INFORMACJE O SPOSOBACH UNIKANIA ZAGROŻEŃ

Wypełniając obowiązek wynikający z art. 56 ust. 3 pkt 20 Prawa telekomunikacyjnego poniżej przekazujemy informację o zagrożeniach związanych ze świadczonymi przez Virgin Mobile Polska usługami telekomunikacyjnymi, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych. Więcej informacji na temat sposobów i ochrony danych osobowych znajduje się na stronie: http://www.bip.uke.gov.pl/

1.ZAGROŻENIA

W niniejszym punkcie znajdują się informacje dotyczące zagrożeń, jakie mogą wystąpić używając telefonów komórkowych lub korzystając z Internetu za ich pośrednictwem. Zalecamy aby zapoznać się z przypadkami jakie mogą doprowadzić w szczególności do utraty cennych danych, które zawarte są w naszym telefonie czy też narazić nas na wysokie opłaty za realizację niezamierzonych przez nas drogich połączeń telefonicznych.

1.1.ZŁOŚLIWE OPROGRAMOWANIE

W przypadku instalacji złośliwego oprogramowania (czyli rozwiązania, aplikacji, które mogą powodować szkody w urządzeniach końcowych, niszczyć lub wykradać dane) na urządzeniu końcowym (np. telefon) może dojść (bez wiedzy użytkownika) do niezamierzonych operacji, w szczególności:

- samoczynny restart urządzenia końcowego (telefonu),
- samoczynna wysyłka danych
- przekierowanie smsów bez wiedzy użytkownika,
- przekierowanie na płatne numery bez wiedzy użytkownika

Instalowanie na urządzeniu końcowym aplikacji niewiadomego pochodzenia może spowodować utratę kontroli użytkownika nad urządzeniem oraz doprowadzić do utraty poufności danych osobistych

1.2. POŁĄCZENIA/SMS NA NUMERY PREMIUM

Należy zwrócić szczególną uwagę na połączenia i SMSy przychodzące z nieznanych numerów zachęcające nas do odesłania SMSa czy też wykonania połączenia na wskazany numer. Nieświadomie na swój koszt wykonujemy wówczas kosztowne połączenie, a zarabia na tym nadawca.

1.3. SPOOFING – podmiana nadawcy

Zjawisko polegające na fałszowaniu, podmianie nadawcy tak aby zmylić odbiorcę i w konsekwencji wyłudzić dane, informacje wrażliwe, np. numer karty kredytowej, numery PIN, hasła, itp. Należy unikać przesyłania danych, informacji wrażliwych za pośrednictwem sms i/lub adresu email.

1.4. KARTA SIM

Należy chronić swoją kartę SIM. Osoby trzecie mogą, z niezabezpieczonej karty SIM, skopiować informacje lub zadzwonić na nasz koszt.

1.5. KRADZIEŻ DANYCH

Powszechnie dostępny z poziomu telefonu Bluetooth może okazać się skutecznym sposobem kradzieży danych z naszego urządzenia końcowego. Należy zwrócić uwagę na komunikaty pojawiające się w telefonie i wyłączać Bluetooth zawsze po zakończonej aktywności. Obecnie na rynku dostępne są również urządzenia/aplikacje, które wykorzystane w niewłaściwym celu mogą wykraść z pamięci urządzenia końcowego zawarte w nim dane (np. CSI Stick) – wystarczy Podpiąć się do urządzenia końcowego, dlatego nie należy pozostawiać urządzenia końcowego w zasięgu osób trzecich.

2. SPOSOBY OCHRONY URZĄDZEŃ KOŃCOWYCH I DANYCH

W niniejszym punkcie prezentujemy kilka z dostępnych na rynku sposobów ochrony zarówno telefonów jak i zawartych w nich cennych danych. Zachęcamy do zapoznania się z poniższymi informacjami.

2.1. BACKUP DANYCH

Zalecamy stosowanie dedykowanych aplikacji do backupu danych i ochrony urządzeń końcowych. W urządzeniu końcowym należy robić backupy cennych dla użytkownika danych. Numery telefonów (kontakty) i cenne informacje należy zapisywać na karcie SIM i/lub karcie pamięci.

2.2. HASŁO/PIN

Zalecane jest, aby wprowadzić numer PIN/HASŁO do urządzenia końcowego. Ta prosta funkcjonalność, dostępna w każdym telefonie, zabezpiecza przed niepowołanym dostępem osób trzecich w przypadku kradzieży lub zagubienia. Wskazane jest, aby po kilku nieudanych próbach wprowadzenia nr PIN/HASŁA telefon był blokowany.