NASK

PORADNIK

Cyber bezpieczne wakacje 2023

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

NASK

PORADNIK

Cyber bezpieczne wakacje 2023

AUTORKI

Anna Kwaśnik
Katarzyna Koletyńska
Zuzanna Polak

REDAKCJA

Tomasz Kulas

WSPARCIE MERYTORYCZNE

CERT Polska

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

Finansowane ze środków Kancelarii Prezesa Rady Ministrów.
Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Kancelarii Prezesa Rady Ministrów.

Spis treści

WSTĘP

Wakacyjne oszustwa phishingowe – jak się nie dać oszukać?

Wakacje są oczekiwanym z utęsknieniem okresem, w którym możemy wreszcie odpocząć od pracy, nauki oraz codziennych obowiązków i uciec od przytłaczającej rutyny. Pełni ekscytacji, z wyprzedzeniem rozmyślamy o miejscu, gdzie będziemy mogli się zrelaksować, oraz o atrakcjach, które nas tam będą otaczały. Czasem już na tym etapie dzielimy się naszą radością na platformach społecznościowych.

Niestety, zdarza się, że – zaangażowani organizacją, a potem korzystaniem z wypoczynku – tracimy czujność i jesteśmy mniej ostrożni. Na to czekają oszuści, którzy również chcą wykorzystać swoje wakacyjne „pięć minut". Stosują metody socjotechniki, które bazują na ludzkich emocjach, takich jak: złość, strach, współczucie, ciekawość, pilność, zaufanie, podekscytowanie.

Mimo, że katalog oszustw internetowych jest naprawdę obszerny, nadal najpopularniejszym typem wyłudzeń jest PHISHING. To rodzaj oszustwa, który opiera się przede wszystkim na różnych technikach manipulacji. Przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Używa do tego różnych metod komunikacji, np. poczty e-mail, komunikatora, telefonu lub osobistego kontaktu, starając się przyciągnąć naszą uwagę.

Oszuści wykorzystują różne sposoby, aby wyłudzić od nas cenne dla nich informacje: oferują fantastyczne oferty i „super okazje", ogłaszają wygraną w konkursie albo informują, że komputer został zainfekowany. Ataki te często wydają się wiarygodne – dokumenty mają oficjalne logo lub podpis, a wygląd stron internetowych nie wzbudza podejrzeń. Wszystkie te zabiegi mają na celu skłonić użytkownika do popełnienia błędu w postaci udostępnienia informacji tj. podania haseł dostępowych, kodu do płatności internetowej (np. BLIK), wrażliwych danych lub podjęcia konkretnych czynności np. otwarcia zainfekowanego załącznika, kliknięcia w link.

Dlaczego cyberprzestępcy są szczególnie aktywni w okresie wakacyjnym?

ZWIĘKSZONA AKTYWNOŚĆ ONLINE

W czasie wakacji mamy tendencję do korzystania z internetu w większym stopniu niż zwykle. Rezerwowanie wakacji, zakupy online, udostępnianie zdjęć z podróży – to wszystko sprawia, że jesteśmy aktywniejsi online, a tym samym bardziej podatni na różnego rodzaju cyberoszustwa.

ODPOCZYNEK I OBNIŻONA CZUJNOŚĆ

Wakacje to czas odpoczynku i relaksu, a także przerwa od codziennych obowiązków i rutyny. Stajemy się bardziej skłonni do podejmowania ryzykowanych zachowań i mniej uwagi przywiązujemy do zagrożeń, które mogą czyhać na nas w sieci. Takie zachowanie może prowadzić do większej podatności na oszustwa i manipulacje ze strony cyberprzestępców.

BEZTROSKIE PODEJŚCIE DO BEZPIECZEŃSTWA

Wakacyjna atmosfera oraz pośpiech mogą wpływać na nasze podejście do cyberbezpieczeństwa. Stajemy się mniej uważni i skłonni do podejmowania ryzykownych działań online, takich jak klikanie w linki bez uprzedniego sprawdzenia od kogo pochodzą i czego dotyczą, udostępnianie poufnych informacji czy pobieranie nieznanych plików.

NASILENIE AKTYWNOŚCI ORGANIZACYJNYCH

Wyjazdy, podróże, rezerwacje – wakacje to czas podróży i planowania wakacyjnych wyjazdów, stąd częstsze korzystanie z usług takich jak rezerwacje hoteli czy zakup biletów lotniczych, kolejowych, czy na wydarzenia muzyczne, festiwale czy wystawy. Cyberprzestępcy wykorzystują te sytuacje do tworzenia fałszywych stron internetowych oferujących atrakcyjne oferty wyjazdów lub wysyłania fałszywych wiadomości e-mail udających potwierdzenia rezerwacji. Wzrasta ryzyko wyłudzenia danych osobowych czy finansowych, ponieważ w czasie wakacji jesteśmy bardziej skłonni do podawania poufnych danych lub dokonywania płatności bez należytej weryfikacji.

„SEZONOWE" LUB „EVENTOWE" OSZUSTWA

Przestępcy często wykorzystują sezonowe trendy i wydarzenia, takie jak letnie wyprzedaże, festiwale czy konkursy wakacyjne, aby przyciągnąć uwagę użytkowników i wyłudzić od nich dane lub pieniądze. Atmosfera wakacyjnego luzu i beztroski sprawia, że jesteśmy bardziej podatni na atrakcyjne oferty czy nagrody, zwłaszcza jeśli są związane z wakacyjnymi przyjemnościami.

WIĘKSZA PODATNOŚĆ NA SOCJOTECHNIKĘ

Cyberprzestępcy wykorzystują socjotechnikę, manipulując emocjami i wywołując presję czasową, aby skłonić nas do podejmowania pochopnych działań, takich jak podanie poufnych informacji czy dokonanie płatności.

WZROST LICZBY DOKONYWANYCH TRANSAKCJI FINANSOWYCH

W okresie wakacyjnym często realizujemy więcej transakcji płatniczych (i na wyższe kwoty), takich jak rezerwacje hotelowe, bilety lotnicze czy zakupy online. To stwarza cyberprzestępcom więcej możliwości kradzieży danych osobowych lub przeprowadzenia oszustw finansowych.

Wszystkie te czynniki sprawiają, że wakacje są okresem atrakcyjnym dla cyberprzestępców, którzy szukają łatwych sposobów na wykorzystanie ludzkiej naiwności i nieostrożności. Dlatego ważne jest, aby zachować czujność i stosować środki ostrożności w celu ochrony siebie i swojego portfela zarówno w okresie wakacyjnym, jak i przez cały rok.

Nie zapominajmy też o edukacji innych członków rodziny i przyjaciół w zakresie cyberhigieny.

Przypominamy najważniejsze, zasady bezpiecznego korzystania z sieci:

AKTUALIZUJ OPROGRAMOWANIE

Upewnij się, że wszystkie urządzenia, takie jak komputer, smartfon czy tablet, mają zainstalowane najnowsze aktualizacje systemu operacyjnego oraz programów antywirusowych. Regularne aktualizacje pomagają w poprawianiu luk w zabezpieczeniach i chronią przed najnowszymi zagrożeniami.

ZADBAJ O BEZPIECZNE HASŁA

Stosuj silne i unikalne hasła dla każdego konta online. Warto także rozważyć korzystanie z menedżera haseł, który pomoże w bezpiecznym przechowywaniu silnych haseł.

STOSUJ DWUSKŁADNIKOWE UWIERZYTELNIANIE

Dzięki zastosowaniu uwierzytelniania 2FA poza hasłem musisz podać dodatkowe dane, np. kod generowany przez aplikację mobilną lub jednorazowy kod, który otrzymujesz SMS-em. Nawet jeśli cyberprzestępca ukradnie hasło, nie uzyska dostępu do Twojego konta.

UWAŻAJ NA PHISHING

Zwracaj szczególną uwagę na wiadomości e-mail, SMS-y czy rozmowy telefoniczne, których się nie spodziewasz, a podczas których oszuści próbują wyłudzić Twoje dane osobowe lub finansowe. Nie klikaj w linki i nie pobieraj załączników, jeśli nie masz pewności co do ich pochodzenia. Mogą zawierać złośliwe oprogramowanie lub przekierować Cię na fałszywe strony, na których oszuści będą próbować wyłudzić Twoje dane.

ZACHOWAJ OSTROŻNOŚĆ W MEDIACH SPOŁECZNOŚCIOWYCH

Uważaj, co udostępniasz na swoich profilach społecznościowych. Unikaj publikowania informacji o swojej lokalizacji, planach wakacyjnych czy zdjęć dokumentujących nieobecność w domu. Przestępcy mogą wykorzystać te informacje do celów niepożądanych, takich jak kradzież lub włamanie.

