Oszustwa wakacyjne i jak się przed nimi ustrzec. Porady policji

Rozpoczął się czas wakacji. Planując letni wypoczynek trzeba zwrócić uwagę nie tylko na bezpieczeństwo w związku z zagrożeniem COVID-19. Oszuści nie próżnują, a nieprawdziwe oferty i „super okazje” mogą okazać się bardzo kosztowne. Biuro dw. z Cyberprzestępczością Komendy Głównej Policji oraz NASK (Naukowa i Akademicka Sieć Komputerowa) we współpracy z Europolem, ostrzegają przed nieuczciwymi ofertami internetowymi w przygotowanej kolejnej kampanii prewencyjnej.

Oszustwo wakacyjne występuje, gdy płacisz biuru podróży, agencji lub podmiotowi prywatnemu za usługi wynajmu oferowane przez Internet, takie jak:

- bilety transportu (samolot, pociąg, łódź itp.);
- zakwaterowanie;
- wynajem samochodów;
- kompletne pakiety wakacyjne, zawierające wszystkie lub

niektóre z powyższych;

i dowiadujesz się, że zarezerwowana usługa nie istnieje lub została opłacona nie z Twoich pieniędzy, ale ze skradzionej karty innej ofiary, co powoduje, że zakup jest nieważny.

Często przestępcy chcą Twoich pieniędzy. Jednak w wielu przypadkach oszustwo jest tylko częścią większego planu – przestępcy wykorzystają skradzione dane karty kredytowej jednej osoby do zakupu legalnych usług turystycznych, które następnie oferują innymosobom po niższej cenie (zarabiają na powtórnej sprzedaży tej samej usługi).

Jakie są sygnały ostrzegawcze?

Kontaktuje się z Tobą agent biura podróży lub firma, z którą nigdy wcześniej nie rozmawiałeś, oferując Ci wakacje po bardzo niskiej cenie.

Oszuści używają fałszywych reklam internetowych, fikcyjnych rozmów dotyczących sprzedaży, e-maili, SMS-ów i komunikatorów, oferując niewiarygodnie niskie stawki, aby skusić Cię do rezerwacji wakacji lub zakupu usługi. Jeśli cena jest zbyt dobra, aby mogła być prawdziwa, prawdopodobnie taka nie jest.

Strona wygląda podejrzanie jeśli:

- Jest tylko kilka szczegółów i zdjęć nieruchomości lub hotelu;
- Recenzje online nie są korzystne lub wcale nie istnieją.
- Jesteś proszony o zapłatę gotówką, przelewem bankowym, np. MoneyWise lub Western Union, a nawet wirtualną walutą, taką jak Bitcoiny. Te metody płatności są trudne do wyśledzenia i nie podlegają zwrotowi (pamiętaj: przestępcy zarabiają na danych ze skradzionych kart innych ofiar i możesz być częścią tego planu).
- Jesteś namawiany do szybkiej zapłaty czyli oszust ostrzega Cię, że nieruchomość zostanie wynajęta komuś innemu lub umowa nie zostanie zawarta, o ile nie

zapłacisz natychmiast. Przestępcy mogą również twierdzić, że możesz skorzystać ze zniżki za szybką płatność.

Jak się zabezpieczyć?

Nie odpowiadaj na niespodziewane e-maile, SMS-y, wiadomości w komunikatorach, mediach społecznościowych lub telefony z ofertami wakacyjnymi.
Linki i załączniki w wiadomościach e-mail mogą prowadzić do złośliwych stron internetowych lub zawierać wirusy zarażające urządzenie.

Zarezerwuj wakacje bezpośrednio w linii lotniczej, hotelu, lub przez renomowanego agenta / organizatora wycieczek.

Przeprowadź dokładne rozeznanie w Internecie aby upewnić się, że firma jest legalna

- Poszukaj logo IATA na stronie internetowej firmy;
- Sprawdź, czy strona internetowa korzysta z bezpiecznego systemu płatności i bezpiecznego protokołu komunikacyjnego (https) do procedury rezerwacji;
- Sprawdź opinie. Ludzie mogli zamieszczać swoje doświadczenia, ostrzegając innych;
- Zwróć szczególną uwagę na nazwę i domenę witryny. Niewielkie zmiany w nazwie lub domenie przypominającej znaną markę mogą skierować Cię do zupełnie innej firmy;
- Sprawdź, czy strona internetowa oferuje pełne dane kontaktowe. Numer telefonu stacjonarnego, adres pocztowy i wszelkie inne informacje, które ułatwiłyby Ci kontakt, gdyby coś poszło nie tak;
- Sprawdź, czy strona internetowa oferuje regulamin, zasady zwrotu pieniędzy i politykę prywatności. Przed udostępnieniem jakichkolwiek danych osobom trzecim upewnij się, że uzyskano Twoją zgodę.

Zachowaj ostrożność przy zakupie biletów lotniczych ze stron internetowych, które sprzedają inne usługi, takie jak

samochody i domy wakacyjne.
Możesz sprawdzić, czy lot istnieje, odwiedzając stronę internetową danej linii lotniczej.

Masz do czynienia bezpośrednio z właścicielem nieruchomości lub agentem prywatnym? Bądź czujny!

