

Informacje o bezpieczeństwie podczas użytkowania oprogramowania.

1. Ogólne zasady bezpieczeństwa

- **Pochodzenie oprogramowania:** Pobieraj i instaluj oprogramowanie tylko z zaufanych źródeł (np. oficjalna strona producenta, autoryzowane sklepy internetowe). Unikaj pobierania oprogramowania z nieznanych lub podejrzanych źródeł.
- **Legalność oprogramowania:** Używaj tylko legalnego oprogramowania. Unikaj używania pirackiego oprogramowania, ponieważ może ono zawierać wirusy lub inne szkodliwe oprogramowanie.
- **Sprawdzenie pliku:** Przed uruchomieniem pliku instalacyjnego oprogramowania, przeskanuj go programem antywirusowym.
- **Klucz licencyjny:** Chronь swój klucz licencyjny oprogramowania. Nie udostępniaj go nikomu.
- **Wymagania systemowe:** Upewnij się, że Twój komputer spełnia minimalne wymagania systemowe oprogramowania.
- **Aktualizacje:** Regularnie aktualizuj oprogramowanie, aby zapewnić jego bezpieczeństwo i stabilność.

2. Bezpieczeństwo instalacji

- **Płyta CD/DVD:**
 - Sprawdź płytę CD/DVD pod kątem uszkodzeń.
 - Uruchom instalator z płyty tylko wtedy, gdy jesteś pewien, że płyta pochodzi z zaufanego źródła.
- **Kod aktywacyjny ESD (Electronic Software Distribution):**
 - Pobierz oprogramowanie tylko z oficjalnej strony internetowej producenta lub autoryzowanego sklepu internetowego.
 - Sprawdź, czy strona internetowa jest zabezpieczona protokołem HTTPS (sprawdź, czy w adresie URL znajduje się "https://").
 - Wprowadź kod aktywacyjny tylko w oknie aktywacji oprogramowania lub na oficjalnej stronie internetowej producenta.
- **Klucz licencyjny:**
 - Zapisz klucz licencyjny w bezpiecznym miejscu.
 - Nie udostępniaj klucza licencyjnego na forach internetowych lub w mediach społecznościowych.

3. Ochrona komputera

- **Program antywirusowy:** Zainstaluj i regularnie aktualizuj program antywirusowy.
- **Zapora ogniowa (firewall):** Włącz zaporę ogniową, aby chronić swój komputer przed nieautoryzowanym dostępem.
- **Kopie zapasowe:** Regularnie twórz kopie zapasowe ważnych danych.
- **Uważaj na phishing:** Uważaj na próby wyłudzenia danych osobowych (phishing). Nie klikaj w podejrzaną linki w wiadomościach e-mail lub SMS-ach.

4. Aktualizacje oprogramowania

- **Automatyczne aktualizacje:** Włącz automatyczne aktualizacje oprogramowania, aby zapewnić jego bezpieczeństwo i stabilność.
- **Sprawdzaj źródło aktualizacji:** Upewnij się, że aktualizacje pochodzą z oficjalnego źródła.

5. Znaczenie stosowania się do ostrzeżeń

- Zastosowanie się do powyższych ostrzeżeń minimalizuje ryzyko zainfekowania komputera wirusami, utraty danych, kradzieży danych osobowych i innych problemów związanych z bezpieczeństwem oprogramowania. Dbaj o bezpieczeństwo swojego komputera, stosując się do powyższych zaleceń.
- Pamiętaj, że powyższa instrukcja jest ogólna. Zawsze stosuj się do zaleceń producenta oprogramowania.