Atak *phishingowy* – najczęściej zadawane pytania

1. **Czy jestem bezpieczny/a?**
   Nie możemy jednoznacznie stwierdzić, czy jesteś całkowicie bezpieczny/a. Twoje hasła nie zostały skompromitowane, jednak informacje z treści e-mail mogły zostać ujawnione. W dalszej treści tego zestawienia znajdują się wyjaśnienia oraz wskazówki, które pomogą zwiększyć twoje bezpieczeństwo i zminimalizować ryzyko negatywnych skutków ataków.
2. **Co się wydarzyło?**
   Atakujący przejął dane logowania do skrzynki poczty elektronicznej pracownika placówki CUK w Białymstoku (zlokalizowanej przy ul. Dubois 10) i uzyskał nieautoryzowany dostęp do jej zawartości. Na pewno przejął adresy e-mail, które znajdowały się w tej skrzynce. Wiemy to, bo sprawca następnie wysłał z tej zaatakowanej skrzynki wiadomości o charakterze *phishingowym* na te pozyskane adresy. Istnieje jednak ryzyko, że mógł mieć również dostęp do treści korespondencji (w tym załączników), którą prowadziłeś/aś z zaatakowanym użytkownikiem lub do treści korespondencji e-mail Ciebie dotyczącej (np. między placówką CUK w Białymstoku przy ul. Dubois 10 a zakładem ubezpieczeń, w którym prezentowaliśmy Ci ofertę lub w którym zawarłeś umowę ubezpieczenia). W tej chwili nie mamy potwierdzenia, że doszło do tej drugiej sytuacji. Jednak ze względu na interes i bezpieczeństwo naszych Klientów zalecamy zapoznanie się z poniższymi informacjami i podjęcie dodatkowych środków bezpieczeństwa.
3. **Jakie moje dane wyciekły?**
   Informacja, która na pewno została wykradziona to adres e-mail.
   Informacje, które mogły zostać wykradzione, to dane ze stopki wiadomości, treść wiadomości, załączniki, dane kontaktowe, hasła, numery kont bankowych oraz inne dane osobowe zawarte w skrzynce pocztowej, która została skompromitowana.
4. **Kiedy dane wyciekły?**
   Wyciek miał miejsce 15.05.2024 o godzinie 13.30.
5. **Dlaczego zostałem/zostałam powiadomiona dopiero teraz?**
   Od czasu wykrycia ataku prowadziliśmy przy współpracy z CERT i Microsoft diagnostykę i analizy mające na celu ustalenie czyje dane i w jakim zakresie mogły zostać przejęte. Dopiero teraz mamy wystarczająco dużo informacji, by móc przedstawić Ci bardziej konkretnie stan faktyczny, wskazać zagrożenia i zarekomendować sposób postępowania niwelującego negatywne skutki naruszenia i zabezpieczającego Twoje dane.
6. **Skąd mam wiedzieć czy moje dane inne niż adres e-mail na pewno wyciekły?**
   Jeżeli prowadziłeś korespondencję e-mail z placówką CUK w Białymstoku przy ul. Dubois 10 na adres w domenie cuk.pl, to treści, które były w niej zawarte mogły zostać przejęte. W tej chwili nie możemy tego potwierdzić. Zalecamy jednak

ostrożność i podjęcie profilaktycznych działań minimalizujących skutki prawdopodobnego wycieku danych o szerszym zakresie (zob. pkt 2) i zwiększających bezpieczeństwo.

7. **Kiedy CUK będzie mieć pewność, czy atakujący pozyskał i ew. przekazał dalej dane co do których istnieje na stan obecny prawdopodobieństwo ich pozyskania?**
   Nie możemy zagwarantować, że uzyskanie stuprocentowej pewności będzie w ogóle możliwe. Wynika to ze specyfiki ataku *phishingowego*. Dlatego też zalecamy, by skorzystali Państwo z poniższych rekomendacji w zakresie bezpieczeństwa.
8. **Czy wiadomo, kim jest sprawca?**
   Nie wiemy kim jest sprawca. Nie możemy też zagwarantować, że ustalenie tego będzie możliwe. Wynika to ze specyfiki ataku *phishingowego*.
9. **Czy były już zgłoszone przypadki wykorzystania danych objętych zdarzeniem w sposób nielegalny, np. podszycie się pod kogoś, zaciągnięcie pożyczki?**
   Do tej pory nie otrzymaliśmy żadnego takiego zgłoszenia.
10. **Czy atakujący kontaktowali się z CUK? Czy wysunęli jakieś roszczenia/groźby?**
    Nie, do tej pory sprawca nie kontaktował się z CUK i nie wysunął żadnych roszczeń, czy gróźb.
11. **Jakie mogą być skutki, o ile doszło do przejęcia moich szerszych danych z wiadomości na zaatakowanej skrzynce?**
    Możliwe konsekwencje to:
    - zawieranie na Twoje dane umów ubezpieczenia lub umów kredytów/pożyczek w instytucjach pozabankowych,
    - uzyskanie dostępu przez osobę trzecią do przysługujących Tobie świadczeń opieki zdrowotnej,
    - korzystanie z Twoich praw obywatelskich, np. poprzez oddanie głosu w wyborach powszechnych,
    - wyrobienie na Twoje dane fałszywych dokumentów, np. kolekcjonerskiego dowodu osobistego,
    - zawarcie na Twoje dane umowy, np. najmu nieruchomości,
    - zarejestrowanie na Twoje dane karty telefonicznej typu pre-paid,
    - posłużenie się Twoimi danymi podczas odbioru mandatu.
12. **Czy mogę bezpiecznie używać konta bankowego?**
    Wyciek nie miał bezpośredniego wpływu na bezpieczeństwo Twojego konta bankowego. Za pośrednictwem wysyłanych wiadomości nie było rozpowszechniane złośliwe oprogramowanie. Jednak dobrą praktyką po każdym wycieku jest zmiana haseł, na dłuższe i bardziej skomplikowane. O tym jak stworzyć bezpieczne hasło przeczytasz tutaj: https://www.gov.pl/web/baza-wiedzy/jak-tworzyc-bezpieczne-hasla. Należy również szczególnie uważać na możliwe próby *phishingu* i *smishingu*.

