Informacje dotyczące cyberbezpieczeństwa dla klientów PGE Obrót S.A.

1.Uważaj na podejrzane e-maile, załączniki i linki (Phising).

Phishing jest formą oszustwa bazującego na wzbudzeniu zaufania celem podstępnego wyłudzenia danych użytkownika i wykorzystania ich w sposób nieuczciwy.

Hakerzy dobrze wiedzą, co zrobić, aby zachęcić użytkownika do otwarcia niebezpiecznego załącznika z wiadomości e-mail albo kliknięcia w link. Podszywają się przy tym pod godne zaufania organizacje, banki, dostawców/kurierów, instytucje rządowe, finansowe przedsiębiorstwa energetyczne czy operatorów telekomunikacyjnych. Otworzenie podejrzanego załącznika lub linka może spowodować uruchomienie programu, którego celem jest zaszyfrowanie danych na komputerze oraz wymuszenie okupu bądź wyłudzenie danych.

2.Uważaj na fałszywe faktury i wezwania do zapłaty.

Nie tylko wykradanie danych czy szyfrowanie dysku może być celem oszustów internetowych. W ostatnim czasie zauważamy duży wzrost dystrybucji wiadomości z fałszywymi fakturami czy też wezwaniami do zapłaty. Oszuści redagując wiadomości e-mail robią to tak aby do złudzenia przypominały one te wysyłane przez GK PGE. Prosimy o dokładną weryfikacje wiadomości dotyczących płatności.

Faktury od GK PGE do klientów przychodzą wyłącznie z domeny „gkpge.pl”. Jeśli klient ma wątpliwości co do otrzymanej wiadomości - prośba o przesłanie jej na adres cert@gkpge.pl lub kontakt telefoniczny pod numerem (+48) 422 222 222.

3.Korzystaj tylko z oryginalnego oprogramowania i regularnie je aktualizuj.

Aktualizacje oprogramowania pozwalają chronić sprzęt przed najnowszymi zagrożeniami. Mogą być uruchamiane automatycznie, ale często wymagają też Twojej zgody. Planuj swoją pracę w taki sposób, aby nie odkładać aktualizacji na później.

4.Pobieraj aplikacje i programy wyłącznie z oficjalnych źródeł.

Wszystkie nasze aplikacje mobilne dostępne są wyłącznie w oficjalnych sklepach Google Play i AppStore. Nasze elektroniczne Biuro Obsługi Klienta udostępnione jest pod adresem www.ebok.gkpge.pl.

Właściciela strony, a co za tym idzie rzetelność informacji na niej znajdujących się możesz zawsze sprawdzić po certyfikacie (symbol kłódki w górnym lewym rogu). Wszystkie strony informacyjne oraz serwisy B2B w GK PGE są stronami szyfrowanymi i posiadają certyfikaty.

5.Stosuj różne i skomplikowane hasła, regularnie je zmieniaj.

Bezpieczne hasło musi być na tyle skomplikowane, aby nikt niepowołany go nie odgadł. Gdy już wymyślisz skomplikowane hasło, upewnij się, że będziesz w stanie je zapamiętać bez zapisywania. Zadbaj o to, aby nie używać tych samych haseł do różnych serwisów, portali. W ten sposób wyciek hasła z jednego serwisu nie będzie miał wpływu na bezpieczeństwo pozostałych.

6.Nie podawaj swoich poufnych danych:

Kontaktując się z naszą infolinią (+48) 422 222 222 w celu weryfikacji tożsamości konsultant nigdy nie poprosi Cię o:

- pełny numer PESEL
- hasła dostępu do usług eBOK/mBOK
- hasła do prywatnych kont pocztowych
- numer konta, z którego dokonywane są płatności