Aplikacje mobilne – szare komórki Twojej komórki

Aplikacje na telefony komórkowe zdobyły sobie popularność wraz z rozpowszechnieniem nowoczesnych, wielofunkcyjnych telefonów – tzw. smartfonów. Mobilne aplikacje oferują wiele funkcji i możliwości, ale ich używanie może się wiązać z zagrożeniami (np. wyłudzeniem danych osobowych, ukrytymi opłatami).

Jak działają aplikacje?

Aplikacje to programy stworzone z myślą o rozrywce, komunikacji, edukacji itp. Są łatwe do zainstalowania i często odwołują się do różnych funkcji telefonu komórkowego, by poszerzyć swoje możliwości (np. wykorzystują bazę kontaktów, pobierają dane z Internetu, zbierają dane z odbiornika GPS).

Gdzie można znaleźć aplikacje?

Zaletą aplikacji na smartfony jest łatwość, z jaką można je ściągać i instalować. Znaleźć je można w internetowych sklepach – app-shops. Aby z nich korzystać, należy zarejestrować się w sklepie. Obok programów płatnych, dostępnych jest również wiele aplikacji darmowych.

Aplikacje są z reguły przeznaczone do smartfonów z konkretnym systemem operacyjnym (tzw. platformą) i bez specjalnych adaptacji nie działają na komórkach innego typu. Najpopularniejsze systemy operacyjne dla smartfonów to: Android, iOS (Apple iPhone), Symbian, Windows Phone, BlackBerry OS i Bada OS (Samsung).

Niektóre ze sklepów oferujących aplikacje (np. App-Store firmy Apple) testują programy przed ich udostępnieniem. Sklep może też usuwać ze swojej oferty programy wadliwe lub zawierające niebezpieczne treści.

Jakie są rodzaje aplikacji?

Liczba dostępnych aplikacji sięga setek tysięcy. Najpopularniejsze z nich to programy umożliwiające korzystanie z portali społecznościowych, gier, dostęp do aktualnych informacji, elektronicznych rozkładów jazdy, prognoz pogody lub poradników. Możliwości tworzenia kolejnych aplikacji są praktycznie nieograniczone.

Uwaga: obok wielu użytecznych programów są również aplikacje stworzone jako żart lub takie, które potajemnie zbierają dane z telefonu użytkownika lub instalują niechciane oprogramowanie.

Na czym zarabiają producenci programów?

Tak jak w przypadku zwykłych programów komputerowych, istnieją aplikacje płatne i bezpłatne. W przypadku bezpłatnych, ich twórcy zazwyczaj czerpią zyski z reklam wyświetlanych w trakcie używania programu. W przypadku aplikacji płatnych, z reguły około 30 proc. opłaty pobiera sklep, reszta to zarobek twórców programu.

Jakie jest ryzyko związane z aplikacjami?

Potajemne zbieranie danych osobowych

Okazuje się, że wiele aplikacji zbiera i przekazuje wrażliwe dane użytkowników, często takie, które nie są niezbędne dla działania aplikacji, np. dane z odbiornika GPS dotyczące miejsca pobytu użytkownika.

Wirusy i szkodliwe aplikacje

W sklepach z aplikacjami znaleźć można nie tylko bezpieczne programy z zaufanych źródeł, ale – coraz częściej – i aplikacje zainfekowane wirusami. Takie programy mogą kasować lub zmieniać dane w komórce (np. kontakty) albo automatycznie wysyłać SMS-y na specjalne, płatne numery.

Polskie Centrum Programu Safer Internet

FUNDACJA DZIECI NIEZNISZCZALNE

NASK

s@ferinternet.pl

Główny Partner
Fundacja Orange

Oszustwa

Twórcy wielu darmowych aplikacji czerpią korzyści z wyświetlanych reklam. Przeważnie są to tylko niegroźne banery reklamowe, czasami jednak otwierają one linki, których kliknięcie powoduje nieświadome złożenie zamówienia, a co za tym idzie, pobranie opłaty. W takiej sytuacji użytkownicy nie są wystarczająco informowani o warunkach umowy i cenach. O tym, że zapłacili orientują się dopiero po fakcie – wiele takich opłat jest zakamuflowanych i doliczanych do rachunku telefonicznego.