SPRAWDZAJ WIARYGODNOŚĆ WIADOMOŚCI I STRON INTERNETOWYCH

Przed dokonaniem zakupów online lub podaniem swoich wrażliwych danych w panelu logowania upewnij się, że odwiedzasz bezpieczne i sprawdzone strony internetowe. Można to zrobić, sprawdzając domenę strony, na której jesteś. Nazwa domeny znajduje się w pasku adresu i jest zazwyczaj oznaczona nieco innym kolorem. Należy ją porównać z domeną, którą zawsze widzimy, gdy się logujemy do danego serwisu. Dodatkowo w wiadomościach e-mail, SMS, zwracaj uwagę na nieścisłości takie jak niepoprawna pisownia czy prośby o podanie poufnych informacji. Jeśli masz wątpliwości, skontaktuj się bezpośrednio z instytucją, której dotyczy komunikat, korzystając z oficjalnych danych kontaktowych. Nie spiesz się, sprawdź zanim zapłacisz.

TWÓRZ KOPIE ZAPASOWE

Wykonuj regularnie kopie zapasowe swoich danych, zarówno na komputerze, jak i na innych nośnikach, takich jak dyski zewnętrzne czy chmurowe usługi przechowywania danych. W przypadku utraty danych z powodu awarii technicznej lub ataku, będziesz mieć możliwość ich odzyskania.

Zostało Ci kilka dni do wyjazdu? Zanim wybierzesz się na wymarzone i bezpieczne wakacje, pamiętaj o:

1. **zaktualizowaniu** systemu swojego urządzenia, wszystkich aplikacji, a zwłaszcza programu antywirusowego
2. **zasadzie** nieinstalowania na swoim urządzeniu aplikacji pochodzących z niezaufanych źródeł
3. **zabezpieczeniu** sprzętu silnymi hasłami (to – w przypadku jego utraty – znacząco utrudni dostęp niepowołanych osób do danych, które tam przechowujesz)
4. **zaszyfrowaniu** urządzenia (to także uniemożliwia osobom postronnym dostęp do Twoich danych)
5. **zrobieniu** pełnej kopii zapasowej danych – jeśli to zrobisz, nawet jeśli coś się stanie Twoim urządzeniom, dane pozostaną bezpieczne i możliwe do odzyskania
6. **usunięciu** z urządzenia lub zgraniu na inny nośnik wrażliwych danych, które nie będą Ci potrzebne w czasie wakacji. Dzięki temu w przypadku np. kradzieży, nie stracisz swoich cennych danych
7. **zadbaniu** o fizyczne bezpieczeństwo swojego sprzętu – miej go zawsze przy sobie, nie udostępniaj nieznajomym osobom

Zapoznaj się z naszym poradnikiem, w którym opisujemy najpopularniejsze oszustwa wakacyjne oraz podajemy wskazówki, jak się przed nimi chronić.

NASK

CYBERBEZPIECZNE WAKACJE 2023. PORADNIK

Wakacyjne zakupy

Fałszywe biura podróży

Wielu z nas, planując dla siebie wymarzone wakacje, szuka wyjątkowych okazji, tanich ofert last minute lub promocji w różnych hotelach, ośrodkach i pensjonatach. Podekscytowani wypoczynkiem i aktywnościami, jakie na nas czekają podczas wakacji, często tracimy czujność i podejmujemy czasem nierozważne decyzje, które mogą mieć dla nas poważne konsekwencje.

Niestety, wśród dostępnych ofert wakacyjnych można natrafić na oszustów, którzy próbują podstępnie wyłudzić od nas pieniądze lub skraść nasze dane.

W jaki sposób sprawdzisz, czy dana oferta jest prawdziwa?

- Przede wszystkim **upewnij się, że firma jest wiarygodna i czy rzeczywiście istnieje**. Oszuści podszywają się pod biura turystyczne i tworzą strony, które wyglądają jak prawdziwe. Zachęcają do skorzystania z luksusowych wakacji, wycieczek ze specjalną zniżką, kuszą bardzo atrakcyjnymi cenami. Jeśli jesteś na stronie internetowej popularnego biura podróży, koniecznie sprawdź czy adres strony jest poprawny – nie zawiera błędów, literówek, a domena jest właściwa. Wiarygodność przedsiębiorcy turystycznego możesz sprawdzić w Centralnej Ewidencji Organizatorów Turystyki i Przedsiębiorców. Jeśli cokolwiek budzi Twoje wątpliwości, zrezygnuj z zakupu.

- **Upewnij się, czy na stronie internetowej wyszczególniono wszystkie dane kontaktowe** (numer telefonu, adres pocztowy i inne). Sprawdź,

czy znajdują się na niej informacje na temat zwrotu pieniędzy, polityki prywatności i regulamin. Twoją czujność powinno wzbudzić podanie małej ilości informacji w ogłoszeniu np. tylko numer telefonu komórkowego lub formularz kontaktowy. Im ogłoszenie bardziej „anonimowe", tym bardziej podejrzane. Nie dzieje się tak bez powodu – przemyśl skorzystanie z takiej oferty.

- **Zachowaj czujność podczas szukania ofert na platformach zakupowych, stronach z ogłoszeniami i w mediach społecznościowych**. Zanim zdecydujesz się na zakup oferty sprawdź, czy hotel, pensjonat lub kwatera, do której się wybierasz, istnieje i znajduje się pod wskazanym adresem. Możesz skorzystać z narzędzi internetowych, które umożliwiają lokalizację adresu. Sprawdź opinie o danym miejscu i zwróć uwagę na to, kiedy zostały umieszczone.

- **Wszystkie rozmowy z usługodawcą przeprowadzaj za pośrednictwem serwisu, z którego korzystasz**. Nie klikaj w przesyłane linki, zwłaszcza gdy za ich pośrednictwem masz dokonać płatności.

- **Uważnie przeczytaj oferty z atrakcyjnymi obniżkami ceny. Oszuści oferując różnego rodzaju kwatery kuszą atrakcyjnymi cenami bądź wysokimi rabatami**. Zanim dokonasz wpłaty sprawdź, czy dany hotel, kwatera lub pensjonat istnieje naprawdę. Jednym ze sprawdzonych sposobów jest poszukanie informacji na temat danego obiektu na forach internetowych i grupach dyskusyjnych. Możesz również sprawdzić na stronie urzędu miasta czy gminy, czy właściciel obiektu rzeczywiście prowadzi działalność gospodarczą.

Jeśli oferta wygląda na bardzo, zaskakująco wręcz atrakcyjną, powinna być traktowana jako podejrzana (co oczywiście nie znaczy, że prawdziwe okazje się nie zdarzają). Zanim dokonasz rezerwacji, dokładnie zapoznaj się z regulaminem – być może oferta zawiera ukryte koszty. Sprawdź też, czy opisywany w niej obiekt naprawdę istnieje.

Fałszywe sklepy internetowe

Okres wakacyjny to także czas letnich wyprzedaży, na których możemy kupić pełnowartościową odzież, sprzęt sportowy lub elektroniczny w korzystnej cenie.

Obecnie wiele osób preferuje kupowanie przez internet jako formę wygodniejszą niż tradycyjne zakupy. Przemawia za tym wiele czynników: zakupy zajmują mniej czasu, łatwiej znaleźć produkt w sieci niż jeździć za nim po sklepach, zakup online pozwala na dotarcie do wybranych produktów z różnych zakątków świata. Niestety, mimo wielu atutów, internetowe zakupy nie zawsze są bezpieczne. Przeglądając strony internetowe sklepów, musimy pamiętać, że niektóre z nich mogą być fałszywe, a skorzystanie z ich usług oznacza w takim wypadku nieprzyjemne konsekwencje.

Fałszywe sklepy internetowe to popularny wśród cyberprzestępców sposób, by pozyskać od nas dane i wyłudzić nasze pieniądze.

Decydując się na zakupy online, powinniśmy pamiętać o kilku podstawowych zasadach:

- **Przede wszystkim włącz czujność i zdrowy rozsądek. Jeśli natrafisz na wyjątkową ofertę, przyjrzyj się jej uważnie.** Zwróć uwagę na adres strony w pasku przeglądarki – czy nie ma błędów, literówek, ani czy adres nie jest łudząco podobny do rozpoznawalnego i popularnego sklepu. Sprawdź także domenę, na jakiej jest zarejestrowany sklep. Przyjrzyj się również całej stronie sklepu – czy jest przejrzysta, estetyczna, nie zawiera błędów językowych ani gramatycznych.

