PKP POLSKIE LINIE KOLEJOWE S.A.

Informacja dla użytkowników usługi kluczowej świadczonej przez PKP Polskie Linie Kolejowe S.A. „Konstrukcji rozkładu jazdy" w sprawie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed nimi

Zabezpieczenie danych przed wyłudzeniem

Aby kradzież się powiodła, cyberprzestępca musi zdobyć dane, które umożliwią mu:

1. Dostęp do naszego konta. Tymi danymi są:
    - login,
    - hasło,
    - adres IP,
    - klucz odblokowujący.
2. Uzyskanie informacji niezbędnych w celu uzyskania dostępu do systemu. W tym celu haker spróbuje od nas pozyskać:
    - login,
    - hasło,
    - adres IP,
    - klucz odblokowujący;

Zdecydowana większość ofiar cyberprzestępców podaje im swoje dane w dobrej wierze lub w ogóle nie wie, że to robi. Przestępcy rozumieją, z której strony najlepiej podejść ofiarę i wykorzystują w tym celu techniki, które mają nieco przytłumić zdrowy rozsądek, a dać pole do popisu emocjom.

Phishing – jak go rozpoznać i nie dać się oszukać

Przykładowa wiadomość mail:

Dzień dobry, po awarii Twoje konto zostało zablokowane ze względu na nieautoryzowany dostęp: potwierdź swoją tożsamość, wprowadzając kod autoryzacyjny. Przejdź na stronę [link].

Tego rodzaju e-maile to typowy przykład narażenia klienta na *phishing, czyli próbę wyłudzenia danych.* Dostajemy na naszą skrzynkę e-mailową wiadomość: ktoś próbował włamać się na nasze konto! Na szczęście administrator w porę wykrył próbę oszustwa i teraz próbuje zweryfikować, czy my to naprawdę my. Musimy tylko kliknąć w przesłany link i podać swoje dane. Rzecz w tym, że nadawcą takiego maila nie jest administrator, lecz grupa przestępcza. Podane przez nas informacje posłużą im do błyskawicznego przejęcia naszego konta.

Schemat działania jest zazwyczaj podobny:

1. Otrzymujemy na naszą skrzynkę alarmujący e-mail, a w nim link do strony i żądanie zalogowania.
2. Po kliknięciu linka, przekieruje on nas do fałszywej strony internetowej, do złudzenia przypominającej oficjalną stronę. Na dodatek strona ta może

zawierać elementy graficzne (np. logo i kolorystykę), a nawet komunikaty bezpieczeństwa, które mają wzmagać u ofiary poczucie zaufania i „zaopiekowania się" nią.

3. Kiedy już zalogujemy się na fałszywej stronie, przestępcy otrzymają nasze dane niezbędne do zalogowania się na naszym prawdziwym koncie (login, hasło).

Aktualizacja oprogramowania

Socjotechniki w rodzaju phishingu to nie jedyne sposoby przestępców na wyłudzenie danych do naszego konta. *Równie łatwo mogą oni „wpuścić" na nasz komputer, tablet czy smartfona wirusa lub tzw. konia trojańskiego (trojana),* który informacje, jakie podajemy przy logowaniu się do konta, po prostu prześle hakerowi. Istnieją np. programy, które sczytują hasło z naszej klawiatury w momencie, gdy je wpisujemy. Dlatego tak ważne jest, abyśmy na bieżąco aktualizowali:

- program antywirusowy i zaporę sieciową (firewall) - jeżeli korzystasz z systemu Windows, a ich nie posiadasz, dla własnego dobra je zainstaluj;
- system operacyjny (np. Windows, itd.);
- przeglądarki internetowe.

Wirusy i trojany, które mogą być niebezpieczne dla naszych kont, najczęściej są pobierane przy okazji np. popularnych programów (plików muzycznych, bezpłatnych gier komputerowych, darmowych aplikacji usprawniających pracę komputera), a także darmowych czy niepewnych operacji w sieci.

1. *Aktualizuj przeglądarki oraz systemy operacyjne* (np. Windows, Mozilla itp.) do najnowszych wersji, które są „odporne" na nowe wirusy i trojany.
2. *Używaj aktualnego i legalnego oprogramowania antywirusowego i zapory sieciowej (firewall).*
3. *Nie ignoruj komunikatów programu antywirusowego.*
4. *Pamiętaj, aby zachować szczególną uwagę przy ściąganiu programów niewiadomego pochodzenia czy wchodzenia na podejrzane strony internetowe.*

O co nie zapyta Administrator

*Jedynym miejscem, w którym jesteśmy proszeni o podanie kluczowych informacji, jakimi są login, hasło jest wyłącznie strona do logowania się do naszego konta użytkownika***.** Od tej zasady nie ma żadnych wyjątków.
Pamiętajmy, że administrator **NIGDY** nie prosi o potwierdzenie naszych poufnych danych w żadnych e-mailach, smsach czy w trakcie rozmów telefonicznych. W szczególności nigdy nie zażąda od nas podania:

- loginu do konta,
- hasła – hasło jest znane tylko i wyłącznie nam, Administrator nie zna naszego kodu dostępu, nie może więc w żaden sposób go potwierdzać.

