EIRO
EUROPEJSKI INSTYTUT ROZWOJU OBYWATELSKIEGO

BEZPIECZEŃSTWO W SIECI

PODSTAWOWE ZAGROŻENIA I SPOSOBY ICH UNIKANIA

BROSZURA EDUKACYJNO-INFORMACYJNA E-USŁUGI PUBLICZNE DLA SENIORA

10 ZASAD BEZPIECZNEGO KORZYSTANIA Z KONTA INTERNETOWEGO

- Starannie przechowuj login i hasło do konta oraz karty kodów jednorazowych lub telefon, na który przysyłane są ww. kody!
- Nie korzystaj z przypadkowych komputerów, tabletów, smartfonów!
- Nie korzystaj z publicznych sieci Wi-Fi!
- Zainstaluj legalne oprogramowanie antywirusowe!
- Wchodząc na stronę bankową upewnij się, czy nie nastąpiło przekierowanie na inną stronę, podobną do strony Twojego banku!
- Nie otwieraj wiadomości i dołączonych do nich załączników, jeśli pochodzą z nieznanego źródła!
- Nie zapamiętuj w przeglądarce internetowej loginów i haseł!
- Kończąc pracę z kontem internetowym zawsze użyj opcji: **WYLOGUJ SIĘ**!
- Jeśli masz jakieś wątpliwości/obawy - lepiej nie loguj się do konta!
- Wszystkie wyżej wymienione zasady stosuj łącznie!

Strona internetowa do zgłaszania incydentów związanych z próbami oszustw w Internecie:
www.incydent.cert.pl

ISTOTA

Internet ułatwia osobom starszym załatwianie wielu bieżących spraw życia codziennego. Dzięki nowoczesnym technologiom senior może np. sprawdzić swoją e-receptę, wysłać pismo do urzędu, zapłacić rachunki czy też zrobić zakupy. Internet daje również niemal nieograniczone możliwości kontaktu z ludźmi z całego świata oraz umożliwia skorzystanie z różnego rodzaju rozrywki on-line. Komputer jest zatem urządzeniem, w którego pamięci przechowujemy różnego rodzaju dane, które powinny być chronione przed osobami postronnymi [dane osobowe, hasła, zdjęcia itp.]. Dlatego niezwykle ważne jest, by wiedzieć, z jakimi zagrożeniami możemy się spotkać w wirtualnym świecie i jak się przed nimi chronić.

KTO MUSI ZACHOWAĆ SZCZEGÓLNĄ OSTROŻNOŚĆ W INTERNECIE?

Każdy, kto korzysta z zasobów Internetu, musi przestrzegać podstawowych zasad cyberbezpieczeństwa. Szczególną jednak ostrożność powinny zachować osoby korzystające z bankowości elektronicznej, usług e-administracji czy też dokonujące zakupów on-line.

Nawet jeśli użytkownikowi wydaje się, że w pamięci posiadanego urządzenia elektronicznego [komputera, tableta, smartfona] nie ma żadnych cennych informacji, powinien on zadbać o jego właściwe zabezpieczenie – to, co uważa bowiem za nieistotne, może okazać się bardzo ważne dla oszusta i tym samym ułatwić mu np. dokonanie kradzieży.

AKTYWNI+
Ministerstwo Rodziny i Polityki Społecznej
Projekt dofinansowany ze środków Rządowego Programu Wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021–2025. Edycja 2022.

CO TO SĄ WIRUSY?

Wirusy to złośliwe oprogramowanie mające najczęściej za zadanie uszkodzenie, dezaktywację naszego urządzenia lub kradzież znajdujących się na nim danych.

JAK CHRONIĆ SIĘ PRZED WIRUSAMI?

Aby zminimalizować ryzyko zainfekowania komputera/tableta/smartfona wirusem komputerowym należy w szczególności:

- **zainstalować program antywirusowy** - na rynku dostępnych jest wiele tego typu programów [bezpłatnych i płatnych];
- **regularnie aktualizować oprogramowanie** - nieaktualizowane oprogramowanie [w tym system operacyjny] stwarza idealne warunki do działania dla hakerów i tworzonych przez nich wirusów komputerowych. Firmy dostarczające oprogramowanie w trybie ciągłym udoskonalają swoje produkty dostarczając użytkownikom aktualizacje, dzięki którym usuwane są wykryte przez producenta danego programu tzw. luki bezpieczeństwa;
- **unikać stron internetowych podwyższonego ryzyka** - są to np. strony zawierające treści pornograficzne, portale z nielegalnym oprogramowaniem;
- **zwracać szczególną uwagę na treści pobierane z Internetu** - m.in. nigdy nie powinno się pobierać załączników z nieznanych źródeł np. z podejrzanych wiadomości e-mail.

JAK ROZPOZNAĆ, ŻE SPRZĘT JEST ZAINFEKOWANY?

Oznaką, że nasz sprzęt jest zawirusowany, może być:

- powolne działanie;
- nadmierne nagrzewanie się;
- zmiana wyglądu strony startowej po włączeniu przeglądarki internetowej;
- zwiększona ilość wyskakujących reklam, często z niecenzuralnymi treściami;
- utrudnione korzystanie z zainstalowanych programów [np. „skaczący" kursor w programie tekstowym].

Każde niestandardowe działanie naszego urządzenia powinno wzbudzić naszą czujność w kontekście zagrożeń wirusami komputerowymi - jeśli sami nie mamy wystarczających umiejętności, skorzystajmy z pomocy innych.

PHISHING

Jest to jedna z najskuteczniejszych metod pozyskiwania danych autoryzacyjnych - w ten sposób oszust uzyskuje dostęp np.: do naszego konta e-mail, banku, portalów społecznościowych, kont w e-sklepach. **Phishing polega na podszywaniu się pod różne instytucje** [np. banki, urzędy, dostawców prądu/gazu, czy też operatorów pocztowych]. Istotą tego rodzaju oszustwa są najczęściej masowo wysyłane wiadomości e-mail/SMS, które mają na celu nakłonienie do kliknięcia w link do fałszywej strony internetowej lub pobranie z załącznika i zainstalowanie złośliwego oprogramowania. We wszystkich przypadkach są to treści mające ukryty w sobie atak socjotechniczny. Przykładowo - wiadomość [**fałszywa, ale wyglądająca na prawdziwą!**] o wszczęciu postępowania sądowego ma na celu zmylić osobę atakowaną, wywołać emocjonalną reakcję i sprawić, aby osoba ta była bardziej podatna na manipulację i nieświadome przekazanie np. swoich danych dostępowych do konta internetowego czy danych z karty płatniczej.

Naszą szczególną uwagę powinna wzbudzić m.in.:

- wiadomość SMS/e-mail o dziwnej lub nieoczekiwanej treści, w tym każda wiadomość, z której wynika, iż dokonując zapłaty np. za usługi pocztowe, prąd czy gaz nie zapłaciliśmy całej wymaganej sumy i w związku z tym jest konieczność dopłaty jakiejś drobnej kwoty;
- prośba o pieniądze od znajomego np. za pośrednictwem portalu społecznościowego [możliwe, że o pieniądze prosi nas złodziej, który uzyskał dostęp do konta społecznościowego np. naszej siostry];
- wiadomość z banku lub od znajomego zawierająca link bez żadnego komentarza albo z poleceniem szybkiego kliknięcia w ten link i uruchomienia strony;
- wiadomość z błędami językowymi, bez polskich znaków itp.;
- telefon/e-mail z naszego banku i prośba o podanie danych niezbędnych do zalogowania się do bankowości internetowej.