- **Sprawdź, czy działają linki umieszczone na stronie, szczególnie te prowadzące do regulaminów i polityk.** Upewnij się, że dane w nich zamieszczone wskazują na istniejącego przedsiębiorcę.

- **Zapoznaj się z polityką zwrotów i reklamacji.** Jeśli strona, na której robisz zakupy, nie ma tego określonego w regulaminie, zrezygnuj z zakupów.

- **Sprawdź, czy sklep istnieje naprawdę**, np. poprzez rejestr KRS. Dobrym rozwiązaniem może być również skontaktowanie się ze sklepem (najlepiej za pośrednictwem numeru telefonu wskazanego w zakładce „kontakt") i upewnienie się, że sklep rzeczywiście funkcjonuje.

- **Zapoznaj się opiniami na temat sklepu i sprzedawcy** – jeśli wszystkie są pozytywne i bardzo do siebie podobne oraz powstały w zbliżonym okresie, to prawdopodobnie jest to fałszywa strona. Uważaj również na opinie, które pojawiły się po kilku latach przerwy, bo być może domena, na której kiedyś istniał sklep, została przejęta przez oszustów.

- **Uważaj na „wyjątkowe okazje", „aktualne tylko dziś", „dedykowane tylko dla Ciebie" „ważne do 22.15"**. Pamiętaj, że jeśli oferta jest zbyt dobra, niespotykanie rzadka oraz niebywale korzystna, wzrasta prawdopodobieństwo, że to oszustwo.

„Oszustwa biletowe”

Wakacje to bardzo dobry okres dla branży muzycznej i kulturalnej. Potwierdzają to dane dotyczące organizacji i promocji wielu festiwali, wystaw i koncertów, które cieszą się ogromnym zainteresowaniem. Niektórzy decydują się na zakup biletu w przedsprzedaży czy w tzw. „pierwszej turze”, inni zaś czekają na ostatni moment.

Często osoby, zainteresowane koncertem, festiwalem czy inną imprezą zorganizowaną, i którym nie udało się kupić biletów, decydują się na ich zakup od osób trzecich lub szukają ich w internecie. Niestety, to dobra okazja dla oszustów, by w nieuczciwy sposób pozyskać od nas pieniądze lub dane.

Co możesz zrobić, aby nie dać się złapać na „oszustwo biletowe”?

1

Zastanów się, zanim zdecydujesz się na zakup biletu z nieoficjalnej strony lub otrzymasz od kogoś link, który rzekomo prowadzi na stronę sprzedawcy. **Sprawdź, jak wygląda strona internetowa (czy nie ma na niej błędów językowych, gramatycznych, czy podany jest kontakt, zwróć uwagę na adres strony).** Jeśli cokolwiek budzi Twoje wątpliwości, zrezygnuj z zakupu.

2

Bądź czujny, jeśli kupujesz bilet na platformie zakupowej i sprzedający proponuje Ci kontakt i zakup z pominięciem platformy. Być może ktoś próbuje Cię oszukać.

3

Kupuj legalnie. Na niektóre wydarzenia „odsprzedaż” biletów jest zabroniona przez organizatorów. Upewnij się, czy w Twoim przypadku możesz odkupić bilet od osoby trzeciej. Staraj się kupować bilety tylko na oficjalnych stronach internetowych i u organizatorów.

NASK

Jak bezpiecznie płacić w czasie wakacji

Karty płatnicze

Płatność kartą czy gotówką? – to pytanie słyszymy niemal codziennie, zarówno przy drobnych zakupach, jak i podczas opłacania pobytu w hotelu, restauracji czy kupowania biletów wstępu na różnego rodzaju wydarzenia. Płatności kartą coraz częściej zastępują tradycyjne pieniądze, a także umożliwiają szybkie transakcje online. Są wygodne i możemy nimi zapłacić nie tylko w Polsce, ale i na całym świecie.

Warto jednak pamiętać, że korzystanie
z kart płatniczych, mimo wielu korzyści,
może się też wiązać z różnymi zagrożeniami.

O czym należy pamiętać, podczas korzystania z kart płatniczych?

1 **Staraj się trzymać w określonym miejscu (zwłaszcza w portfelu) tylko jedną kartę płatniczą.**
W razie jej utraty inne karty (schowane głębiej lub w innym miejscu) nadal będą do wykorzystania. Do zablokowania jednej karty potrzebujesz mniej czasu – wystarczy telefon do banku lub kilka kliknięć w aplikacji.

2 **Nigdy nie spuszczaj swojej karty z oczu.** Nie pozwól, żeby ktokolwiek z obsługi hotelu, restauracji, sklepu czy innego punktu usługowego, zabrał kartę. W niektórych krajach jest to często spotykana praktyka, wtedy jednak lepiej płacić gotówką lub podejść z obsługą do terminala. Jeśli się zdarzy, że ktoś z obsługi będzie chciał lub próbował zeskanować Twoją kartę lub zażąda podania numeru PIN bądź kodu CVC/CVV, nie zgadzaj się – jest to niezgodne z prawem i nikt nie może wysuwać takich żądań.

3 **Nigdy nie zapisuj kodu PIN w widocznym i łatwo dostępnym miejscu**, np. na karcie, albo na kartce, którą nosisz w portfelu.

4 **Chroń dane swojej karty.**
Jeśli dokonujesz płatności kartą za zakupy online, a strona na której wprowadzasz dane, wygląda podejrzanie, zrezygnuj z transakcji.

5 **Rozważ korzystanie z jednorazowych kart wirtualnych lub przedpłaconej karty płatniczej,** których możesz używać do płatności online podczas wyjazdów.

6 **Wprowadź limity na swojej karcie płatniczej.**

O czym należy pamiętać, podczas korzystania z kart płatniczych?

7 **Zanim skorzystasz z bankomatu, sprawdź, czy nie są do niego podpięte jakieś urządzenia.** Oszuści montują na bankomatach nakładki na klawiatury, dodatkowe czytniki i ukryte kamery, które kopiują zapis z paska na karcie i nagrywają numer PIN. Jeśli z jakichś względów bankomat wzbudza Twoje podejrzenia, rozważ wypłatę pieniędzy bez wprowadzania karty (np. wypłata BLIK). Staraj się korzystać z bankomatów stojących w oddziałach lub blisko oddziałów banku. W ten sposób w razie kłopotów szybko znajdziesz pomoc.

8 **Wypłacając pieniądze, zawsze zasłaniaj ręką wpisywany kod PIN, aby osoby postronne nie mogły go zobaczyć.**

9 **Jeśli zobaczysz na swoim rachunku transakcje, których nie dokonałeś lub dostaniesz wiadomość z banku o nieudanej transakcji kartą**, natychmiast skontaktuj się z bankiem i wyjaśnij sytuację.

10 **Pamiętaj, pracownik banku, który będzie się z Tobą kontaktował w jakiejkolwiek sprawie, nigdy nie poprosi Cię o hasło dostępu do Twojego konta czy numer PIN.** Zachowaj czujność przy rozmowie z pracownikiem banku i zastosuj procedurę oddzwaniania na oficjalną infolinię.

11 Jeśli masz wątpliwości, co do korzystania z kart płatniczych, zawsze możesz skorzystać z innych sposobów płatności. W tym przypadku również zachowaj ostrożność i nie podawaj kodu do płatności innym osobom.

12 **W razie kradzieży lub zgubienia karty, jak najszybciej skontaktuj się ze swoim bankiem i zablokuj ją.**

Płatności online

Zakupy internetowe, a także płacenie za większość usług za pośrednictwem internetu stały się naszą codziennością. Tę formę płatności wykorzystujemy do zakupu wycieczek, biletów i innych atrakcji, z których korzystamy podczas wypoczynku.

Oto najważniejsze zasady dokonywania bezpiecznych płatności online, które mogą uchronić przed utratą oszczędności:

1. Zanim dokonasz płatności online, upewnij się, że korzystasz z zaufanego serwisu.

2. **Zweryfikuj, czy strona na której jesteś, jest prawdziwa.** Zwróć uwagę na adres witryny – czy nie zwiera błędów, literówek, znaków specjalnych. Jeśli cokolwiek budzi Twoje wątpliwości, zrezygnuj z transakcji.

