Uważaj na złośliwe oprogramowania!

Złośliwe oprogramowanie czyli *malware* to szerokie określenie na wszelkie programy stworzone w celu wyrządzania szkód, kradzieży danych lub uzyskania nieuprawnionego dostępu do urządzenia.

Najczęstsze rodzaje złośliwego oprogramowania:

- **Wirusy i Robaki**
- **Trojany:** Podszywają się pod przydatne aplikacje, ale po zainstalowaniu otwierają hakerom „tylne drzwi" do systemu,
- **Ransomware:** Szyfruje pliki na dysku i żąda opłaty za ich odblokowanie,
- **Spyware:** Oprogramowania szpiegujące, które po cichu zbiera dane, np. historie przeglądania lub loginy,
- **Adware:** Agresywnie wyświetla reklamy, przekierowuje na niebezpieczne strony,
- **Kyloggery:** Rodzaj szpiega, który rejestruje każdy naciśnięty klawisz, co pozwala na kradzież loginów i haseł,
- **Rootkity:** Ukrywają obecność innych złośliwych programów w systemie, dając cyberprzestępcom pełna kontrolę,

➢ **Nowy trojan Albiriox:** to zaawansowane złośliwe oprogramowanie, które atakuje użytkowników systemu Android.

- **Kradzież pieniędzy –** Głównym celem trojana jest przejmowanie kontroli nad aplikacjami bankowymi i portfelami kryptowalutowymi,
- **Zdalne sterowanie –** Pozwala cyberprzestępcom na zdalne wykonywanie operacji na telefonie np. kliknięcia, przeciągnięcia, co umożliwia realizację przelewów bez wiedzy właściciela,
- **Kradzież danych –** Wyświetla fałszywe ekrany logowania ponad autentycznymi aplikacjami, aby wyłudzić hasła i kody PIN,
- **Maskowanie działań –** Może wyświetlić całkowicie czarny ekran lub fałszywy komunikat o „aktualizacji systemu", podczas gdy w tle napastnik czyści konto bankowe,
- **Szeroka lista celów –** Trojan monitoruje ponad 400 aplikacji finansowych, giełd kryptowalutowych i portfeli cyfrowych z całego świata,

- **Sposób infekcji:**
    - ✓ Fałszywe strony Google Play,
    - ✓ Instalacja aplikacji spoza oficjalnych źródeł, rozsyłane w wiadomościach SMS lub przez WhatsApp,

Jak rozpoznać zainfekowane urządzenie?

- ✓ **Nagłe spowolnienie:** System lub aplikacje działają znacznie wolniej niż zwykle.
- ✓ **Problemy z baterią i temperaturą:** Urządzenie szybko się rozładowuje i nagrzewa bez wyraźnego powodu.
- ✓ **Wyskakujące okienka:** Widzisz reklamy lub fałszywe ostrzeżenia o wirusach.
- ✓ **Zmiana ustawień:** Twoja strona główna w przeglądarce nagle się zmieniła bez Twojej zgody.
- ✓ **Częste zawieszanie się sytemu**
- ✓ **Podejrzewasz dziwną aktywność:** Znajomi otrzymują od Ciebie dziwne wiadomości, których nie wysyłałeś.

Jak się chronić?

1. **Aktualizuj system i aplikacje.**
2. **Używaj antywirusa.**
3. **Bądź ostrożny,** nie klikaj w podejrzane linki w SMS-ach i nie otwieraj załączników od nieznanych nadawców.
4. **Pobieraj z zaufanych źródeł:** korzystaj tylko z oficjalnych sklepów, tj. Google Play czy AppStore.

W przypadku podejrzenia infekcji należy uruchomić skanowanie antywirusowe, usunąć podejrzane rozszerzenia przeglądarki, zmienić hasła do kont, zablokować dostęp do Bankowości Internetowej oraz powiadomić placówkę Bankową.