Zasady bezpiecznego korzystania z FortiPay

Zalecenia dla klientów

1. Swoje dane dostępu znasz tylko Ty i nikt inny.

Nigdy nikomu nie udostępniaj swoich danych do logowania do internetowego środka płatniczego FortiPay (dalej też "bankowość internetowa"), w szczególności identyfikatora użytkownika, loginu, hasła, kodu PIN, kodu autoryzacyjnego ani ich nie wysyłaj za pomocą poczty e-mail lub portali społecznościowych. Szczególnie podczas logowania, zadbaj o swoją prywatność i sprawdź, czy inne osoby nie mogą zarejestrować Twoich danych logowania. Nie zostawiaj komputera ani telefonu komórkowego bez nadzoru, używaj blokad klawiatury i kodów dostępu do swojego urządzenia. Unikaj używania produktów tzw. bankowości internetowej w miejscach publicznych (środki transportu publicznego, restauracje, ...) lub w obszarze monitorowanym (np. w zasięgu kamer bezpieczeństwa)

2. Uważaj z jakiego miejsca wchodzisz do bankowości internetowej.

Nie korzystaj z bankowości internetowej na komputerach, na których nie masz pewności, czy są na nich zainstalowane szkodliwe programy. Unikaj korzystania z publicznych komputerów w kafejkach internetowych, na lotniskach i w centrach informacyjnych. O ile to możliwe korzystataj z bankowości internetowej tylko ze swojego komputera lub telefonu komórkowego. Zawsze sprawdzaj nagłówek przeglądarki, aby upewnić się, że uzyskujesz dostęp do bezpiecznych połączeń internetowych. Bezpieczna strona internetowa zaczyna się od https: // (ważne jest „s” na końcu), lub sama przeglądarka zwrócici ci uwagę symbolem zamkniętej kłódki przed nazwą strony.

3. Strzeż się nieznanych linków i stron internetowych.

Odwiedzaj tylko znane i zaufane witryny w Internecie. Dzisiejsi napastnicy są bardzo zaradni, potrafią wiernie odtworzyć na przykład strony do logowania w bankowości internetowej i sprytnie cię do niej poprowadzić. Uważaj więc na jakiekolwiek nieznane linki w internecie lub w poczcie e-mail, które doprowadzą cię do miejsca przypominającego formularz zgłoszeniowy do bankowości internetowej, poczty e-mail lub portali społecznościowych. O ile masz jakąkolwiek wątpliwość co do stronylogowania do bankowości internetowej, nie rejestruj się. W nagłówku przeglądarki zawsze się upewnij i sprawdź, czy rzeczywiście jesteś na właściwej stronie internetowej a nie na fałszywej. Szczególnie niebezpieczne są strony z treścią erotyczną lub strony do pobierania oprogramowania, filmów, czy muzyki, które często zawierają dużo niebezpiecznego oprogramowania i wirusów.

4. Podejrzany e-mail? Nie otwieraj, raczej usuń.

Spółka nigdy nie wysyła e-maili skłaniających do przesłania danych identyfikacyjnych, loginów, haseł, kodów autoryzacji PIN, danych kart płatniczych, etc. Na takie wyzwania nigdy nie reaguj. W skrzynce pocztowej otwieraj tylko zaufane wiadomości e-mail od znanych i widocznych nadawców. Jeśli wiadomość e-mail wygląda podejrzanie, najlepiej ją usunąć. Jeśli już ją otworzyłeś, nie otwieraj załączników ani linków, które zawiera. A jeśli uda ci się niechcący kliknąć na link lub otworzyć załącznik, szybko go zamknij i nie pozwól na zainstalowanie czegokolwiek. Następnie zalecamy sprawdzenie komputera lub urządzenia mobilnego za pomocą oprogramowania antywirusowego.