3. Upewnij się, że hasło do konta jest trudne do odgadnięcia.

4. **Regularnie sprawdzaj swoje konto bankowe i historię transakcji, aby upewnić się, że nie ma na nim nieautoryzowanych transakcji.** W przypadku jakichkolwiek podejrzeń, natychmiast skontaktuj się z bankiem.

5. **Zachowaj ostrożność i nie udostępniaj swoich danych osobowych lub finansowych osobom, których nie znasz lub którym nie ufasz.** Unikaj również klikania w linki, które otrzymałeś z nieznanego źródła lub otwierania podejrzanych załączników w e-mailach.

6. **Uważnie czytaj powiadomienia z aplikacji Twojego banku, zwłaszcza gdy dotyczą autoryzacji płatności.** Jeśli cokolwiek się nie zgadza, skontaktuj się ze swoim bankiem.

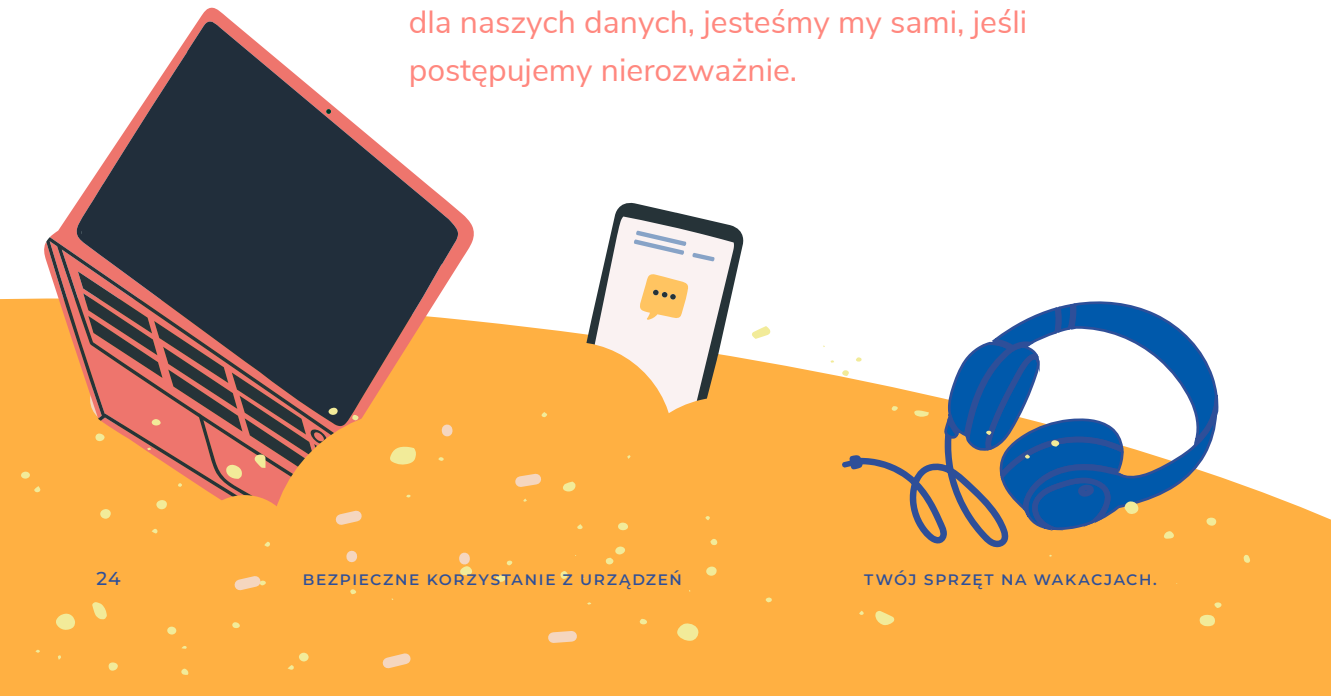
NASK

Bezpieczne korzystanie z urządzeń

Twój sprzęt na wakacjach

Urządzenia mobilne, a zwłaszcza telefony towarzyszą nam każdego dnia, również podczas wakacji. Są naszym okiem i uchem na świat. Używamy ich do robienia zakupów np. biletów, rezerwacji miejsc, opłacania rachunków za pobyt w hotelu, utrzymywania kontaktów oraz komunikacji z rodziną i nowo poznanymi znajomymi. Są naszym organizerem, pamiętnikiem, notesem. Przechowujemy w nich mnóstwo danych – nasze zdjęcia, filmy, dokumenty i inne ważne pliki lub informacje.

Korzystając z urządzeń mobilnych, musimy pamiętać, że podobnie jak komputery i laptopy, mogą one zostać zainfekowane szkodliwym oprogramowaniem. Prowadzi to do utraty danych lub ich wycieku, a to z kolei może skutkować poważnymi konsekwencjami. Możemy je stracić także w wyniku kradzieży lub zgubienia urządzenia. Jednak największym zagrożeniem dla naszych danych, jesteśmy my sami, jeśli postępujemy nierozważnie.



Jak zabezpieczyć sprzęt, zanim wyjedziesz na wymarzone wakacje:

1. **Pamiętaj o włączeniu automatycznej blokady ekranu.** Dzięki temu korzystanie z telefonu będzie możliwe dopiero po jego odblokowaniu. Większość urządzeń można zablokować poprzez kod PIN, hasło, wzór, ale również za pomocą biometrii – odcisk palca lub wizerunek twarzy.

2. **Włącz szyfrowanie danych.** Jeśli ktoś ukradnie lub znajdzie twój telefon, mimo blokady ekranu, będzie mógł odtworzyć jego zawartość. Aby tego uniknąć, włącz szyfrowanie danych. Jeśli Twój telefon ma kartę pamięci, również zadbaj o jej zaszyfrowanie.

3. **Włącz automatyczne aktualizowanie systemu operacyjnego i aplikacji, z których korzystasz.** Dzięki temu Twój sprzęt jest bardziej odporny na różne ataki i zagrożenia.

4. **Jeśli podejrzewasz, że zgubiłeś telefon lub został on skradziony, możesz skorzystać z rozwiązania „znajdź mój telefon”.** Sprawdź na stronie producenta Twojego sprzętu w jaki sposób to zrobić.

5. Urządzenia mobilne gromadzą różne, obszerne informacje o Tobie. Żeby tego uniknąć, **przejrzyj dokładnie ustawienia prywatności Twojego telefonu, sprawdź uprawnienia aplikacji z których korzystasz.** Zwróć uwagę, jakie aplikacje działają w tle oraz upewnij się, że poufne powiadomienia (takie jak kody weryfikacyjne) nie pojawiają się na ekranie, gdy urządzenie jest zablokowane.

Jak zabezpieczyć sprzęt, zanim wyjedziesz na wymarzone wakacje:

6 Funkcjonalność naszych telefonów zależy od aplikacji, z których korzystamy. Zanim je pobierzesz, zapoznaj się z ich regulaminem. **Aplikacje ściągaj tylko z oficjalnych i zaufanych źródeł.**

7 **Rób kopie zapasowe danych, które przechowujesz na swoim urządzeniu.** Możesz je zapisywać na wirtualnym dysku, dzięki czemu będziesz miał do nich dostęp w dowolnym czasie.

8 **Telefonu służbowego używaj tylko w celach służbowych.** Zachowaj szczególną ostrożność, gdy z niego korzystasz, a jeśli nie musisz – nie zabieraj go ze sobą na wyjazd prywatny. Nie rób też zdjęć ani filmów, które przypadkowo mogą zawierać poufne informacje. Stosuj się do zaleceń pracodawcy.

9 W razie utraty telefonu **skontaktuj się z operatorem swojej sieci komórkowej i zablokuj kartę SIM.** Dzięki temu ktoś kto ukradł lub znalazł telefon nie będzie mógł wykonywać połączeń na Twój koszt.

Co możesz zrobić, aby odzyskać dane z urządzenia i co zrobić, aby nikt inny nie mógł ich przeglądać?

1

Sprawdź, jakie możliwości daje producent Twojego sprzętu w sytuacji jego utraty – zgubienia lub kradzieży. Większość producentów pozwala na zdalne zablokowanie sprzętu w razie jego utraty, ale także odnalezienie go. Dopóki telefon się nie rozładuje i nie zostanie wyłączony, to na mapie będzie można podejrzeć jego aktualne położenie ze sporą dokładnością dzięki modułowi GPS oraz łączności Wi-Fi lub Bluetooth.

2

Włącz w swoim urządzeniu możliwość szyfrowania danych oraz karty pamięci, dzięki czemu osoby trzecie nie będą miały do nich dostępu, nawet jeśli urządzenie trafi w ich ręce.