13. **Co to jest *phishing*?**

    Phishing to rodzaj cyberataków, w których przestępcy podszywają się pod zaufane osoby lub instytucje za pomocą fałszywych wiadomości e-mail w celu wyłudzenia poufnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe. Celem jest nakłonienie ofiary do kliknięcia w link i wprowadzenia swoich danych na złośliwej stronie internetowej.

14. **Co to jest smishing?**

    Smishing (*SMS phishing*) to rodzaj *phishingu* przeprowadzanego za pomocą wiadomości SMS. Atakujący wysyłają fałszywe SMS-y, które wyglądają na autentyczne, często zawierające linki do złośliwych stron internetowych lub numery telefonów do fałszywych infolinii, w celu wyłudzenia poufnych informacji lub nakłonienia ofiary do zainstalowania złośliwego oprogramowania.

15. **Czy muszę zmienić hasło?**

    Jeśli nie kliknąłeś/aś w link w wiadomości *phishingowej* otrzymanej z adresu e-mail (w domenie cuk.pl) pracownika palcówki CUK w Białymstoku przy ul. Dubois 10 i nie wpisałeś/aś danych logowania do formularza wyłudzającego lub nie wysłałeś/aś danych logowania mailem na prośbę sprawcy ataku, to nie ma takiego zagrożenia. Atakujący nie miał bezpośredniej możliwości uzyskania dostępu do Twojego hasła. Jednak dobrą praktyką po każdym wycieku jest profilaktyczna zmiana hasła do skrzynki, na dłuższe i bardziej skomplikowane, zob. https://www.gov.pl/web/baza-wiedzy/jak-tworzyc-bezpieczne-hasla. Warto również zabezpieczyć konto wieloskładnikowym uwierzytelnianiem (MFA).

16. **Co to jest MFA?**

    MFA (Multi-Factor Authentication) to wieloskładnikowe uwierzytelnianie, które zwiększa bezpieczeństwo logowania do konta poprzez wymaganie więcej niż jednego dowodu tożsamości. MFA zazwyczaj łączy:

    - Coś, co wiesz (hasło, PIN),
    - Coś, co masz (telefon, klucz USB),
    - Coś, czym jesteś (dane biometryczne, jak odcisk palca).

    Stosowanie MFA znacznie zwiększa bezpieczeństwo konta, ponieważ wymaga dodatkowego potwierdzenia tożsamości, nawet jeśli jedno z uwierzytelnień zostanie skompromitowane.

17. **Czy wyciek ma wpływ na inne moje dane i konta?**

    Wyciek nie miał bezpośredniego wpływu na bezpieczeństwo innych Twoich kont. Za pośrednictwem wysłanych wiadomości nie było rozpowszechniane złośliwe oprogramowanie. Jednak dobrą praktyką po wycieku jest zmiana hasła do powiązanych ze skrzynką serwisów, na dłuższe i bardziej skomplikowane. W miarę możliwości zabezpiecz konta wieloskładnikowym uwierzytelnianiem (MFA). Należy również szczególnie uważać na możliwe próby *phishingu* i *smishingu*.