Administrator nie wysyła także:

- e-maili z linkami kierującymi do strony do zalogowania się na konto internetowe,

- smsów z odsyłaczami do logowania,
- aplikacji lub certyfikatów bezpieczeństwa na telefon komórkowy. Jeżeli otrzymałeś taką wiadomość, to znaczy, że ktoś – i to z pewnością nie administrator – próbuje zainfekować Twój telefon złośliwym oprogramowaniem, dzięki któremu uzyska dostęp do kodów, które są ostatnią zaporą przed kradzieżą.

Strona internetowa: autentyczna czy fałszywa?

Jeżeli przyjrzymy się dokładnie, dostrzeżemy znaczące różnice pomiędzy oficjalną stroną do logowania, a stroną przygotowaną przez hakerów.

Pamiętaj! Jeżeli chcesz zalogować się do swojego konta, **zawsze wpisuj pełny adres w przeglądarce lub przynajmniej sprawdzaj poprawność tego adresu**. Jeżeli adres logowania jest trudny do zapamiętania, możesz przejść na stronę główną PKP PLK S.A., a potem na podstronę logowania.

Procedury postępowania przy logowaniu do konta

1. Pamiętamy nazwę strony lub bezpośredniej strony logowania do systemu.
2. Wpisujemy pełny adres tej strony w przeglądarce, nigdy w Google czy innej wyszukiwarce. Istnieją bowiem konie trojańskie, które mogą podmienić domyślną wyszukiwarkę i przekierować nas na fałszywą stronę PKP PLK S.A..
3. Sprawdzamy poprawność adresu (m.in. pod kątem literówki), a następnie weryfikujemy czy przy adresie URL do strony logowania do systemu ISZTP pojawia się:
   - kłódka,
   - protokół https://.
4. Sprawdzamy certyfikat bezpieczeństwa.
5. Po wykonaniu operacji wylogowujemy się ze strony i wyłączamy przeglądarkę.

Symbol kłódki i protokół https:// w adresie strony

Oznaczają one, że strona, na którą się logujesz, jest szyfrowana i bezpieczna.

Podstawowa zasada przy logowaniu brzmi*: kłódka i https:// muszą pojawiać się razem.* Od tej reguły nie ma wyjątków, w szczególności w rodzaju: „przebudowa strony", „chwilowa aktualizacja", „czasowa awaria" itp. Standardowy protokół, na

którym działają strony internetowe, to http://. Pamiętajmy, że literka „s” przy https:// oznacza szyfrowanie, nie może go więc zabraknąć.

Na koniec należy wspomnieć, że cyberprzestępcy, chcąc maksymalnie utrudnić nam życie, *tworzą także fałszywe strony, na których przy adresie www pojawia się zapis: https:// - nie ma za to kłódki*. Dlatego kolejny punkt – weryfikacja certyfikatu – jest niezbędnym krokiem przy logowaniu się do konta internetowego.

Weryfikacja certyfikatu strony

Certyfikat strony www potwierdza, że naprawdę znaleźliśmy się na właściwej stronie. Przy każdym logowaniu do swojego konta należy poświęcić nie więcej niż pół minuty i przyjrzeć się certyfikatowi, który został wystawiony dla danej strony. Sprawdzamy przede wszystkim:

- *aktualność certyfikatu* (czy nie wygasł i jaka jest data jego obowiązywania),
- *odcisk palca SHA*.

Jak to zrobić? Poniżej prezentujemy, jak zweryfikować certyfikat w kilku prostych krokach, na przykładzie przeglądarki Firefox:

1. Wchodzimy na stronę logowania do naszego konta.
2. Klikamy na symbol kłódki.
3. Rozwijamy pasek „Zabezpieczone połączenie”.
4. Wyświetla się nam informacja o tym, że połączenie jest bezpieczne, a strona jest prowadzona przez konkretną instytucję. Ale my chcemy mieć 100% pewności, więc...
    - klikamy na przycisk „Więcej informacji” - wtedy dopiero wyświetli się okno prowadzące do certyfikatu,
    - klikamy na „Wyświetl certyfikat”. Dopiero teraz otrzymujemy informacje, jakich szukaliśmy.