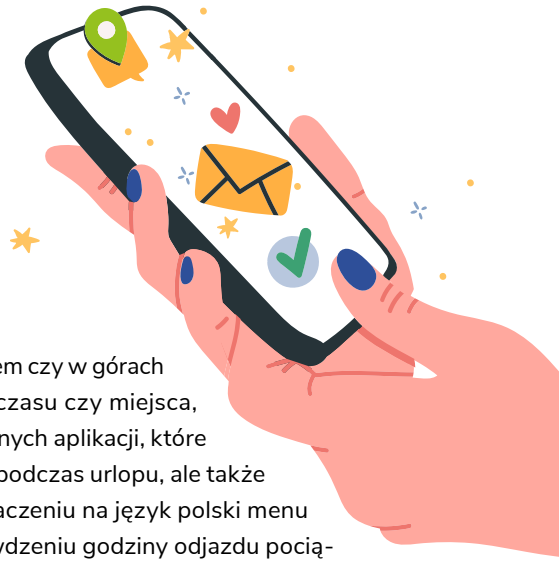
3

Na rynku są dostępne różne programy i aplikacje, za pomocą których można odzyskać dane z telefonu. Jeśli się zdecydujesz na korzystanie z nich, sprawdź czy na pewno są bezpieczne i pobieraj je tylko z oficjalnych źródeł.

4

Jeśli nie potrafisz sam odzyskać danych z Twojego urządzenia (a jest ono np. uszkodzone), skorzystaj z usług specjalistów i zanieś telefon do serwisu.

Fałszywe aplikacje



Wakacje w Polsce, za granicą, nad morzem czy w górach – obecnie wszędzie, niezależnie od czasu czy miejsca, korzystamy ze smartfonów. Istnieje wiele różnych aplikacji, które ułatwiają nam kontakt z rodziną i znajomymi podczas urlopu, ale także pomagają m.in. w dokonaniu zakupów, tłumaczeniu na język polski menu w restauracji, wyszukaniu połączenia i sprawdzeniu godziny odjazdu pociągu, czy optymalizacji zużycia paliwa podczas wakacyjnej wyprawy samochodem.

Nowo pojawiające się aplikacje czynią nasze życie łatwiejszym, ale otwierają też drzwi cyberprzestępcom , którzy mogą użyć ich do swoich nieuczciwych działań.

Oszuści szybko opanowali umiejętność tworzenia i rozpowszechniania szkodliwych aplikacji, których wygląd bardzo przypomina te prawdziwe. Podszywają się pod legalne marki, używając oficjalnych logotypów firm, znaków towarowych i obrazów, aby przekonać użytkownika do pobrania i zainstalowania szkodliwego oprogramowania.

Mimo wielu narzędzi i zabezpieczeń, fałszywe kopie legalnych aplikacji są powszechnie dostępne w oficjalnych i nieoficjalnych sklepach z aplikacjami. Jeśli zainstalujesz jedną z nich, przestępcy będą mogli przejąć kontrolę nad urządzeniem i mieć dostęp do Twoich wiadomości e-mail, SMS-ów, listy kontaktów, zdjęć, informacji o lokalizacji. Mogą nawet podsłuchiwać Twoje rozmowy.

Oto wskazówki, w jaki sposób bezpiecznie korzystać z aplikacji mobilnych:

Instaluj aplikacje pochodzące tylko z zaufanych źródeł, takich jak oficjalne sklepy z aplikacjami.

W przypadku produktów firmy Apple jest to App Store, urządzeń z systemem Android – Google Play, a sprzętu firmy Amazon – Amazon App Store. Aplikacje mobilne pobierane z tych źródeł są sprawdzane i weryfikowane pod kątem bezpieczeństwa, a te, które uważane są za niebezpieczne, zostają usuwane.

Sprawdzaj oceny i opinie na temat aplikacji.

Jeśli aplikacja jest dostępna w sklepie od dłuższego czasu i ma dużo pozytywnych ocen, to jest bardziej prawdopodobne, że można z niej bezpiecznie korzystać. Przy pobieraniu każdej kolejnej zwróć uwagę na liczbę pobrań, przejrzyj opinie i komentarze innych osób dostępne w internecie. Często użytkownicy, którzy natrafili na fałszywą aplikację, w komentarzach ostrzegają pozostałych. Jeśli podczas instalowania aplikacji wyświetli się ostrzeżenie, nie ignoruj go.

Sprawdź dokładnie uprawnienia, których wymaga aplikacja.

Zastanów się czy rzeczywiście powinna mieć dostęp do danych takich jak kontakty, lokalizacja, pamięć, aparat, mikrofon oraz innych, które wydają się niezwiązane z funkcjami oferowanymi przez instalowany program. Jeżeli warunki zainstalowania aplikacji budzą Twoje podejrzenia lub są nie do zaakceptowania np. nie chcesz przyznać uprawnień, których żąda dana aplikacja, poszukaj innej, która spełni Twoje oczekiwania.

Oto wskazówki, w jaki sposób bezpiecznie korzystać z aplikacji mobilnych:

Regularnie aktualizuj aplikacje.

Przestępcy stale poszukują luk w oprogramowaniu danej aplikacji i wymyślają sposoby, aby wykorzystać te podatności do zainfekowania urządzenia. Większość platform i producentów umożliwia automatyczne wykonywanie aktualizacji – skorzystaj z tego i włącz taką opcję. Pamiętaj! Im częściej sprawdzasz i instalujesz aktualizacje, tym Twoja aplikacja jest bardziej bezpieczna.

Nie pobieraj aplikacji z linków,

które otrzymasz od osób trzecich, nawet jeśli pochodzą od znajomego. Być może ktoś się pod niego podszywa, a wskazany link prowadzi do strony zawierającej szkodliwe oprogramowanie.

Instaluj tylko te aplikacje, których potrzebujesz i z których rzeczywiście korzystasz.

Regularnie rób przegląd aplikacji i zostawiaj tylko te, które są ci potrzebne. Pamiętaj, że każda aplikacja może posiadać luki bezpieczeństwa bądź naruszać kwestie prywatności.

Usuwaj nieużywane aplikacje.

Jeśli nie korzystasz już z danej aplikacji, po prostu ją odinstaluj. Zawsze możesz ją zainstalować ponownie, jeśli zajdzie taka potrzeba.

Publiczne sieci Wi-Fi

Pojawienie się i popularyzacja bezprzewodowych hotspotów miały wpływ na wiele aspektów naszego życia. Dzięki dostępowi do darmowych, bezprzewodowych sieci Wi-Fi możemy pracować zarówno w podróży, jak i przy kawie w pobliskiej restauracji, łączyć się z portalami społecznościowymi, oglądać filmy, grać. Darmowa łączność Wi-Fi dostępna jest prawie wszędzie – w restauracjach, hotelach, bibliotekach, pociągach, centrach handlowych, na lotniskach – a my chętnie z niej korzystamy.

Jak zatem bezpiecznie korzystać z internetu, używając do tego sieci Wi-Fi, i uniknąć niebezpiecznych sytuacji? Wystarczy przestrzegać kilku zasad:

Traktuj publiczne sieci Wi-Fi jako niezaufane.

Podczas wszelkich działań związanych z przekazywaniem poufnych informacji czy danych np. w przypadku zakupów online czy operacji bankowych, upewnij się, że jesteś na właściwej stronie i korzystasz z połączenia szyfrowanego (adres w przeglądarce rozpoczyna się od HTTPS://), albo skorzystaj z dedykowanej aplikacji mobilnej. W razie wątpliwości użyj pakietu danych od Twojego operatora komórkowego.

Twórz kopie zapasowe, zabezpiecz swój sprzęt przed utratą.

Zgubienie albo kradzież sprzętu zdarza się także podczas wakacji. Na urządzeniach przechowujemy mnóstwo wrażliwych informacji, które cyberprzestępcy mogą wykorzystać, nim zdążysz zablokować numer lub zmienić hasła. Zanim wyruszysz w wakacyjną podróż, zainstaluj aplikację lokalizującą Twoje urządzenie lub aktywuj funkcję resetującą smartfon w przypadku zgubienia czy kradzieży. Aplikacja pomoże odnaleźć urządzenie albo zablokować i usunąć dane, gdy oszust będzie próbował się do niego dostać. Dobrą praktyką jest także zrobienie kopii zapasowej danych, które znajdują się na naszym urządzeniu. W przypadku utraty sprzętu pozwoli to na ich odzyskanie.

