## Cyber(nie)bezpieczeństwo na wakacjach – nie daj się oszukać!

CSIRT KNF ostrzega - cyberprzestępcy podszywają się pod znane platformy oferujące zakwaterowanie, jak booking.com czy airnb.pl. Podpowiadamy jak chronić się przed wakacyjnymi cyberoszustwami.

Wszyscy cieszymy się z nadchodzących wakacji, zadbajmy jednak o to, aby zasłużony urlop nie zakończył się przykrą przygodą. Szukając w internecie idealnego miejsca na wypoczynek możemy natknąć się na fałszywe strony, które podszywają się pod znane platformy i serwisy zajmujące się turystyką.



Cyberprzestępcy nie jeżdżą na wakacje

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego – [CSIRT KNF](https://www.knf.gov.pl/dla_rynku/CSIRT_KNF), opublikował w mediach społecznościowych [listę fałszywych stron](https://www.facebook.com/109673327865601/photos/a.110293624470238/413448290821435/?type=3&__xts__%5B0%5D=68.ARAs2B6QzwK9M0fuY8ITrZy16RA101IrrVJA1S1iIbDK7EtSbRAmjidsPceRZXuA5Mk8vGAkNHYoGZde-wjQtxlG2RFx4K-oLkbsVO6U6Ifcn7rJnAIZdM1J8epIxTaJNOLDA8pqMce-NtnJAPJjz-io1ufkLRI3jCwk0v-wws5B78QwNAk9cJN67WOhmPO3PvUNjwxa-ZqTDKl1ecU4vp5gxoy7dBxJXuIg_e8-ApnuQnmGgZdjZ3MfnP4loUTVD00IdB6-jj2sKeZ9hvLCQejOOclN29NOYjhfoC2mAP91G_O8YkE) podszywających się pod znane serwisy oferujące wynajem krótkoterminowy jak np. Booking.com i Airbnb.pl. Jeśli klikniemy z przygotowany przez oszustów link, zostaniemy przekierowani na fałszywą stronę, która jest łudząco podobna do prawdziwej strony danego serwisu. Mechanizm działania cyberprzestępców jest taki sam jak przy innych oszustwach związanych z płatnościami online i bankowością elektroniczną. Przestępcy mogą wyciągnąć od nas pojedyncze wpłaty za nieistniejący wynajem lub wręcz otrzymać dostęp do naszego konta bankowego. Wówczas możemy zostać bez pieniędzy, a na miejscu nie będzie na nas czekał opłacony pokój.

Jak nie dać cię wakacyjnym cyberoszustom? Poniżej podajemy kilka wskazówek, które warto stosować!

* Nigdy nie ufaj, zawsze weryfikuj!

Zbyt piękne, żeby było prawdziwe? To dlatego, że prawdopodobnie tak jest. Nie wierz w promocje i oferty, które są niewiarygodnie okazyjne i trwają tylko jeszcze przez godzinę. Najlepiej rezerwować wakacje przez renomowanego agenta / organizatora wycieczek, bezpośrednio w linii lotniczej lub w hotelu.

* Nie odbieraj podejrzanych e-maili

Nie klikaj w przesłane linki, sprawdzaj domeny i adresy, z których otrzymujesz e-maile. Przestępcy będą w nich odwoływać się do tego, co teraz znajduje się w centrum naszej uwagi – noclegi, hotele, tanie loty. Nie daj się nabrać na oferty limitowane, ostatnie miejsca, bilety za grosze.

* Nie ufaj dzwoniącym konsultantom

Nawet takim, którzy dzwonią z „Twojego banku”. Nie instaluj sugerowanych przez nich aplikacji na swoim smartfonie, zwracaj uwagę na stosowane socjotechniki – straszenie, przestrogi, pośpiech i przekonywanie za wszelką cenę. Jeśli nie masz pewności – odłóż słuchawkę i zadzwoń do banku z pytaniem, czy ktoś z oddziału kontaktował się z Tobą w ostatnim czasie.

* Nie loguj się do niezabezpieczonych sieci wifi

Sieci w domu czy pracy zazwyczaj są dobrze zabezpieczone. Jednak będąc w przestrzeni publicznej każdą sieć, z którą się łączymy, powinniśmy traktować jako potencjalnie niebezpieczną. Jeśli już musisz połączyć się przez publiczną sieć, nie wykonuj wtedy operacji na koncie bankowym lub takim, które zawiera wrażliwe dane.

A co jeśli padłeś ofiarą cyberoszustwa?

Jeśli podejrzewasz oszustwo internetowe zgłoś to do zespołu CSIRT NASK:

* na stronie: [https://incydent.cert.pl](https://incydent.cert.pl/)
* e-mailem: **Błąd! Nieprawidłowy odsyłacz typu hiperłącze.**
* sms-em: 799 448 084

