ZASADY BEZPIECZNEGO KORZYSTANIA Z SERWSIU TRANSAKCYJNO-INFORMACYJNEGO

(„STI") WG. PROSERVICE AGENT TRANSFEROWY SP. Z O.O.

1. **Upewnij się, że logujesz się na prawidłową stronę STI** - adres strony powinien zaczynać się od HTTPS i posiadać symbol zielonej kłódki, co oznacza, że połączenie jest szyfrowane. Na stronę STI nie zaleca się wchodzenia przez linki przekazywane w wiadomościach email. Należy unikać wchodzenia na stronę STI za pomocą adresów zapisanych „w ulubionych" lub przez strony logowania proponowane przez wyszukiwarki internetowe.

2. **Jeśli nastąpi problem z certyfikatem strony – nie ignoruj go –** należy czytać uważnie komunikaty o zagrożeniach, które pojawią się w przeglądarce. Nie ignoruj informacji o nieważnym lub błędnym certyfikacie, koniecznie zachowaj ostrożność. Kliknięcie dwukrotnie na symbol kłódki umożliwia wyświetlenie informacji na temat certyfikatu, czyli dacie jego ważności i dla kogo został wystawiony.

3. **Podstawą bezpieczeństwa jest hasło –** Silne hasło to podstawa, imię męża, partnera czy dzieci, data urodzenia nie są dobrym zabezpieczeniem. Hasło powinno być odpowiednio długie, mieć co najmniej 8 znaków, duże i małe litery, znaki specjalne oraz przynajmniej jedną cyfrę.

4. **Chroń swoje dane uwierzytelniające do STI –** Nie zapisuj danych wrażliwych w sposób łatwo dostępny dla innych osób np. w notesie, na karteczkach czy telefonie.

5. **Bezpieczeństwo urządzeń –** urządzenie z którego korzystasz powinno mieć zainstalowany program antywirusowy z aktualną bazą wirusów, dzięki temu będzie bardziej zabezpieczone przed złośliwym oprogramowaniem. Systematycznie aktualizuj przeglądarki internetowe to zapewnia większy poziom bezpieczeństwa. Jeśli masz możliwość zabezpiecz urządzenia dodatkowym hasłem, chroni to twoje urządzenia przed dostępem osób niepowołanych np. w sytuacji gdy urządzenie zgubimy lub gdy zostanie nam ukradzione. Należy zachować ostrożność i nie otwierać wiadomości i plików, które wydają nam się podejrzane, a ich pochodzenie nie jest potwierdzone.

6. **Co to jest PHISHING?-** definicja: *metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.*

Czyli jak to działa?: Najczęściej wykorzystywaną formą ataku przy pomocy metody phishingu jest przygotowanie przez cyberprzestępcę specjalnej strony internetowej łudząco podobnej do docelowej, gdzie nieświadoma ofiara podaje swoje dane dostępowe. Wprowadzone na niej login i hasło, zamiast otworzyć dostęp do określonej strony, trafiają do cyberprzestępcy, który gromadzi je i wykorzystuje przeciwko nam. Pewnie wielu z was zastanawia się, w jaki sposób taki przestępca zmusi nas do wejścia na tak spreparowaną stronę – istnieje na to bardzo prosta metoda. Najczęściej przesyłana jest ofierze na adres poczty elektronicznej fałszywa wiadomość mailowa, gdzie przestępca, podszywając się pod jakąś instytucję lub osobę, zachęca do zapoznania się z nową ofertą lub prosi o wprowadzenie danych uwierzytelniających poprzez podany link. Wiele osób niestety daje się na to nabrać.

Jak się bronić?: Społeczeństwo ma coraz większą świadomość tego, co dzieje się w cyberprzestrzeni. Zwiększa to zapotrzebowanie na rzetelną edukację w tej dziedzinie. Oto kilka podstawowych zasad ograniczających ryzyko „złowienia":

- **Ignoruj wszystkie podejrzane maile od nieznanych nadawców!** Przy pomocy rozesłanych linków stron internetowych, bardzo podobnych do docelowych, przestępcy wyłudzają nasze dane uwierzytelniające. Niech nie zmyli Cię podobna kolorystyka, układ strony czy też zamieszczone tam logo firmy.
- **Regularnie uaktualniaj system** i oprogramowanie, dzięki czemu będziesz miał pewność, że załatane są w nim znane luki bezpieczeństwa.
- **Korzystaj z oprogramowania antywirusowego**, które powinno zaalarmować Cię o fałszywej lub podejrzanej witrynie internetowej.
- **Nie podawaj danych uwierzytelniających** na stronach nieposiadających protokołu https. Przy adresie strony powinna znajdować się zielona kłódka, która informuje nas o tym, że połączenie jest szyfrowane, a dostawca zaufany.
- **Ignoruj prośby mailowe** o przesłanie danych uwierzytelniających lub innych danych osobowych.