Chroń swoje dane.

W żadnym wypadku nie podawaj nikomu danych dostępowych do swoich kont. Pamiętaj o polityce bezpiecznych haseł – muszą być silne i unikatowe (stosuj zasadę: jedno hasło do jednego konta). Jak stworzyć takie hasła, przeczytasz w poradniku CERT Polska. Warto też korzystać z dwuskładnikowego uwierzytelniania wszędzie tam, gdzie jest to możliwe. Szczególnie dotyczy to bankowości internetowej, poczty e-mail czy portali społecznościowych, czyli miejsc, w których podajemy swoje poufne dane.

Wyłącz udostępnianie plików w sieci.

Sprawdź, czy Twoje urządzenie ma włączoną opcję udostępniania plików w sieci. Jeśli tak – koniecznie wyłącz udostępnianie plików i drukarek, które umożliwia innym urządzeniom w sieci dostęp do zasobów na Twoim urządzeniu.

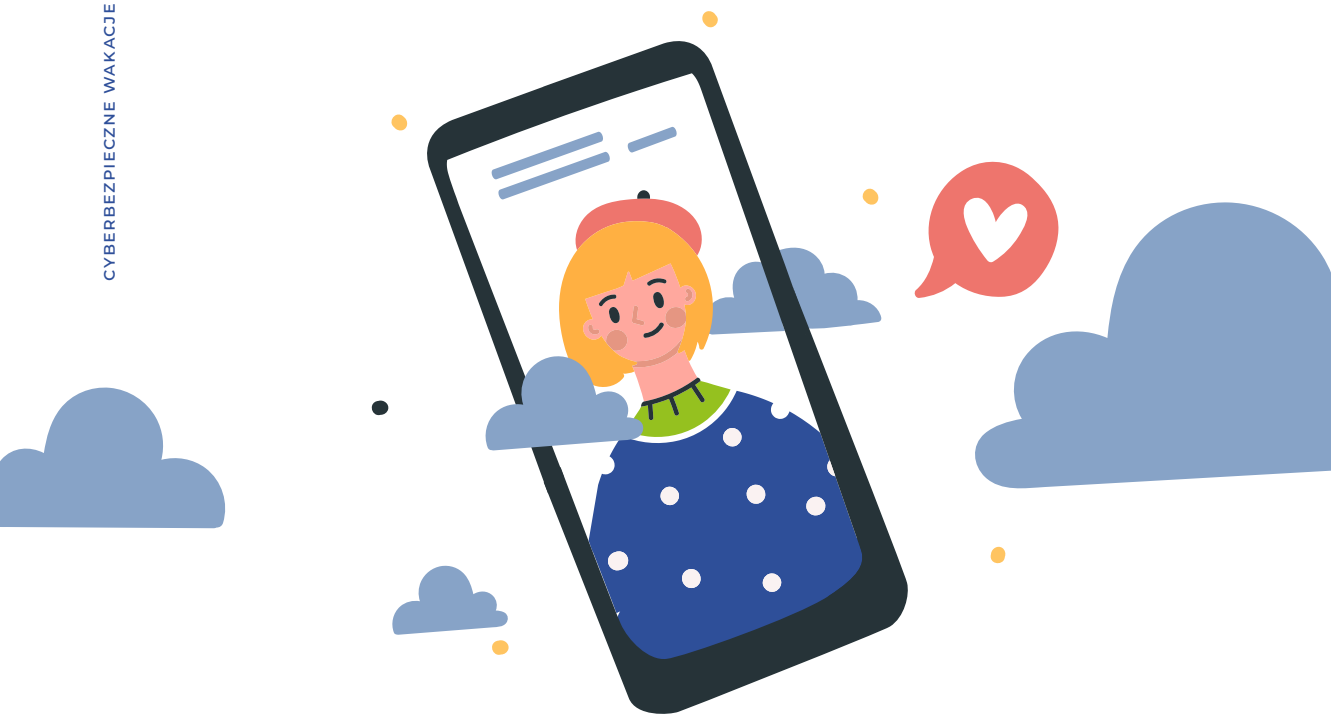
Chroń swój sprzęt.

Łącząc się z publiczną siecią Wi-Fi musisz mieć pewność, że sprzęt jest odpowiednio zabezpieczony. Pomocna jest w tym bieżąca aktualizacja aplikacji, systemu operacyjnego i oprogramowania. Pamiętaj także o aktualizowaniu programu antywirusowego.

NASK

Dane osobowe i wizerunek online

Twój wizerunek online



Jedna z najlepszych pamiątek, jakie przywozimy z wakacji, to zdjęcia i filmy z miejsc, które odwiedziliśmy. Dzięki rozwojowi technologii możemy je przygotować w wysokiej rozdzielczości, a ich jakość oddaje wszystko to, co zobaczyliśmy. Dzięki temu, że zawsze są pod ręką (najczęściej w naszym smartfonie lub w chmurze), możemy do nich wracać, kiedy tylko chcemy.

Zdjęcia i filmy z wakacji chętnie pokazujemy naszym znajomym i bliskim, a także dzielimy się nimi w mediach społecznościowych. Jednak zanim je opublikujemy warto się zastanowić, jakie informacje o nas można z nich wyczytać oraz kto i w jaki sposób może to wykorzystać.

1 **Przede wszystkim pamiętaj, że każda Twoja aktywność w internecie pozostawia cyfrowy ślad**, a zdjęcia i filmy raz wrzucone do sieci, pozostają w niej na zawsze. To, co teraz wydaje Ci się atrakcyjne i zabawne, za kilka miesięcy może być powodem do wstydu czy skrępowania lub zażenowania. Pomyśl, zanim wrzucisz do sieci prywatne zdjęcia lub filmy.

2 **Dbaj o treści publikowane w mediach społecznościowych.** Zdjęcia i filmy, które zamieścisz na swoich profilach mogą trafić do nieplanowanego odbiorcy np. Twojego pracodawcy lub osób zajmujących się rekrutacją. Pamiętaj o ustawieniach prywatności, zadbaj również o prywatność swoich bliskich. Nie udostępniaj zdjęć swoich członków swojej rodziny czy znajomych w sytuacjach, które mogą być dla nich niezręczne. Pamiętaj, że mogą trafić w niepowołane ręce.

3 **Nie przekazuj zdjęć osobom nowo poznanym.** Podczas wakacji chętnie poznajemy nowych ludzi i jesteśmy otwarci na różne relacje i znajomości. Zanim jednak podzielisz się z kimś prywatnymi informacjami na swój temat lub prześlesz materiały o charakterze intymnym, zastanów się, jak mogą zostać wykorzystane. Niestety, nie wszyscy mają czyste intencje – **uważaj, aby nie paść ofiarą szantażu z wykorzystaniem Twoich prywatnych zdjęć, szczególnie o charakterze erotycznym.**

4 **Nie pokazuj lokalizacji.** Jeśli udostępniasz relacje na żywo, udostępniasz swoją lokalizację lub w inny sposób dzielisz się tym, że nie ma Cię w miejscu zamieszkania, **możesz ściągnąć do domu złodziei.**

5 **Nie wstawiaj zdjęć i relacji, na których pokazujesz swoje dokumenty np. bilet** (lotniczy, na koncert) – zawarte na nim dane mogą zostać wykorzystane przez oszustów.

6 **Pamiętaj, aby nigdy nie udostępniać swoich prywatnych danych osobom, których nie znasz.** Nie podawaj też haseł ani kodów dostępu do poczty email, konta bankowego. Nigdy nie podawaj numerów karty płatniczej osobom trzecim.

7 **Zadbaj o szyfrowanie swoich danych** w telefonie, karcie pamięci i innych urządzeniach – w razie utraty sprzętu osoby niepowołane nie będą mogły ich przeglądać.

Kradzież danych osobowych

Kradzież tożsamości to zagrożenie, na które możemy się natknąć zarówno w świecie realnym, jak i wirtualnym. Nasze dane to cenna waluta zarówno dla oszustów, jak i różnych firm i organizacji.

Kradzież naszych danych może prowadzić nie tylko do utraty środków finansowych, ale również zagrażać naszemu wizerunkowi online, a w niektórych przypadkach może zostać wykorzystana przy popełnianiu przestępstwa internetowego.

Oszuści, którzy kradną nasze dane osobowe, mogą wykorzystać je do wyłudzeń finansowych, szantażu czy zniszczenia naszej reputacji.

Co możesz zrobić, żeby uniknąć ryzyka kradzieży tożsamości?

