**Plany wakacyjne dla Twoich cyfrowych gadżetów**

**Paszport, ubezpieczenie, rezerwacja biletów i hoteli - wszystko to wydaje się naturalne podczas planowania wakacji. Ale czy podczas przedwyjazdowego szaleństwa pamiętamy o odpowiednim przygotowaniu naszych smartfonów, tabletów czy laptopów? Warto zwrócić na to uwagę – statystyki pokazują, że większość Europejczyków nie opuszcza domu bez urządzeń mobilnych. Dzięki poradnikowi opracowanemu przez ekspertów z Kaspersky Lab każdy z łatwością zabezpieczy swoje ulubione gadżety przed wakacyjnym wyjazdem.**

Niezależnie od tego, czy planujemy wyjazd do południowo-wschodniej Azji, wypad do Nowego Jorku, zwiedzanie Rzymu czy wypoczynek na plaży nad Bałtykiem, wielu z nas nie może wyobrazić sobie wakacji bez swojego smartfona, tabletu a nawet laptopa. Oprócz prywatnej komunikacji, inną ważną przyczyną korzystania z internetu podczas urlopu jest ... niestety praca, czyli logowanie się do firmowych serwerów pocztowych i innych systemów korporacyjnych. Dlatego, w czasie wypoczynku ochrona urządzeń z dostępem do internetu jest równie istotna jak ważny paszport czy rezerwacja hotelu. Podczas przygotowań do wakacji warto zatem uwzględnić zalecenia zawarte w poradniku opracowanym przez specjalistów z Kaspersky Lab.

**Jak przygotować urządzenia mobilne do wyjazdu wakacyjnego**

Używaj aplikacji i rozwiązań bezpieczeństwa: W swojej domyślnej konfiguracji notebooki, smartfony i tablety nie są należycie chronione. Dlatego też na urządzeniach należy zainstalować oprogramowanie zabezpieczające (np. Kaspersky Mobile Security). Zapewni to ochronę prywatności i wszelkich danych przechowywanych na urządzeniu, a także umożliwi bezpieczne przeprowadzenie poufnych transakcji online.

Bądź przygotowany na zagrożenie: Zestaw pierwszej pomocy może pomóc w nagłych przypadkach medycznych. Ale co ze smartfonem lub innym urządzeniem mobilnym? Na urlopie należy być przygotowanym na najgorsze – czyli na zgubienie lub kradzież telefonu – i zawczasu zanotować wszystkie ważne dane ze swojego telefonu: numer infolinii operatora GSM, identyfikator klienta, swój numer telefonu, 15-cyfrowy numer IMEI (International Mobile Equipment Identifier), który jest niezbędnym numerem seryjnym urządzenia oraz numer karty SIM.

Bądź czujny: Nigdy nie trać swojego urządzenia mobilnego z oczu. Smartfony mają niewielkie rozmiary, w wyniku czego złodzieje mogą niezauważenie odejść z nimi w kilka sekund. Jeżeli tak się stanie, dobre mobilne rozwiązanie bezpieczeństwa pozwoli zdalnie zablokować dostęp do skradzionego urządzenia lub nawet wymazać wszystkie zapisane w nim dane - dzięki temu nikt nie uzyska do nich dostępu. Niektóre rozwiązania pozwalają także zdalnie odnaleźć urządzenie, jeżeli jest ono wyposażone w moduł GPS.

Uważaj na hotspoty: Bądź ostrożny podczas korzystania z hotspotów, czyli darmowej sieci Wi-Fi w hotelach lub kawiarniach, gdyż czają się tam zagrożenia! Jeśli jest to możliwe, nie korzystaj z bankowości online, nie rób zakupów internetowych lub innych poufnych transakcji, chyba że korzystasz z bezpiecznego połączenia VPN. Jeżeli jesteś za granicą i musisz korzystać z banku online lub z innego serwisu, który wymaga podawania wrażliwych danych, rozważ zakup lokalnej przedpłaconej karty SIM z mobilnym dostępem do internetu.

Upewnij się, że Twoje urządzenia są w pełni chronione: Aplikacje zabezpieczające zapewniają wszechstronną ochronę urządzeń. Mimo to powinieneś upewnić się, że wewnętrzne funkcje ochrony systemu są aktywne. Za przykład niech posłuży smartfon lub tablet: zawsze aktywuj blokadę ekranu, aby dostęp do urządzenia był możliwy dopiero po wpisaniu kodu PIN.

Przemyśl strategię hasła: Wielu użytkowników używa jednego skomplikowanego hasła do wszystkiego lub używa różnych, prostych haseł do poszczególnych usług online. Niestety ta strategia może bardzo szybko zawieść. Dlatego, do każdej usługi powinieneś używać oddzielnych haseł, składających się z minimum 8 znaków zawierających cyfry, symbole oraz duże i małe litery.

Informację oraz infografikę można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.