Pobierasz aplikację 📲 albo otwierasz załącznik z e-maila: **„Ważne dokumenty – pilne!”**. Wszystko wygląda w porządku, ale w tle dzieje się coś, czego nie widzisz. Twoje urządzenie zaczyna działać wolniej, a po jakimś czasie zauważasz, że pieniądze z konta znikają z Twojego konta 💸. Winowajcą jest **malware**. 😨

🎯 **Co to jest malware?**
To złośliwe oprogramowanie instalowane na Twoim urządzeniu bez Twojej wiedzy. Może przechwytywać dane logowania, śledzić Twoje działania online, a nawet zablokować Ci dostęp do Twoich plików (tzw. ransomware). Malware często dostaje się na urządzenie przez:

👉 aplikacje pobrane spoza oficjalnych sklepów,
👉 fałszywe załączniki w e-mailach,
👉 kliknięcie w podejrzane linki.

🛡 Jak się chronić?
✅ **Pobieraj aplikacje tylko z oficjalnych źródeł** – upewnij się, że są to sklepy, takie jak Google Play lub App Store. 📥
✅ **Nie otwieraj załączników od nieznanych nadawców** – to popularny sposób na rozprzestrzenianie malware. 📧
✅ **Używaj programu antywirusowego** – regularnie skanuj swoje urządzenia, aby wykryć zagrożenia. 🔒
✅ **Aktualizuj system i aplikacje** – zabezpieczenia są stale ulepszane, aby chronić Cię przed nowymi atakami.

📌 Co zrobić, jeśli podejrzewasz malware?
👉 Odłącz urządzenie od Internetu, aby zatrzymać przesyłanie danych.
👉 Przeskanuj urządzenie programem antywirusowym i usuń złośliwe oprogramowanie.
👉 Zmień hasła do swoich kont – najlepiej z innego, bezpiecznego urządzenia.
👉 Skontaktuj się z bankiem, jeśli malware mogło przechwycić Twoje dane logowania.

Malware działa cicho, ale jego skutki mogą być poważne. Zadbaj o swoje bezpieczeństwo i pamiętaj, że ostrożność to Twój najlepszy sojusznik. ♡

#Malware #CyberBezpieczeństwo #ZłośliweOprogramowanie #BezpiecznaBankowość #UważajNaZałączniki