1 **Przejrzyj ustawienia prywatności** swoich kont w mediach społecznościowych, ogranicz widoczność swojego konta i wyłącz geolokalizację. Dokładnie przemyśl, co udostępniasz w mediach społecznościowych. W tym przypadku mniej znaczy bezpieczniej.

2 **Zadbaj o bezpieczeństwo logowania** się do swojego konta. Przestępcy mogą podszywać się pod Ciebie i oszukiwać Twoich znajomych w celu wyłudzenia pieniędzy. Dlatego tam, gdzie to jest możliwe włącz uwierzytelnianie dwuskładnikowe. Dzięki temu dane bądź informacje, które udostępniasz, będą bezpieczniejsze.

3 Pod żadnym pozorem nie zostawiaj „pod zastaw" i **nie pozwalaj na kopiowanie dokumentów** takich jak dowód osobisty, paszport, prawo jazdy, legitymacja, np. za wypożyczenie sprzętu. W sytuacjach, które wymagają podania danych, wystarczy spisanie ich z dokumentu. **Pamiętaj! Dane pozyskane z dokumentów tożsamości przestępcy mogą wykorzystać np. do wyłudzenia kredytów, pożyczek czy innych zobowiązań.**

4 **Nigdy nie publikuj w sieci zdjęć swoich dokumentów.** Zastanów się też czy warto wypełniać ankiety internetowe, w których trzeba podać swoje dane osobowe, np. PESEL czy adres zamieszkania.

5 **Zgłaszaj kradzież lub zaginięcie dokumentów.** W przypadku zgubienia lub kradzieży dokumentów np. paszportu czy dowodu osobistego należy jak najszybciej zareagować i zgłosić sprawę na policję, do urzędu, który je wydał a także w banku.

6 **Chroń swoje karty płatnicze!** W żadnym przypadku nie przechowuj w tym samym miejscu karty płatniczej i numeru PIN do niej. Nie noś go nigdy przy sobie. Zawsze zasłaniaj tę stronę karty, na której widnieje miejsce na Twój podpis. Znajduje się tam unikalny 3-cyfrowy kod CVV/CVC, który w połączeniu z numerem karty oraz imieniem i nazwiskiem i datą ważności znajdującymi się na przodzie karty umożliwia płatności w internecie z użyciem karty.

7 **Zabezpiecz swój smartfon.** Ważne jest odpowiednie zabezpieczenie sprzętu hasłami lub weryfikacją biometryczną (odcisk palca, rozponawanie twarzy). W przypadku zgubienia urządzenia należy zgłosić ten fakt swojemu operatorowi

NASK

CYBERBEZPIECZNE WAKACJE 2023. PORADNIK

Wakacyjne oszustwa finansowe

Fałszywe wakacyjne oferty pracy

Bogata oferta wakacyjnej pracy sezonowej, spowodowana m.in. okresem turystycznym, daje możliwość znalezienia atrakcyjnego zajęcia, nie tylko w kraju, ale także za granicą. Niestety, oferty pracy sezonowej, zwłaszcza takie, która obiecują „szybki zarobek", mogą być nie tylko nieprawdziwe, ale i niebezpieczne. W niektórych przypadkach związane są z wyzyskiwaniem i handlem ludźmi.

W internecie codziennie pojawiają się setki nowych ogłoszeń z ofertami pracy, które zazwyczaj nie są weryfikowane przez publikujące je serwisy. Przestępcom nie brakuje kreatywności, kiedy w grę wchodzi możliwość szybkiego wzbogacenia się kosztem nieświadomych niczego osób. Dlatego szukając pracy należy bardzo uważać, by nie stać się ofiarą oszustwa czy handlu ludźmi.

Poniżej kilka wskazówek, jak skutecznie i bezpiecznie możesz szukać wakacyjnego zarobku:

Zweryfikuj pracodawcę.

Upewnij się, że pracodawca rzeczywiście istnieje. Na stronach CEIDG oraz KRS możesz sprawdzić, czy dany podmiot został zarejestrowany. Wyszukaj firmę w internecie, sprawdź opinie o niej. Jeżeli pracodawca samodzielnie prowadzi rekrutację, to ogłoszenie zazwyczaj jest zamieszczone na jego stronie internetowej, gdzie jest możliwość bezpośredniej aplikacji, albo przekierowanie do formularza na portalu, który taką rekrutację prowadzi. Unikaj ofert, które nie mają podanej nazwy firmy, adresu, a rzekomi pracodawcy kontaktują się wyłącznie mailowo lub telefonicznie.

Uważaj na podejrzane oferty pracy.

W ogłoszeniach zwracaj uwagę na sformułowania typu: „praca tylko dla kobiet", „tylko młode panie", „szybko", „łatwo", „wypłata uzależniona od zaangażowania", „wysokie zarobki" itd. Odpowiadając na takie ogłoszenia, często przekazujemy w nich nasze dane osobowe, które przestępcy wykorzystują do zasilania ich bazy danych sprzedawanych następnie na czarnym rynku. Oszuści wykorzystują fakt, że osoby poszukujące pracy nie widzą niczego złego w przekazywaniu „przyszłemu pracodawcy" swoich danych osobowych takich jak np. imię i nazwisko, adres zamieszkania, numer telefonu, data i miejsce urodzenia, numer dowodu osobistego, PESEL czy numer konta bankowego. Czerwona lampka powinna się zapalić, kiedy w danej ofercie nie jest potrzebne doświadczenie, proponowana kwota za godzinę jest wysoka, a pracodawca nie wymaga niezbędnych dokumentów.

Czytaj dokładnie, co podpisujesz.

Jeśli zdecydujesz się na podjęcie pracy, zadbaj o podpisanie umowy, która zwiększa Twoje bezpieczeństwo oraz możliwość późniejszego domagania się zapłaty. Dodatkowo umowa określa Twój zakres obowiązków, a także to, do czego zobowiązuje się pracodawca. Dokładnie czytaj, co podpisujesz.

Wszelkie dokumenty związane z zatrudnieniem np. umowy, aneksy, zobowiązania muszą zawierać dokładne, konkretne i zrozumiałe dla Ciebie zapisy. Zadbaj o swoje dokumenty takie jak paszport, polisa ubezpieczeniowa, umowa – sfotografuj je i wyślij kopie do zaufanej osoby, np. członka rodziny. Zachowaj też całą korespondencję: wszystkie e-maile i informacje od potencjalnego „pracodawcy". Pomoże to w komunikacji z policją, jeśli zajdzie taka potrzeba. W przypadku podjęcia pracy, zwłaszcza za granicą, koniecznie poinformuj bliskich z kim i dokąd jedziesz. Jeżeli potencjalny pracodawca proponuje niepodpisywanie umowy, pamiętaj, że w razie nieprzewidzianych okoliczności pozostajesz bez żadnej ochrony.

Chroń swoje pieniądze.

Fałszywe oferty pracy wykorzystywane są przede wszystkim do wyłudzania pieniędzy. Oszust zamieszcza na portalu z ogłoszeniami bądź wysyła e-mailem „bardzo korzystną" ofertę pracy, na którą odpowiada zainteresowana osoba. Rekrutacja przebiega szybko i już po kilku dniach osoba może zgłosić się do pracy. Oszust zapewnia, że wszystko jest już załatwione, jedyne co musi zrobić, to wpłacić niewielką kwotę, np. na zakup biletu lotniczego, wykupienie wizy, pozwolenia na pracę czy opłacenie wynajętego mieszkania. Po wpłaceniu określonej kwoty, oszuści najczęściej znikają, kontakt się urywa.

Nie płać prowizji za dostęp do „dobrych" ogłoszeń.

Wiarygodny pracodawca nie pobiera opłaty wstępnej przy rekrutacji. **Jeśli potencjalny pracodawca poprosi Cię o zapłatę za sprawdzenie przeszłości, raporty kredytowe, opłaty administracyjne, materiały lub szkolenia, zrezygnuj z aplikowania.** Podobnie w przypadku opłaty za pracę za granicą – zgodnie z prawem agencje pracy mogą prosić jedynie o opłatę za tłumaczenie dokumentów. Jeśli nie jesteśmy pewni, czy organizacja, z którą mamy do czynienia, działa legalnie, wystarczy sprawdzić, czy widnieje w Rejestrze Agencji Zatrudnienia.

PAMIĘTAJ!