Zakupy wewnątrz aplikacji (in-app)

W przypadku niektórych aplikacji (np. gier) istnieje możliwość zakupu punktów lub wirtualnych dóbr podczas używania programu (tzw. zakupy in-app). Zakupy te są bardzo szybkie, zwykle nie wymagają przejścia przez standardowy proces zamawiania produktu, co powoduje, że nieświadomie możemy wydać na nie pieniądze. Problem dotyczy szczególnie dzieci, które bawiąc się smartfonami, mogą robić zakupy, nawet o tym nie wiedząc.

Wielu producentów aplikacji na komórki nie wypełnia swoich obowiązków dotyczących informowania klienta, wynikających z praw ochrony konsumenta. W takich przypadkach zazwyczaj można odstąpić od zawartej umowy. Dodatkowo sklep powinien unieważnić umowę zawartą przez dziecko, ponieważ osoby nieletnie nie posiadają zdolności do czynności prawnych. W razie problemów i wątpliwości warto zwrócić się do działu obsługi klienta sklepu, z którego pobrano aplikację.

Porady dotyczące bezpiecznego używania aplikacji

- Zastanów się, których aplikacji naprawdę potrzebujesz lub które chcesz wypróbować. Czytaj recenzje i oceny programów, lepiej nie instaluj tych, które są nisko oceniane przez użytkowników.
- Usuwaj z telefonu aplikacje, których już nie używasz. W ten sposób minimalizujesz ryzyko, że będą one pracować w tle, wykorzystując dane z Twojego telefonu.
- Instaluj tylko aplikacje z oficjalnych sklepów, ponieważ są one albo sprawdzone, albo też operator może je zablokować lub usunąć w razie problemów.
- Przy instalacji programów sprawdzaj ustawienia prywatności (np. w systemie Android jest taka możliwość, zanim klikniesz „instaluj"). Uważaj na aplikacje, które przy uruchamianiu proszą o dostęp do zbyt wielu zasobów.
- Nie usuwaj samodzielnie zabezpieczeń systemu operacyjnego (tzw. „jailbreak" lub „rooting"), ponieważ ułatwia to działanie szkodliwych aplikacji i utrudnia instalację uaktualnień systemu, w tym również tych, które dotyczą bezpieczeństwa.
- Uważaj szczególnie na aplikacje bezpłatne i pojawiające się w nich linki reklamowe.
- Dzieci bawiące się smartfonem i grające w gry mogą nieświadomie kliknąć w płatny link bądź dokonywać zakupów in-app.
- Dezaktywuj możliwość dokonywania zakupów in-app i włączaj je tylko wtedy, gdy rzeczywiście chcesz ich użyć. W iPhonie można to przykładowo zrobić w zakładce Ustawienia/Ogólne/Ograniczenia, a w Androidzie poprzez dezaktywację usługi Google Checkout.
- Zabezpieczaj telefon przed dostępem osób niepowołanych (stosuj kod PIN i hasła dostępu).
- Instaluj w telefonie oprogramowanie antywirusowe i ochronne, aby wykrywać i usuwać szkodliwe aplikacje (bezpłatne programy to np. Lookout albo NetQin dostępne dla różnych systemów operacyjnych, Smart Surfing dla iPhone'a albo AVG Mobilation dla Androida). Różne programy oferują też możliwość zlokalizowania zgubionego bądź ukradzionego telefonu i zdalną blokadę dostępu do danych.
- Jeśli używasz Internetu w telefonie, wykorzystując wykupione pakiety danych, zwróć uwagę na to, ile danych ściągają programy w trakcie ich używania. Możesz też np. wyłączyć automatyczne aktualizacje i instalować je manualnie, gdy masz jeszcze zapas przesyłu danych lub możliwość użycia bezpłatnego łącza Wi-Fi.

Jeśli masz wątpliwości dotyczące bezpieczeństwa korzystania z aplikacji, skontaktuj się z Helpline.org.pl (bezpłatny numer telefonu 800 100 100). Helpline org.pl to wspólny projekt Fundacji Dzieci Niczyje i Fundacji Orange.

800 100 100
helpline.org.pl

Bezpłatną poradę prawną dotyczącą Twoich praw jako klienta i użytkownika aplikacji mobilnych uzyskasz na Infolinii Konsumenckiej Federacji Konsumentów: 800 007 707.

Tłumaczenie: FDN