Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tymi zagrożeniom.

- Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości e – mail, SMS, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu.
- Nie ujawniaj danych osobowych w tym danych autoryzacyjnych, dopóki nie ustalisz czy rozmawiasz z osoba uprawnioną do przetwarzania Twoich danych.
- Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
- Nie otwieraj wiadomości e – mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
- Każdy e – mail można sfałszować, sprawdź w nagłówku wiadomości pole „Received from" (ang. otrzymane od). W tym polu znajdziesz rzeczywisty adres serwera Nadawcy.
- Porównaj adres konta e – mail Nadawcy adresem w polu „From" oraz „Reply to" – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
- Szyfruj dane poufne wysyłane pocztą elektroniczną.

Sprawdź adres URL, z którego domyślnie dany podmiot/instytucja wysyła do Ciebie SMSy; cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę), otrzymując SMS, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako Nadawcę wiadomości SMS.

- Jeśli na podejrzanej stronie podałeś/łaś swoje dane do logowania lub jeżeli włamano się na Twoje konto e – mail – jak najszybciej zmień hasło.
- Chroń swój komputer, urządzenie mobilne, programem antywirusowym, zabezpieczającym przed zagrożeniami takie jak wirusy, robaki, trojany, niebezpieczne aplikacje takie jak ransomware, adware, keylogger, spyware, dialer, phishing, narzędzia hakerskie, backdorry, rootkity, bootkity i exploity.

- Aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe. Brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu/aplikacji mają otwartą furtkę do korzystania z luk w oprogramowaniu.
- Logowanie do e – usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
- Korzystaj z różnych haseł do różnych usług elektronicznych.
- Tam gdzie to możliwe (konta społecznościowe, konto e – mail, usługi e – administracji, usługi finansowe) stosuj dwuetapowe uwierzytelnienie za pomocą SMS, PIN, aplikacji generującej jednorazowe kody autoryzacyjne, tokeny, klucze fizyczne.
- Zmieniaj regularnie hasła.
- Nie udostępniaj nikomu swoich haseł.
- Pracuj na najniższych możliwych uprawnieniach użytkownika.
- Wykonuj kopie bezpieczeństwa.
- Skanuj podłączane urządzenia zewnętrzne.
- Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
- Kontroluj uprawnienia instalowanych aplikacji.
- Unikaj z korzystania otwartych sieci Wi-Fi.
- Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarką a serwerem.
- Zadbaj o bezpieczeństwo routera (ustal silne hasło do sieci Wi-Fi, zmień nazwę sieci Wi-Fi, zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-Fi, np. WPA2 i wyższe, aktualizuj oprogramowanie routera, wyłącz funkcję WPS, aktywuj funkcję „Gościnna Sieć Wi-Fi Guest Network”.
- Szyfruj dyski twarde komputera, przenośne.

Informacje i porady o Cyberbezpieczeństwie uzyskasz na stronach:

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

https://www.cert.pl/publikacje/

https://akademia.nask.pl/publikacje/

https://dyzurnet.pl/

Zgłaszanie incydentów bezpieczeństwa: *https://incydent.cert.pl/*