- Poproś o dodatkowe zdjęcia i zadaj pytania dotyczące rezerwacji, pokoju, połączenia Wi-Fi, lokalizacji i obszaru;
- Nie rezerwuj w witrynach, które nie mają ikony kłódki (https) na pasku adresu;
- Zachowaj szczególną ostrożność, jeśli zostaniesz poproszony o dokonanie płatności przelewem bankowym lub gotówką; zawsze płać kartą, aby zakup był chroniony, lub skorzystaj z bezpiecznej strony płatniczej, takiej jak PayPal.

Po zakupie,

- sprawdź, czy otrzymałeś niezbędne bilety elektroniczne lub dokumenty rezerwacji;
- przejrzyj swoje dane osobowe, daty, dane hotelu oraz numery i godziny lotów;
- spróbuj potwierdzić bezpośrednio z linią lotniczą, wypożyczalnią samochodów lub hotelem, że rezerwacja została dokonana.

JEŚLI…

- Płacisz za bilety, ale ich nie dostajesz;
- Dzwonisz do firmy, w której kupiłeś bilety, ale Twoje połączenia nie są odbierane lub otrzymujesz informację, że firma nie zapewnia zwrotów;
- Powiedziano ci, że przedstawiciel klienta spotka się z Tobą na miejscu, aby przekazać Ci bilet, ale nikt się nie pojawia;
- Otrzymujesz bilety pocztą lub e-mailem jako e-bilety, ale kiedy przyjeżdżasz na miejsce, system bezpieczeństwa

Cię nie wpuszcza, ponieważ bilet jest fałszywy lub skradziony.

To jesteś ofiarą oszustwa biletowego online. Zachowaj wszystkie dowody, złóż zawiadomienie o popełnieniu przestępstwa w najbliższej jednostce Policji.

Oszustwo biletowe ma miejsce wtedy, kiedy kupujesz bilety online ze strony internetowej lub od agenta na dowolne wydarzenie, na które wymagany jest biletu wstępu, na koncert muzyczny lub festiwal, wydarzenie sportowe, takie jak mecz piłki nożnej lub występ na żywo, ale bilety albo nie docierają, albo okazują się fałszywe lub skradzione.

Jakie są znaki ostrzegawcze?

- Reklamowane bilety są albo wyprzedane na stronie oficjalnych sprzedawców, albo oficjalnie jeszcze nie trafiły do sprzedaży, ale znajdujesz witrynę, która twierdzi, że bilety są dostępne.
- W niektórych przypadkach promowane wydarzenie nawet nie istnieje.
- Adres strony internetowej jest bardzo podobny do legalnej strony internetowej sprzedaży biletów.
- Oszuści tworzą własne fałszywe firmy zajmujące się sprzedażą biletów; ich strony internetowe są łatwe do wykonania i wyglądają autentycznie. Jednak zdradzają je: adres internetowy zaczynający się od http (zamiast https) oraz brak zamkniętej kłódki w pasku adresu. Przy czym obecność kłódki i skrótu „https” nie gwarantują autentyczności strony.
- Witryna jest reklamowana za pośrednictwem poczty e-mail lub mediów społecznościowych, oferując możliwość zakupu biletów na popularne wydarzenie.
- Może to być forma phishingu; oszuści wykorzystują ogromne zapotrzebowanie na najpopularniejsze wydarzenia.
- Ograniczone dane kontaktowe wyświetlane w witrynie, z której kupujesz bilety. Powinien znajdować się tam numer

telefonu stacjonarnego i dokładny adres pocztowy.

Jak się chronić?

Zastanów się dwa razy, zanim klikniesz w link przesłany w e-mailu, komunikatorze lub mediach społecznościowych, w którym oferowane są bilety, ponieważ mogą przekierować Cię na fałszywą stronę lub zainfekować urządzenie złośliwym oprogramowaniem.

Kupuj bilety tylko w kasie klubu, u organizatora, u oficjalnego agenta lub w znanej i renomowanej witrynie wymiany biletów. Sprzedawcy zwykle informują Cię o innych legalnych punktach sprzedaży. Zawsze kontaktuj się z nimi osobiście lub sprawdź w Internecie, czy masz do czynienia z autoryzowanym sprzedawcą.
Sprawdź politykę zwrotów sprzedawcy i zawsze zachowaj paragon do czasu wydarzenia.

Przeprowadź rozeznanie, aby upewnić się, że firma jest legalna:

- Sprawdź, czy strona korzysta z bezpiecznego systemu płatności i bezpiecznego protokołu komunikacyjnego (https);
- Sprawdź recenzje. Ludzie mogli opisywać swoje doświadczenia, ostrzegając innych. Lub może nie być w ogóle recenzji;
- Zwróć szczególną uwagę na nazwę i domenę witryny. Niewielkie zmiany w nazwie lub domenie przypominającej znaną markę mogą skierować Cię do zupełnie innej firmy;
- Sprawdź, czy witryna ma pełne dane kontaktowe. Numer telefonu stacjonarnego, adres pocztowy i wszelkie inne informacje, które ułatwiłyby Ci kontakt, gdyby coś poszło nie tak. Jeśli witryna ma stronę „Skontaktuj się z nami”, ale oferuje tylko formularz do wypełnienia, może to wskazywać na fałszywą stronę internetową;
- Sprawdź, czy strona internetowa oferuje regulamin,

zasady zwrotu pieniędzy i politykę prywatności. Przed udostępnieniem jakichkolwiek danych osobom trzecim upewnij się, że uzyskano Twoją zgodę.

źr.: KPP Limanowa