Pamiętaj o bezpiecznej poczcie mailowej

*** Złośliwe oprogramowanie - wirusy, robaki i trojany trafiają do naszych komputerów właśnie przez pocztę e-mail:|**
- uważaj, jakie wiadomości otwierasz ,aby nie doprowadzić do zainfekowania sprzętu, uszkodzenia lub utraty ważnych danych.
- zainstaluj program antywirusowy
***Spam- tego typu wiadomości nie stanowią bezpośredniego zagrożenia dla komputera, ale mogą utrudniać korzystanie z poczty:**
-korzystaj ze skrzynki pocztowej, która sama filtruje niechciane wiadomości.
- korzystaj z funkcji „Zgłoś spam", aby nie otrzymywać maili od niechcianego nadawcy.
***Phishing - to forma internetowego oszustwa, w której ktoś podszywa się pod osobę lub instytucję w celu wyłudzenia pewnych danych – uważaj, by Twoje hasła lub numery kart kredytowych nie dostały się do osób nieupoważnionych.**
***Nieznane pliki w załączniku- przez te załączniki możesz pobrać zarażony plik i zainfekować komputer.**
-zanim otworzysz taki plik, przeskanuj go programem antywirusowym
- do wszystkich załączników pochodzących od nieznanego nadawcy podchodź ostrożnie.

Pamiętaj o bezpiecznej chmurze

**** Dyski w chmurze, takie jak np.: OneDrive, Google Drive czy DropBox to przestrzeń, w której możemy magazynować dane, robić kopie zapasowe plików, a także przechowywać własne dokumenty. Dostęp do nich jest możliwy z każdego urządzenia podłączonego do sieci, dlatego możemy z nich korzystać praktycznie z każdego miejsca na świecie.***
****Zwróć uwagę, czy dostawca danej chmury świadczy usługi zgodnie z normą ISO 27018.** Jest to **kodeks postępowania dotyczący ochrony danych osobowych w chmurach funkcjonujących jako podmioty przetwarzające dane osobowe. Określa on, że nasze dane przechowywane w chmurze są poufne, a usługodawca nie może ich wykorzystywać. *zwróć uwagę, czy usługodawca oferuje szyfrowane połączenie. Dzięki Certyfikatowi SSL możesz mieć pewność, że przesyłane przez Ciebie informacje będą szyfrowane, a tym samym nie będą mogły zostać odczytane przez osoby niepowołane.***
**** pamiętaj, aby ustawić silne hasło, które uniemożliwi innym dostanie się do naszej chmury.***
****nie zapisuj haseł, wylogowuj się, nie współdziel Swoich kont.***

Pamiętaj o bezpiecznej sieci wifi

****konfiguracja routera podczas pierwszego uruchomienia- najpierw ustaw nowe hasło - skomplikowane i silne. To pierwszy krok zabezpieczający!***
****aby zmienić hasło do wi-fi zaloguj się do panelu administracyjnego routera. W polu z trybem zabezpieczeń oraz uwierzytelnianiem wybierz opcję WPA-Personal/WPA2. Wybierz szyfrowanie AES. Wpisz swoje nowe hasło i zapisz zmiany.***
****następny etap to Filtr MAC zabezpieczający Twoją sieć wi-fi – dopuszcza on lub blokuje konkretne urządzenia, ale też utrudnia podłączenie nowych urządzeń do sieci, gdy ktoś zechce c skorzystać z Twojej sieci wi-fi.– w zabezpieczeniu pomoże Ci także zmiana SSID, czyli nazwy sieci na własną, a także wyłączenie WPS, czyli mechanizmu, który ułatwia podłączanie nowych urządzeń.***