5. Chroń się przed spamem.

Najlepszym narzędziem do usuwania najbardziej niepożądanych i niebezpiecznych wiadomości jest skonfigurowanie i aktywne korzystanie z ochrony przed spamem poczty e-mail. Większość programów pocztowych takich jak Outlook i inne, posiadają ochronę antyspamową. Jego ustawienie jest często intuicyjne i proste. Rozważ skorzystanie z innych programów zabezpieczających, takich jak oprogramowanie antyspyware i antyadware, w celu ochrony przed niechcianymi reklamami i złośliwymi programami.

6. Używaj i aktualizuj zarówno program antywirusowy, jak i firewall na komputerze i w telefonie.

Regularnie skanuj swoje urządzenia za pomocą programu antywirusowego. Nie wyłączaj oprogramowania antywirusowego, nie zapomnij o jego regularnej aktualizacji (automatyczna aktualizacja może być konfigurowana przez Internet) i korzystaj z najnowszej wersji, która jest chroniona przed szkodliwym oprogramowaniem i złośliwym oprogramowaniem. Oszuści nie śpią, więc im starszy jest program antywirusowy, tym mniej skutecznie chroni przeciw nowym zagrożeniom. Zalecamy również używanie zapory firewall na twoim komputerze. Wyposaż w program antywirusowy również swój inteligentny telefon komórkowy. Stwierdzenie, że wirusy nie atakują telefonów, jest niebezpiecznym mitem, który może ci się wymścić. Jeśli podejrzewasz, że wirus zaatakował twój komputer lub telefon komórkowy, nie używaj go do dostępu do bankowości internetowej lub innych usług z wykorzystaniem danych osobowych (e-mail, sieci społecznościowe, sklepy internetowe, itp.) i skontaktuj się ze specjalistą IT.

7. Aktualizuj swoje urządzenia, komputer i telefon komórkowy.

Regularnie aktualizuj także swoje programy i system operacyjny. Szczególnie ważne jest zaktualizowanie przeglądarki internetowej na komputerze i telefonie oraz wszystkich tak zwanych wtyczek (takich jak Flash Player). Zaktualizuj także wszystkie programy bezpieczeństwa. Obejrzyj także problem łatek systemu operacyjnego i nie zwlekaj z ich instalacją. W przypadku smartfonów i tabletów zalecamy korzystanie z najnowszej wersji systemu operacyjnego (oprogramowania układowego), którą producent oficjalnie oferuje dla urządzenia. Wszystkie stare wersje twoich programów stanowią potencjalne zagrożenie dla bezpiecznego surfowania i dla twoich finansów. Nigdy nie instaluj na komputerze lub telefonie programów o nieznanym pochodzeniu. W telefonach komórkowych instaluj aplikacje wyłącznie z oficjalnych sklepów z aplikacjami - Google Play (Android) App Store (iOS), Windows Marketplace (Windows Phone).

8. Śledź swoje saldo i transakcje, rozbieżności zgłaszaj u nas.

Rozeznanie o tym, ile pieniędzy pozostało na koncie i jakich transakcji dokonałeś, jest najlepszym narzędziem wczesnego ostrzegania, że coś jest nie tak. Jeśli zauważysz jakąkolwiek operację, której nie przeprowadzałeś/-aś lub masz wątpliwości co do prawidłowości salda konta natychmiast skontaktuj się z nami telefonicznie tel. +420 558 335 000 lub poprzez e-mail i devizy@devizy.cz. Nie zwlekaj ze zgłoszeniem jakiejkolwiek nieprawidłowości! Tylko szybka reakcja może zapobiec dalszym stratom lub znaleźć szybkie rozwiązanie.

9. Regularnie monitoruj aktualizacje zabezpieczeń internetowych.

Im więcej masz informacji, tym bezpieczniej potrafisz poruszać się w Internecie. Zatem śledź na bieżąco najnowsze informacje na temat bezpieczeństwa w Internecie i stosuj się do wszystkich zalecanych zasad.