Dane, których nikt nie ma prawa od Ciebie żądać, to:

- **numer Twojej karty bankowej,**
- **jej kod CVV/CVC,**
- **PIN,**
- **a także dane do logowania w bankowości internetowej.**

Nigdy i pod żadnym pozorem:

- **nie przelewaj płatności, nie wysyłaj gotówki komuś, kogo nie znasz,**
- **nie podawaj numerów karty płatniczej,**
- **ani innych poufnych informacji!**

Nie bądź „mułem finansowym”

Przestępcy wykorzystują fałszywe, wakacyjne oferty pracy do „prania” nielegalnie pozyskanych pieniędzy, a osoby „zatrudniane” w firmach, często nie wiedzą, że biorą udział w przestępstwie.

Oferty pracy na „muła finansowego” to przeważnie ogłoszenia o rekrutacji na stanowiska pośrednika finansowego czy specjalisty ds. rozliczeń, a rzekomy pracodawca podszywa się pod banki, parabanki lub operatorów płatności.

Taka sezonowa, wakacyjna „praca” polega na tym, że osoba zatrudniona przesyła pieniądze, które wpływają na jej konto do wskazanych przez „pracodawcę” osób czy banków, lub też wypłaca w bankomacie i realizuje przelewy pocztowe na inne konta, za co otrzymuje prowizję. Transakcje odbywają się za pośrednictwem systemu płatności, który uniemożliwia identyfikację odbiorcy.

Pomimo tego, że ofiary często nie zdają sobie sprawy, że biorą udział w procederze prania pieniędzy i że to, co robią, jest nielegalne, nie zwalnia ich to z odpowiedzialności karnej.

Nigdy nie otwieraj osobistego konta bankowego, które ma być używane jako narzędzie Twojej pracy. Nie podawaj nikomu swoich danych osobowych, numeru konta bankowego. Zachowaj ostrożność w przypadku ofert dotyczących łatwego zarobku.

Fałszywe inwestycje i reklamy

Okres wakacyjny to często czas refleksji, poszukiwania nowych pasji, nawiązywania kontaktów z ludźmi oraz rozważania możliwości otworzenia własnego biznesu. Przeglądając strony i serwisy internetowe, nietrudno trafić na reklamy funduszy inwestycyjnych, które oferują możliwość szybkiego wzbogacenia się, a nawet kilkukrotnego pomnożenia majątku.

Charakterystyczna jest łatwość osiągnięcia sukcesu – wystarczy tylko wpłacić swoje oszczędności, zalogować się do określonej platformy i czekać na zysk. Czy jest to bezpieczne? Niestety, w wielu przypadkach takie ogłoszenia pochodzą od oszustów, którzy w podstępny sposób wyłudzają od nas pieniądze lub nasze prywatne dane. „Szybki zysk!", „Zainwestuj w kryptowaluty", „Oferta ważna tylko dziś", „On zarobił pierwszy milion, a Ty?" Tego typu i inne podobne hasła powinny wzbudzić Twoją czujność. Uwaga! Często w takich reklamach są wykorzystywane wizerunki znanych instytucji i osób, np. sportowców, polityków czy aktorów.

Na oferty fałszywych funduszy inwestycyjnych możemy się natknąć wszędzie – w mediach społecznościowych, serwisach z ogłoszeniami, reklamach w sieci czy podczas rozmowy telefonicznej. Jeśli oszuści zauważą nasze zainteresowanie inwestycją, będą nieustannie namawiać na skorzystanie z ich oferty.

Coraz częściej cyberprzestępcy podszywają się pod różne firmy i fundusze inwestycyjne, wykorzystując do tego wyszukiwarki i pozycjonowanie stron. Użytkownik, który szuka informacji w internecie na temat określonej firmy, wpisuje w wyszukiwarkę hasło, po czym zostaje przekierowany do wyników wyszukiwania. Najczęściej wybiera jedną z pierwszych pozycji, która może być niezweryfikowaną reklamą, przekierowującą potencjalną ofiarę na fałszywą witrynę prowadzoną przez oszustów. Na pierwszy rzut oka strona może wydawać się prawdziwa, zawierać wszystkie potrzebne elementy. Niestety, jeśli użytkownik wprowadzi na niej swoje dane, prawdopodobnie zostają one przechwycone przez oszustów, którzy wykorzystają je do swoich celów, np. kradzieży pieniędzy z konta bankowego ofiary.

W jaki sposób możesz się ochronić przed oszustwami inwestycyjnymi:.

1

Zawsze sprawdzaj czy domena, na którą wchodzisz, jest prawdziwa.

Podobne sztuczki oszuści stosują w reklamach banków i innych ważnych instytucji, dlatego zawsze należy sprawdzać, czy strona, na której jesteś, jest prawdziwa. W tym celu należy dokładnie zweryfikować adres URL – czy jest poprawny, nie ma w nim błędów, znaków specjalnych lub literówek, oraz czy to właściwa domena. Jeśli cokolwiek budzi Twoje wątpliwości, zakończ sesję.

2

Poradź się specjalisty.

Jeśli chcesz zainwestować swoje oszczędności, a nie masz doświadczenia, poszukaj zaufanego doradcy finansowego, brokera lub maklera giełdowego, który pomoże Ci podjąć pierwsze kroki. Nie podejmuj swoich decyzji pochopnie.

3

Zweryfikuj firmę, inwestycję czy osobę, która namawia Cię do zainwestowania.

Zachęcamy do śledzenia informacji zamieszczanych przez Urząd Komisji Nadzoru Finansowego i CSIRT KNF, gdzie możesz zapoznać się z listą stron firm i podmiotów, które są fałszywe.

Podsumowanie

Pamiętaj, aby również po wakacjach zadbać o bezpieczeństwo swoich danych oraz pieniędzy.

1. **Sprawdź swoje aktywności finansowe w banku** – przejrzyj wszystkie wakacyjne transakcje.
2. **Usuń z urządzeń aplikacje**, które zainstalowałeś na czas wakacji, a z których już nie korzystasz.
3. **Zmień hasło**, jeśli uważasz, że którekolwiek z twoich urządzeń lub kont mogło zostać zagrożone.
4. **Utwórz kopię zapasową** nowych danych, aby nie stracić fajnych zdjęć, filmów z wakacji.

Gdzie szukać pomocy

CERT POLSKA

Oszustwa i incydenty związane z bezpieczeństwem internetowym

Oszustwa komputerowe
formularz na stronie CERT Polska
e-mail: cert@cert.pl

Szkodliwe wiadomości SMS
SMS na numer: 799 448 084

Złośliwe strony wyłudzające dane i środki finansowe
formularz na stronie
https://incydent.cert.pl/domeny

UODO

Przypadki naruszenia ochrony danych osobowych

https://www.uodo.gov.pl/pl

CSIRT KNF

Przypadki oszustw finansowych

https://www.facebook.com/profile.php?id=100065127625555

https://twitter.com/CSIRT_KNF

Naruszenia na serwisach społecznościowych i portalach internetowych

- **administrator** danego serwisu, poczty e-mail, portalu społecznościowego (np. Twitter, Facebook, Instagram, YouTube);
- **formularz lub e-mail** (najczęściej w zakładce kontakt lub przycisk zgłoś naruszenie).

Reklamacje nieudanego wyjazdu

- Urząd Ochrony Konkurencji i Konsumentów
- Rzecznicy praw konsumentów
- Europejskie Centrum Konsumenckie (ECK Polska).

Jeśli padniesz ofiara oszustwa, kradzieży lub innego incydentu zagrażającemu Twojemu bezpieczeństwu za granicą, zgłoś sprawę do polskiej ambasady w danym kraju.

Źródła wiedzy

Publikacje

„Biuletyn Bezpieczeństwa Komputerowego OUCH!"

„ABC cyberbezpieczeństwa"

Jak bezpiecznie kupować w Internecie

Poradnik ransomware (2021)

Bezpieczna poczta i konta społecznościowe

Kompendium wiedzy o hasłach

Serwisy internetowe

CERT Polska: https://cert.pl/

Europejski Miesiąc Cyberbezpieczeństwa: https://bezpiecznymiesiac.pl/

NoMoreRansom: https://www.nomoreransom.org/pl/prevention-advice.html

https://legalniewsieci.pl

https://kwestiabezpieczenstwa.pl

Media społecznościowe

CERT Polska

https://facebook.com/CERT.Polska,

https://twitter.com/CERT_Polska

CSIRT KNF

https://www.facebook.com/profile.php?id=100065127625555

https://twitter.com/CSIRT_KNF

Europejski Miesiąc Cyberbezpieczeństwa

https://www.facebook.com/ECSMPL

https://twitter.com/EcsmPolska

NASK

EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA