Szanowni Państwo,

Poniżej kilka informacji i zasad o cyberbezpieczeństwie.

Jako Spółka stosujemy światowe standardy w zakresie bezpieczeństwa i poufności danych. Stale pracujemy nad rozwiązaniami mającymi chronić Twoje dane i staramy się, aby były one zgodne z najnowszymi standardami bezpieczeństwa. Niemniej to od Ciebie zależy, czy będziesz z nich korzystał we właściwy sposób.

Najczęściej występujące zagrożenia w sieci oraz porady cyberbezpieczeństwa:

PHISHING – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych osobowych, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do określonych działań.

Ochrona przed PISHINGIEM:

Zdecydowana większość wiadomości phishingowych jest dostarczana za pośrednictwem poczty elektronicznej lub portali społecznościowych

- Zazwyczaj serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie. Taka prośba powinna wzbudzić czujność, zawsze warto w takim wypadku potwierdzić autentyczność listu poprzez kontakt z administratorami strony. Banki i instytucje finansowe nigdy nie wysyłają listów z prośbą o ujawnienie (wpisanie w formularzu) jakichkolwiek danych (loginu, hasła, numeru karty). Próby podszycia się pod nie powinny być zgłaszane do osób odpowiedzialnych za bezpieczeństwo.
- Nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila. Stosunkowo prosto jest zmodyfikować ich treść tak, by pozornie wskazujące na autentyczną witrynę kierowały do nieautoryzowanej, podszywającej się strony.
- Należy regularnie uaktualniać system i oprogramowanie, w szczególności klienta poczty e-mail i przeglądarkę WWW.
- Nie należy przesyłać mailem żadnych danych osobistych typu hasła, numery kart kredytowych itp. Prośby o podanie hasła i loginu w mailu należy zgłosić osobom odpowiedzialnym za bezpieczeństwo.
- Banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to pracownikom banku i nie podawać na niej żadnych danych.
- Nie zaleca się używania starszych przeglądarek internetowych (np. Internet Explorer 6), które bywają często podatne na różne błędy. Alternatywnie można korzystać z innych programów, jak Mozilla Firefox czy Opera lub Internet Explorer 9 i 10 (których najnowsze wersje wyposażone są w filtry antyphishingowe) albo z oprogramowania firm trzecich chroniącego przed phishingiem.

MALWARE - Złośliwe oprogramowanie, infekujące urządzenia. Działa na szkodę użytkownika, powodując także straty finansowe. Najczęstszym źródłem infekcji są:

- załączniki lub odnośniki tzw. linki w wiadomości e-mail,
- przejęta przez przestępców lub podstawiona, fałszywa strona,
- podstawione reklamy na zwykłych stronach.

W jaki sposób można rozpoznać, że „złośliwe" oprogramowanie zainfekowało nasze urządzenie? Poprzez spowolnienie działania urządzenia,

- pojawienie się większej ilości spamu na poczcie,
- strony startowe, których użytkownik nie ustawiał w przeglądarce.

Przykładem złośliwego oprogramowania (malware) jest **Ransomware** – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okupu za możliwość dalszego korzystania z komputera.

Ochrona przed **MALWARE**:

- Niewyłączanie Zapory Windows,
- Cykliczne skanowanie pod kątem niechcianego oprogramowania,
- Nieklikanie w podejrzane linki i reklamy,
- Niewchodzenie na strony jakkolwiek budzące w nas podejrzenia,
- Rozważne pobieranie i otwieranie wszelkich załączników,

Podsumowując, użytkownicy muszą być coraz bardziej uważni, gdyż nadal najpopularniejszym sposobem infekcji pozostaje wysłanie phishingowej wiadomości e-mail lub rozsyłanie złośliwych sms-ów z linkami. Dlatego kluczowe jest weryfikowanie pochodzenia wiadomości oraz otwieranie tylko takich załączników, które są znanego pochodzenia i zostały sprawdzone pod kątem bezpieczeństwa.