Bezpieczeństwo aplikacji społecznościowych

#socialmedia #bezpieczeństwo_danych #smartfon

Bezpieczeństwo dzieci w Internecie

Internetowe życie dzieci i nastolatków toczy się przede wszystkim za pośrednictwem **smartfonów**. Młodzi ludzie rzadziej siedzą przed ekranem stacjonarnego komputera, za to coraz częściej serfują w sieci za pomocą urządzeń mobilnych. Bezpieczeństwo smartfonów to trzy obszary: bezpieczeństwo samego urządzenia, bezpieczeństwo znajdujących się w nim danych oraz sposób korzystania z niego przez dzieci.

Bezpieczeństwo smartfonu

Większość dostępnych na rynku urządzeń ma dobre zabezpieczenia techniczne, z których warto skorzystać. Podstawową ochroną jest hasło dostępu do urządzenia – może to być **PIN, odcisk palca czy skan twarzy**.

Bezpieczeństwo aplikacji

Smartfon, podobnie jak komputer, ma swój system operacyjny oraz aplikacje. Producenci oprogramowania regularnie przygotowują nowe wersje, które nie tylko wprowadzają dodatkowe funkcje, ale także coraz lepsze zabezpieczenia. Dlatego trzeba uaktualniać zarówno cały system operacyjny, jak i poszczególne aplikacje. I pamiętać, że nie wolno pobierać aplikacji z niewiarygodnych źródeł. To dotyczy także bardzo popularnych aplikacji, jak Messenger, Discord czy WhatsApp.

Niektóre aplikacje domagają się dostępu do danych. Im więcej danych dostarcza się aplikacjom, tym większe prawdopodobieństwo ich wypłynięcia lub wykorzystania przez cyberprzestępców.

Bezpieczeństwo danych

Smartfony to tak naprawdę przenośne komputery, na których przechowywane są kluczowe informacje, również finansowe. Chcąc zapewnić ich bezpieczeństwo należy korzystać z silnych haseł do wszystkich kont oraz hasła dostępu do urządzenia.

Jakie wprowadzić zasady i czego nauczyć dzieci, by zwiększyć ich bezpieczeństwo w sieci?

1. **Zasada ograniczonego zaufania** – nie wszystkie informacje w Internecie są prawdziwe i publikowane w dobrej wierze; im coś jest bardziej zachęcające tym wymaga większej ostrożności.
2. **Kontrola rodzicielska**.
3. **Wieloetapowe uwierzytelnianie**.
4. Założyć, że treści w Internecie są publiczne.
5. **Ograniczone udostępnianie** treści – może być wykorzystana przez rówieśników do ośmieszania lub hejtu.
6. Unikanie instalowania aplikacji nieznanego pochodzenia.
7. **Przedpłacona karta podarunkow**a na internetowe zakupy zamiast dostępu do karty kredytowej.
8. Wyłączenie u operatora **SMSów premium**.
9. Bezpieczne przechowywanie haseł zapisanych w tradycyjnym notatniku.

Gdzie szukać pomocy?

Telefon zaufania dla dzieci i młodzieży to **116 111** lub **800 12 12 12**, czynny codziennie, 24 godziny na dobę. Strona internetowa: **116111.pl** – wystarczy się zarejestrować i skontaktować z konsultantami mającymi dyżur online.

Telefon dla rodziców, nauczycieli oraz opiekunów to **800 100 100**, czynny w dni powszednie w godzinach 12:00 – 15:00. Strona internetowa: **800100100.pl**.

Poradnia Dziecko w Sieci Fundacji Dajemy Dzieciom Siłę: tel. **+48 22 826 88 62**, ul. Przybyszewskiego 20/24, Warszawa, e-mail: **poradniadws@fdds.pl**.

Gdzie zgłosić incydent lub przestępstwo internetowe?

Zgłoś incydent | CERT.PL

Policja 997

Dowiedz się więcej