Bezpieczne wakacje w sieci

NASK akademia

NASK

1

Zadbaj o swój smartfon i inne urządzenia mobilne

Gdy urządzenia mobilne zabieramy ze sobą na wakacje, nietrudno o ich zgubienie, uszkodzenie czy kradzież. Pamiętaj o ich dobrym zabezpieczeniu.

- Zabezpiecz telefon / laptop / tablet silnym hasłem dostępu, co utrudni korzystanie z niego przez niepowołane osoby i uchroni Cię przed wykradzeniem poufnych danych, jeśli stracisz urządzenie
- Nie zostawiaj telefonu / laptopa w widocznych i łatwo dostępnych miejscach
- Sprawdź, czy masz przy sobie telefon, gdy wychodzisz z autokaru, lotniska, hotelu, kawiarni itp.
- Przed wyjazdem na wakacje zrób kopię zapasową – w razie kradzieży, zagubienia czy zniszczenia urządzenia nie utracisz wszystkich danych
- W przypadku utraty telefonu skontaktuj się ze swoim operatorem sieci komórkowej i zgłoś utratę telefonu, aby zablokować numer*, nie zapomnij o zmianie haseł do wszystkich aplikacji, które miałeś zainstalowane na telefonie
- W przypadku kradzieży urządzenia powiadom policję *

2

Poznajesz nowe osoby?

Nowo poznana osoba to nie jest Twój dobry znajomy– miej do niej ograniczone zaufanie.

- Zabezpiecz swoje konto na profilu społecznościowym silnym hasłem
- Nikomu nigdy nie udostępniaj swojego hasła
- Chroń swoje dane – nie podawaj zbyt wielu szczegółów o sobie. Nawet pozornie nieistotne informacje, złożone w całość, mówią o Tobie wiele i mogą być wykorzystane przeciwko Tobie
- Pamiętaj o wylogowaniu z konta na profilu społecznościowym
- Nie pobieraj załączników i nie klikaj w nieznane linki, które dostajesz od nieznajomych
- Jeśli zamierzasz spotkać się z osobą poznaną w sieci, powiedz o tym komuś, do kogo masz zaufanie, zabierz na spotkanie koleżankę lub kolegę

*jeśli nie masz 18 lat, muszą to zrobić za Ciebie rodzice

3

Publikujesz zdjęcia z wakacji?

Zdjęcie raz wrzucone do sieci zostaje tam na zawsze i może zostać użyte nie tak, jak byś sobie tego życzył.

- Zanim wrzucisz do sieci zdjęcie lub film, zastanów się, czy za rok również chciałbyś je zobaczyć lub czy chciałbyś, aby zobaczyli je Twoi rodzice
- Szanuj prywatność innych: jeśli chcesz zamieścić zdjęcie, na którym są także Twoi znajomi, zapytaj, czy nie mają nic przeciwko temu
- Zastanów się, czy zdjęcia/filmy, które wydają Ci się zabawne, nie są raniące lub upokarzające dla innych
- Sprawdź, czy to, co publikujesz nie narusza prawa

4

Korzystasz z publicznej sieci Wi-Fi?

Zawsze traktuj otwarte sieci publiczne jako niezaufane- nigdy nie możemy mieć 100% pewności, kto taką sieć udostępnia, ani kto z niej w danej chwili korzysta. Zdarza się, że przestępcy internetowi podszywają się pod dostawcę, chcąc wyłudzić wrażliwe dane.

- Staraj się korzystać tylko z zabezpieczonych hasłem sieci bezprzewodowych
- Jeśli korzystasz z niezabezpieczonej sieci: nie loguj się do banku, nie dokonuj transakcji finansowych, nie korzystaj z serwisów, które wymagają podania wrażliwych danych (nieznanym osobom nie udostępniaj prywatnych danych: imienia i nazwiska, numeru telefonu, adresu; nigdy nie podawaj: haseł, PINów, kodów do banku, bankomatów itp.)

Robisz zakupy online?

Kupowanie w sieci daje wiele możliwości, ale niesie za sobą także zagrożenia. Zanim coś kupisz zastanów się, czego tak na prawdę potrzebujesz i czy miejsce, w którym robisz zakupy jest godne zaufania.

- Przed dokonaniem zakupów sprawdź wiarygodność sprzedającego: poszukaj informacji o nim, historii wcześniejszych transakcji, sprawdź czy posiada wpis do KRS, certyfikaty zaufania, itp.
- Twoje podejrzenia powinien wzbudzić brak danych kontaktowych oraz brak w regulaminie informacji na temat procedury reklamacyjnej
- Udostępniaj tylko te dane, które są konieczne do dokonania zakupów
- Używaj zaufanych opcji płatności: zawsze sprawdzaj, czy strona przez którą dokonujesz płatności posiada certyfikat bezpieczeństwa (zielona kłódka)
- Uważaj na e-maile, w których sprzedający prosi Cię o dodatkowe informacje: najczęściej służą one wyłudzeniu danych. Jeśli masz wątpliwości, skontaktuj się bezpośrednio ze sklepem
- Zawsze pamiętaj o wylogowaniu się po dokonaniu zakupów: może Cię to uchronić przed hakerskim atakiem

Chcesz wiedzieć więcej?

Zajrzyj na stronę
www.akademia.nask.pl