**Dziesięć sposobów na bezpieczne wakacje - porady od ekspertów z Kaspersky Lab**

**Prawie każdy z nas dokumentuje swoje wakacyjne przygody w postaci filmów i zdjęć, a w wielu przypadkach chcemy dzielić się nimi na bieżąco ze swoimi przyjaciółmi i rodziną. To dlatego do torby podróżnej pakujemy smartfony, tablety, aparaty fotograficzne i już kilka godzin po dotarciu na miejsce próbujemy połączyć się z internetem.**

Niestety roaming danych jest bardzo drogi, dlatego turyści chętniej wybierają publiczne sieci Wi-Fi. Chociaż rozwiązanie to jest bardzo powszechne – pod wieloma względami jest również ryzykowne. Eksperci z Kaspersky Lab przygotowali dziesięć porad, jak zadbać o bezpieczeństwo danych podczas wakacyjnego wyjazdu.

1. Zabezpiecz się na wypadek kradzieży sprzętu. Utrata sprzętu nadal stanowi poważny problem, ponieważ użytkownicy nieustannie zapodziewają gdzieś, gubią lub pozwalają sobie ukraść swoje urządzenia. Fizyczna ochrona to podstawowy i niezbędny pierwszy krok w kierunku ochrony informacji osobistych i danych finansowych. Wprawdzie nie możemy przykuć swojego smartfona do nadgarstka, ale istnieją pewne środki, które pomogą zapobiec utracie sprzętu. Rozwiązaniem jest włączenie śledzenia GPS w celu zlokalizowania zgubionego telefonu, w połączeniu z możliwością zdalnego wyczyszczenia danych. W takim przypadku możliwe będzie usunięcie wszystkich danych, gdy wszystkie próby odnalezienia sprzętu zawiodą. W funkcję taką wyposażoną są niektóre pakiety bezpieczeństwa mobilnego, takie jak Kaspersky Mobile Security.

2. Stosuj blokadę ekranu przy użyciu hasła, aby nikt nie mógł odblokować Twojego urządzenia i uzyskać dostępu do Twoich informacji osobistych.

3. Zabezpiecz wszystkie swoje urządzenia. Laptopy, smartfony i tablety – wszystkie są równie podatne na zagrożenia bezpieczeństwa. Cyberprzestępcy często szpiegują publiczne sieci w celu przechwycenia danych przesyłanych za pośrednictwem łącza, w tym danych uwierzytelniających operacje bankowe, haseł do kont lub innych informacji osobistych.

4. Dla bardziej technicznych użytkowników - ustaw własne połączenie VPN i wykorzystuj je podczas łączenia się za pośrednictwem publicznej sieci Wi-Fi lub hotelowego łącza internetowego – zarówno przewodowego, jak i bezprzewodowego. Cyberprzestępcy często wykorzystują hotelowe łącza internetowe w celu dokonywania szkodliwych działań wobec niczego niepodejrzewających gości. W internecie można bez problemu znaleźć darmowe rozwiązania, które pozwalają na łatwe stworzenie własnego połączenia VPN. Należą do nich między innymi: Hamachi, Comodo Unite oraz Shrew Soft.

5. Bądź ostrożny podczas korzystania z otwartej sieci Wi-Fi. Jeżeli zamierzasz skorzystać z sieci Wi-Fi w kawiarni lub na lotnisku, sprawdź je, prosząc pracownika o dostarczenie informacji dotyczących punktu dostępowego, łącznie z jego nazwą i adresem IP. Niektórzy szkodliwi użytkownicy tworzą fałszywe publiczne sieci Wi-Fi o identyfikatorach podobnych do nazw lokali oferujących darmowy internet bezprzewodowy.

6. Jeśli korzystasz z publicznych sieci Wi-Fi, nie loguj się na strony, z których mogłyby wyciec Twoje informacje osobiste, takie jak Facebook, Twitter, strony bankowe czy strony, na których przechowywane są informacje dotyczące Twojej karty płatniczej. Jeżeli musisz uzyskać dostęp do stron zawierających informacje poufne, łącznie z portalami społecznościowymi, sklepami internetowymi i serwisami bankowymi, użyj lokalnej sieci komórkowej (patrz punkt 10).

7. Stosuj skuteczny program antywirusowy na wszystkich swoich urządzeniach.

8. Unikaj korzystania z serwisów bankowości internetowej, kont osobistych oraz sklepów internetowych na publicznych komputerach (w kawiarenkach internetowych, na lotniskach, w klubach, hotelach i bibliotekach). Tego rodzaju maszyny mogą zawierać różne programy szpiegujące, które śledzą i rejestrują dane wpisywane z klawiatury i przechwytują ruch internetowy.

9. Wyłączaj Bluetooth, gdy nie jest potrzebny. Jeżeli moduł Bluetooth w Twoim smartfonie lub tablecie jest włączony bez przerwy, Twoje informacje mogą być dostępne i przechwycone przez innych.

10. Wynajmij przenośny hotspot 3G/4G lub kup kartę przedpłaconą lokalnego operatora GSM, aby uniknąć niezabezpieczonych połączeń i kosztów roamingu danych w miejscu, w którym spędzasz urlop.

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