Bezpieczny smartfon – poradnik

Smartfon

To przenośne urządzenie z systemem operacyjnym, pełniące jednocześnie rolę telefonu komórkowego oraz kieszonkowego komputera

Najpopularniejsze **systemy operacyjne** dla smarftonów to:

symbian

Loga systemów operacyjnych stanowią własność ich właścicieli, zostały użyte wyłącznie w celach informacyjnych

W Polsce odsetek smartfonów w stosunku do ogółu telefonów na rynku wynosi **24 procent*** i systematycznie rośnie

*wg. badania Google i IPSOS – Our Mobile Planet

Sprzedaż smartfonów na świecie przekroczyła w 2011 **487 milionów egzemplarzy**

23 procent Polaków* używa smartfonu do korzystania z sieci wielokrotnie w ciągu dnia, **58 procent*** bez terminala nie wychodzi z domu

Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.

Do czego używamy smartfonów?

Przeglądamy
strony WWW

Korzystamy z usług
bankowości elektronicznej

Wysyłamy
i odbieramy wiadomości
e-mail

Robimy **zdjęcia,**
kręcimy **filmy wideo**

Robimy **zakupy** on-line

Kupujemy
aplikacje

Angażujemy się w
serwisach
społecznościowych

Używamy
usług
lokalizacyjnych

Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.

Czym ryzykujesz, używając smartfona?

Dzisiejsze smartfony, dzięki swoim możliwościom i mocy obliczeniowej,
to pełnowartościowe komputery,
tylko w mniejszym „opakowaniu”

Ich lawinowo rosnąca popularność, powoduje iż przestępcy coraz częściej piszą przeznaczone wyłącznie na smartfony
złośliwe oprogramowanie

W lutym 2011 telefonom z systemem Android zagrażało
9 wirusów

Rok później było ich już...
1358
co oznacza ponad 150--krotny wzrost!

Komórkowy malware, podobnie jak w przypadku komputerów stacjonarnych, może
wykradać wrażliwe dane z zarażonej maszyny

Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.

Co można wykraść ze smartfona?

Loginy i hasła
do odwiedzanych przez Ciebie witryn WWW (w tym stron banków, sklepów, czy portali aukcyjnych)

Informacje na temat
miejsc, które odwiedzasz
(daty, godziny i lokalizacje, w których „meldował” się Twój smartfon)

Dane na temat miejsc, w których zrobiłaś/eś
zdjęcia i/lub filmy wideo
(czyli informacje nt. tego gdzie regularnie lub w danej chwili przebywamy)

Historię przeglądania witryn WWW

No i nie zapominajmy oczywiście o
liście kontaktów, SMSach, czy e-mailach

Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.

Jak zminimalizować ryzyko?

Korzystaj wyłącznie z
dedykowanej aplikacji do bankowości elektronicznej,
przygotowanej przez Twój bank
(gdzie transmisja jest szyfrowana już na poziomie aplikacji)

Jeśli nie musisz,
nie używaj opcji lokalizacyjnych
(jeśli aplikacja dla sprawniejszego działania wymaga lokalizacji, włączaj ją i wyłączaj ręcznie)

Available on the App Store

Google play

Instaluj aplikacje
wyłącznie
z oficjalnych sklepów
(przed publikacją są one sprawdzane, m.in. pod względem złośliwego kodu)

ovi

BlackBerry App World

Jeśli nie używasz np. bezprzewodowej słuchawki,
wyłączaj Bluetooth

orange

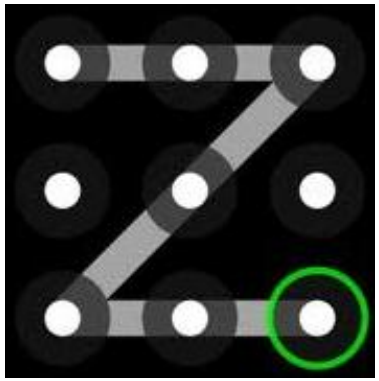
Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.

Jak zminimalizować ryzyko?

Korzystając z internetu,
bądź ostrożna/y tak samo, jak na komputerze
(nie klikaj w podejrzane linki, nie odpisuj na maile z nieznanego źródła)

Zainstaluj
program antywirusowy,
a najlepiej również program, pozwalający na
zdalne wyczyszczenie danych
w przypadku zagubienia/kradzieży telefonu

Blokuj dostęp do telefonu
za pomocą hasła, wzoru, bądź kodu PIN



ktoś, kto ukradnie/ znajdzie Twój telefon, na pewno zacznie od takiego wzoru i wpisania najpopularniejszych PINów: 1234 i 1111 ☺

Poradnik przygotowany przez Orange Polska.
Zajrzyj na stronę naszej jednostki CERT, zajmującej się bezpieczeństwem w sieci.