.	Poproś dzwoniącego o przedstawienie się (np. kim jest, skąd dzwoni i dlaczego potrzebuje określonych informacji). Potwierdź tożsamość dzwoniącego, korzystając z procedury weryfikacji obowiązującej w firmie.
Osoby przesadnie przyjazne i sympatyczne albo próbujące Cię zastraszyć twierdzą, że dzwonią w bardzo pilnej lub ważnej sprawie, a nawet grożą złożeniem skargi. Osoby te mogą przytaczać znane informacje, w tym imię i nazwisko Twojego działu lub przełożonego, aby wywrzeć presję i skłonić do ujawnienia informacji.	**Zaufaj swojemu instynktowi.** W przypadku odebrania podejrzanego połączenia, podczas którego dzwoniący prosi o podanie danych dotyczących rachunków bankowych lub pracowników, nie należy udzielać żadnych informacji. Połączenie należy zgłosić zgodnie z wewnętrznymi procedurami obowiązującymi w firmie.
Nietypowe prośby, których spełnienie wymaga „pójścia na skróty" lub odstąpienia od ustalonych procedur.	W razie wątpliwości zadawaj pytania, które pomogą ustalić, czy prośba jest autentyczna. Przed podjęciem dalszych działań skontaktuj się z przełożonym lub menedżerem ds. systemu HSBCnet w celu uzyskania drugiej opinii.
Otrzymujesz wiadomość email, która wydaje się pochodzić od kolegi/koleżanki z pracy. Przy wysyłaniu odpowiedzi adres email odbiorcy zmienia się na adres osoby spoza firmy.	Jeżeli uważasz, że otrzymana wiadomość jest podejrzana, nie odpowiadaj na nią, nie klikaj żadnych łączy i nie otwieraj żadnych załączników. Zgłoś wiadomość administratorowi systemu HSBCnet i prześlij ją dalej na adres: hsbcnet.phishing@hsbc.com. Następnie usuń wiadomość email ze swojej skrzynki odbiorczej.
Otrzymujesz niespodziewaną wiadomość tekstową, której nadawca podaje się za pracownika HSBC i prosi o kliknięcie łącza w celu podjęcia pilnych działań.	Nie klikaj żadnych łączy w otrzymanych niespodziewanie wiadomościach tekstowych. Nie odpowiadaj na wiadomość, korzystając z danych kontaktowych zamieszczonych w wiadomości. W razie wątpliwości zweryfikuj wiadomości, zwracając się do znanych Ci osób wyznaczonych do kontaktu w HSBC.

Jak zabezpieczyć swoją firmę:

- Należy zwiększać świadomość zagrożeń opartych na inżynierii społecznej wśród pracowników firmy oraz wdrażać zasady zgłaszania podejrzanych sytuacji.
- Nigdy nie należy udostępniać nieznanym osobom informacji finansowych ani informacji dotyczących firmy.
- Nie należy spieszyć się z podejmowaniem decyzji.
- Nie należy klikać łączy w wiadomościach tekstowych lub elektronicznych ani otwierać lub pobierać załączników, chyba że mamy pewność, że są bezpieczne.
- Należy zachować ostrożność podczas udostępniania informacji w mediach społecznościowych, gdyż w ten sposób możemy przekazywać oszustom z pozoru mało istotne informacje, które łącznie dają szerszy obraz.
- Należy dzwonić tylko na znane i sprawdzone numery telefonu. Jeżeli ktoś twierdzi, że jest współpracownikiem, należy sprawdzić imię i nazwisko tej osoby w wykazie pracowników danego podmiotu i oddzwonić do tej osoby na jej numer wewnętrzny.
- Wszelkie podejrzane wiadomości email należy przesyłać na adres: **hsbcnet.phishing@hsbc.com.**

W przypadku podejrzenia, że firma padła ofiarą oszustwa, należy skontaktować się bezpośrednio z przedstawicielem HSBC.