

PRZEWODNIK PO CYBERBEZPIECZNYCH WAKACJACH

...to, że Ty masz wakacje, nie oznacza, że przestępcy też!

To niesamowity ośrodek... Szkoda, że nie istnieje







Zanim zaczniesz się pakować, zwróć uwagę na wakacyjne oszustwa.

- Jeśli to możliwe, zarezerwuj wakacje bezpośrednio w linii lotniczej, hotelu, lub za pośrednictwem renomowanego agenta / organizatora wycieczek.
- Zrób dokładne rozeznanie w internecie, aby upewnić się, że firma jest legalna.
- Upewnij się, że lot / zakwaterowanie / pociąg itp. naprawdę istnieje.
- Sprawdź opinie innych klientów.
- Płać kartą kredytową lub skorzystaj z bezpiecznej strony płatności.



Czy zamknąłeś drzwi?

Twoje cyfrowe życie potrzebuje takiej samej ochrony jak Twój dom. Zanim wyruszysz:

-  Powstrzymaj się od ogłaszania dat swoich podróży w mediach społecznościowych.
-  Przejrzyj ustawienia prywatności swoich kont w mediach społecznościowych i wyłącz geolokalizację.
-  Wykonaj kopię zapasową danych, zachowując kopie online i offline.
-  Upewnij się, że wszystkie urządzenia są chronione hasłem, kodem PIN lub informacjami biometrycznymi.
-  Zaktualizuj oprogramowanie na swoich urządzeniach.
-  Przejrzyj dane zapisane na urządzeniach – dostęp do nich może być wymagany przy wjeździe do niektórych krajów. Weź tylko niezbędne minimum lub zaszyfruj dane!

Uważaj na wyboje na trasie

Po drodze może Ci grozić wiele niebezpieczeństw. Bądź czujny przez całą podróż.



Nie ufaj publicznym kioskom ładującym – portlet ładowarki może zostać sfalszowany w celu kradzieży danych z Twoich urządzeń.



Jeśli wynajmujesz samochód, unikaj parowania telefonu z systemem komputerowym, nawet jeśli wydaje się to wygodne - możesz zostawić więcej danych niż zamierzałeś!



Ponownie przemyśl, co udostępniasz w mediach społecznościowych i unikaj upubliczniania swojej lokalizacji.

Unikaj korzystania z publicznej sieci Wi-Fi – każdy może skonfigurować bezprzewodowy hotspot.

Jeśli publiczna sieć Wi-Fi jest jedyną możliwością, skorzystaj z VPN.

Zachowaj ostrożność korzystając z publicznych komputerów – unikaj dostępu do bankowości internetowej lub zapisywania jakichkolwiek danych uwierzytelniających w przeglądarkach takich maszyn.

Pit stop: chodzi o pieniądze

Zrób sobie przerwę, aby zapoznać się ze środkami bezpieczeństwa podczas korzystania z kart płatniczych.

Jeśli zauważysz coś nietypowego w bankomacie, nie korzystaj z tego urządzenia.

Korzystając z bankomatu, uważaj na inne osoby w pobliżu – zasłoń klawiaturę, aby chronić swój kod PIN.

Nie pozwól nikomu kopiować odwrotnej strony karty

Martwisz się o bezpieczeństwo? Używaj gotówki lub kart przedpłaconych

Nie zostawiaj swoich kart bez opieki.

Nigdy nie trać karty z oczu podczas transakcji.

A droga wiedzie w przód i w przód.

Wakacje dobiegają końca, ale po powrocie jest jeszcze wiele do zrobienia.

- Poświęć trochę czasu na sprawdzenie swojej aktywności bankowej – sprawdź wszelkie podejrzane transakcje.
- Usuń wakacyjne aplikacje, których już nie potrzebujesz.
- Zmień hasło, jeśli uważasz, że którekolwiek z twoich urządzeń lub kont mogło zostać zagrożone.
- Utwórz kopię zapasową nowych danych – nie chcesz stracić tych fajnych zdjęć z wakacji!



NASK



EUROPOL

EC3
European Cybercrime
Centre

Wiele z tych wskazówek można zastosować w życiu codziennym – pamiętaj o nich!
Jeśli padniesz ofiarą cyberprzestępstwa, zgłoś to policji.