BEZPIECZEŃSTWO SERWISU PTE PZU SA

W sieci Internet można spotkać się z atakami polegającymi na próbach wyłudzenia danych logowania. Atak polega na uruchomieniu fałszywej strony, która wyglądem imituje oryginalną, lecz w rzeczywistości służy wyłudzeniu danych dostępowych do systemu. Zagrożenie to nazywane jest phishingiem.

- Przed rozpoczęciem wprowadzania danych należy sprawdzić, czy adres na stronie wypełniania formularza online zaczynającej się od https://secure.pzuci.pl jest poprzedzony przedrostkiem https, zaś obok pojawia się symbol kłódki w kolorze zielonym. Symbol kłódki oznacza połączenie szyfrowane.
- Zaleca się kliknąć w symbol kłódki, po czym otworzy się okno z właściwościami certyfikatu, gdzie należy sprawdzić następujące parametry gwarantujące oryginalność strony secure.pzuci.pl:
  a) zakładka „Ogólne" („General"):
     - „Wystawiony dla:" („Issued to") – prawidłowa informacja to: „secure.pzuci.pl"
     - „Wystawiony przez:" („Issued by") – aktualny certyfikat wystawiony jest przez „Unizeto Technologies S.A."
     - Data ważności certyfikatu („Valid from... to...") – prawidłowa informacja to: „Ważny od 2017-06-20 do 2019-06-20":
  b) zakładka „Szczegóły" („Details") tzw. „Odcisk palca" („Thumbprint") – prawidłowa wartość tego pola to: 9e 57 9c b0 7d b3 e9 18 e0 5f 83 2f 84 53 c0 22 49 60 4d 58,
  c) zakładkę „Ścieżka certyfikacji" („Certification path") – prawidłowa ścieżka zawiera trzy elementy: „Certum Certification Authority/Certum Organization Validation CA SHA2/secure.pzuci.pl"

INFORMACJA O ZAGROŻENIACH WYNIKAJĄCYCH ZE ŚWIADCZENIA USŁUG DROGĄ ELEKTRONICZNĄ / ELEKTRONICZNYCH KANAŁÓW DOSTĘPU

Podstawowe zagrożenia związane z korzystaniem z usług w sieci Internet – w tym usług oferowanych przez Grupę PZU w ramach elektronicznych kanałów dostępu – to:

- podszywanie się w celu wyłudzenia informacji,
- działanie złośliwego oprogramowania,
- niechciana poczta – spam.

Zagrożenia dotyczą nie tylko komputerów, ale też innego sprzętu przenośnego, np. smartfonów, tabletów.

Phishing – to wyłudzanie danych umożliwiających dostęp do danej usługi (loginu, hasła, PIN), numerów kart kredytowych itp. Najczęściej są to fałszywe powiadomienia imitujące komunikaty z instytucji rozsyłane drogą elektroniczną, w których nakłania się użytkowników do zalogowania na spreparowane strony internetowe naśladujące oryginalne. Celem jest przechwycenie danych dostępowych.

Złośliwe oprogramowanie – takie programy, które są wykorzystywane w celach przestępczych lub mają na celu wyrządzenie szkody użytkownikowi. Należą do nich m.in. wirusy komputerowe i oprogramowanie szpiegujące.

- **Wirus komputerowy** to oprogramowanie złośliwe, które przenosi się poprzez zapis zainfekowanego pliku na nośniku danych np. dysku twardym, pendrive. Celem wirusa jest kradzież lub usunięcie danych, zakłócenie pracy urządzenia lub przejęcie kontroli nad komputerem. Najczęściej do zarażenia wirusem elektronicznym dochodzi po pobieraniu plików z niezaufanego źródła internetowego lub otwarciu załącznika w poczcie elektronicznej.

- **Program szpiegujący** – to taki, który w sposób ukryty monitoruje i przesyła dane o użytkowniku do przestępcy. Może gromadzić i przekazywać zarówno dane umieszczone na urządzeniu jaki i śledzić nasze działania np. ruchy myszką, tekst wpisywany z klawiatury.

Niechciana poczta lub spam to niezamawiane lub niepotrzebne wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców. Często przenoszą wirusy komputerowe, oprogramowanie szpiegujące, odnośniki do złośliwych lub fałszywych stron.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

1. Każdy użytkownik serwisu powinien dbać o bezpieczeństwo swoich urządzeń, które służą dostępowi do sieci Internet. Takie urządzenie powinno posiadać program antywirusowy z aktualną bazą definicji wirusów, aktualną i bezpieczną wersję przeglądarki internetowej oraz włączoną zaporę sieciową (ang. firewall). Użytkownik powinien ponadto cyklicznie sprawdzać, czy system operacyjny i programy zainstalowane na nim posiadają najnowsze aktualizacje, ponieważ w atakach wykorzystywane są błędy wykryte w zainstalowanym oprogramowaniu. Producenci programów starają się eliminować takie zagrożenia za pomocą aktualizacji.
2. Dane dostępowe do usług oferowanych w sieci Internet – np. loginy, hasła, PIN, certyfikaty elektroniczne itp. – powinny być zabezpieczone. Nie należy ich ujawniać lub przechowywać na urządzeniu w formie, która umożliwia nieautoryzowany dostęp i odczyt.
3. Zaleca się ostrożność podczas otwierania załączników lub klikania odnośników w wiadomościach, których się nie spodziewaliśmy np. od nieznanych nadawców. W przypadku jakichkolwiek wątpliwości warto się skontaktować z nadawcą np. telefonicznie.
4. Zaleca się uruchomienie w przeglądarce internetowej filtrów antyphishingowych czyli narzędzi, które sprawdzają, czy wyświetlona strona internetowa jest autentyczna i nie służy wyłudzaniu informacji, np. poprzez podszywanie się pod osobę lub instytucję.
5. Pliki powinny być pobierane tylko z zaufanych miejsc. Nie zalecamy instalowania oprogramowania z niezweryfikowanych źródeł. Dotyczy to również urządzeń przenośnych, np. smartfonów, tabletów.
6. Podczas używania domowej sieci bezprzewodowej (Wi-Fi) należy ustalić bezpieczne i trudne do złamania hasło dostępu do sieci. Rekomenduje się także korzystanie z najwyższych możliwych standardów szyfrowania sieci bezprzewodowych Wi-Fi, które są możliwe do uruchomienia na posiadanym sprzęcie np. WPA2.