18. W jaki sposób korzystać teraz z poczty elektronicznej? ? Jak się zabezpieczyć?

- Zalecamy przejrzeć korespondencję e-mail prowadzoną z placówką CUK w Białymstoku (zlokalizowaną przy ul. Dubois 10) na adres w domenie cuk.pl (to wskaże co mogło wyciec).
- Zmień hasło do skrzynki pocztowej.
- Zmień hasła do serwisów powiązanych ze skrzynką pocztową.
- Zmień hasła wszędzie, jeżeli używasz tego samego (lub podobnego) hasła.
- Włącz dwuskładnikowe uwierzytelnianie (MFA).
- Jeżeli starego hasła do poczty (lub podobnego) używałeś w innych serwisach, tam również koniecznie je zmień.
- Sprawdzaj swoją skrzynkę pocztową pod kątem nietypowych wiadomości (również wychodzących, w koszu, archiwum oraz innych nietypowych folderach (np. RSSFeed)).
- Nie klikaj w linki, które wzbudzą jakiekolwiek wątpliwości.
- Nie pobieraj i nie otwieraj załączników do podejrzanych wiadomości.
- Sprawdź, czy od czasu incydentu nie nastąpiły nieautoryzowane logowania.
- Sprawdź, czy w regułach skrzynki nie ma przekierowań na obce adresy email.
- Sprawdź, czy adres odzyskiwania hasła nie został podmieniony.
- Jeżeli otrzymałeś podejrzanego emaila lub trafiłeś na budzącą wątpliwości stronę wyślij zgłoszenie na adres cert@cert.pl lub wypełnij formularz na stronie https://incydent.cert.pl.

19. Jak na przyszłość zabezpieczyć się przed wyciekiem z mojego konta?

- używaj trudnego hasła (12 lub więcej znaków, małe i wielkie litery, cyfry, znaki specjalne),
- używaj menedżerów haseł (np. keepass) do przechowywania poświadczeń do kont,
- nie używaj tego samego (ani podobnego) hasła w wielu serwisach,
- używaj logowania wieloskładnikowego w miarę możliwości,
- nie klikaj w linki w wiadomościach, których się nie spodziewasz,
- w razie wątpliwości co do tożsamości nadawcy wiadomości skontaktuj się z nim inną drogą (np. telefonicznie) i zapytaj, czy to rzeczywiście on do Ciebie napisał.

20. Czy powinienem/powinnam zastrzec swój PESEL?

Od 1 czerwca 2024 r. instytucje finansowe (np. banki) będą miały obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. Jeżeli więc w korespondencji e-mail z placówką CUK w Białymstoku (przy ul. Dubois) w domenie cuk.pl podawałeś/aś lub mogłeś podać np. dane ze swojego dowodu osobistego, czy innego dokumentu lub nawet sam nr PESEL, to atakujący mógł/może mieć do nich dostęp. Podobnie jeśli nie

korespondowałeś/aś mailowo z tą placówką, ale korzystałeś z jej usług, otrzymałeś ofertę ubezpieczenia, zawarłeś polisę lub złożyłeś w niej dokumenty (np. wypowiedzenie polisy), Twoje dane i dokumenty mogły być zawarte na tej zaatakowanej skrzynce, np. w korespondencji między pracownikami placówki a zakładami ubezpieczeń. Zalecamy więc profilaktyczne zastrzeżenie numeru PESEL i odblokowywanie go jedynie w razie potrzeby.

21. **W jaki sposób mogę zastrzec numer PESEL?**
    Numer PESEL możesz zastrzec w najbliższym urzędzie gminy, zob. https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie lub przez Internet, w tym w aplikacji mObywatel, zob. https://info.mobywatel.gov.pl/uslugi/zastrzez-pesel. Za pomocą tej aplikacji, w dowolnym momencie możesz też w razie konieczności wycofać zastrzeżenie jednym kliknięciem.
22. **Czy warto założyć konto w Biurze Informacji Kredytowej (BIK) i aktywować alert?**
    Tak, jeśli założyszi konto w Biurze Informacji Kredytowej oraz aktywujesz Alert BIK. będziesz informowana/-y o próbie uzyskania kredytu na Twoje dane oraz jeśli ktoś będzie sprawdzał Twoje dane w Rejestrze Dłużników BIG. Zachęcamy także do pobrania raportu BIK, aby upewnić się, iż podmiot trzeci nie zaciągnął z wykorzystaniem Twoich danych kredytu lub innego zobowiązania.
23. **Czy muszę oddać komputer do serwisu?**
    Za pośrednictwem wysłanych wiadomości nie było rozpowszechniane złośliwe oprogramowanie. Jeżeli jednak kiedykolwiek klikałeś w budzące wątpliwości odnośniki lub odwiedzałeś podejrzane strony, dobrym pomysłem jest oddanie komputera/laptopa/telefonu/tabletu w ręce specjalisty.
24. **Jakie dalsze kroki podejmie CUK?**
    Chcemy jak najdokładniej określić zakres danych, które uległy faktycznemu wyciekowi. Współpracujemy w tym zakresie z CERT oraz Microsoft. Będziemy na bieżąco informować o wszelkich nowych ustaleniach PUODO oraz zakłady ubezpieczeń. Po zakończeniu pełnej diagnostyki o sprawie poinformujemy organy ścigania. CUK podejmie analizę możliwości i ewentualne wdrożenie dodatkowych rozwiązań zabezpieczających.

Ostatnia aktualizacja: 2024-06-04, godz. 11:21