

## Twój urlop – pracowity czas dla cyberprzestępców!

**Wakacje. Co prawda zostało jeszcze trochę czasu, ale już teraz zaczynasz planować swój wymarzony urlop - szukasz stron z ciekawymi ofertami podróży, biletami w okazyjnej cenie i tańszymi noclegami. Pamiętaj jednak, że zawsze należy zachować czujność. Świadomość istniejących zagrożeń pozwala na uniknięcie niebezpieczeństw, które cziphają w wirtualnym świecie.**

To między innymi próby wyłudzenia naszych danych wrażliwych - takich jak: dane ujawniające pochodzenie, poglądy, przekonania itp., wyłudzenia poufnych informacji - np. PESEL, login, hasło, numer konta bankowego, seria i numer dowodu osobistego, a nawet bezpośredniej kradzieży pieniędzy. Każda strona internetowa może zostać wykorzystana przez oszustów działających w sieci, którzy celowo wprowadzają odbiorcę w błąd i narażają go na duże straty. Zjawiskiem, na które należy uważać, nie tylko planując letni wypoczynek, jest phishing.

*PHISHING - rodzaj nieuczciwych działań, które opierają się na wykorzystywaniu technik socjotechnicznych w celu nakłonienia użytkowników do odwiedzenia fałszywej witryny internetowej. Użytkownicy podają na niej poufne informacje, takie jak dane logowania, a oszuści przejmują je. Inną techniką ataku phishingowego jest wysłanie SMS-a z linkiem do fałszywej strony lub wysłanie wiadomości e-mail zawierającej załącznik ze złośliwym oprogramowaniem. Kliknięcie w link lub pobranie załącznika najczęściej kończy się przejściem naszych danych do logowania do usług bankowości elektronicznej.*

W nadchodzącym sezonie wakacyjnym cyberprzestępcy z pewnością będą chętnie podszywać się pod hotele i serwisy pośredniczące w rezerwacji noclegów.

Wyobraź sobie, że szukasz niedrogiego noclegu i wchodzisz na stronę, na której wyświetlają się oferty w okazyjnej cenie. Znalazłeś wspaniałą, tani domek z przychylnymi opiniami. Obawiając się, że ktoś może Cię uprzedzić postanawiasz szybko zarezerwować lokum. Wypełniłeś pola, które wymagały podania Twoich danych osobowych, napisałeś do właściciela i w jednej z wiadomości zwrotnych zostałeś poproszony o przelanie kilkuset złotych w ramach zaliczki. W pośpiechu dokonałeś płatności, jednak po otrzymaniu pieniędzy gospodarz przestał odpowiadać...

Niestety, właśnie padłeś ofiarą oszustwa. Strona internetowa, z której korzystałeś wyglądem tylko przypominała stronę znanego serwisu, jednak w adresie przeglądarki znalazła się drobna literówka. Coraz częściej podmienione zostają pojedyncze znaki. Przykładowo, kiedy litera „m” zostanie zamieniona na dwie litery „r” i „n” (czyli po połączeniu „rn”) wygląda to bardzo podobnie do „m”. Pamiętaj również, że gdy link, zawiera nietypowe elementy, np. znak szczególny w środku słowa, to powinno wzbudzić Twoją podejrzliwość. Szczegóły często okazują się być bardzo ważne w kontekście Twojego bezpieczeństwa.

Phishing w kontekście poczty elektronicznej jest częścią szerszego zjawiska – tak zwanego spamu. Cyberprzestępca udostępniając różne wiadomości stara się nakłonić Cię do kliknięcia w załączony link i tym samym do przejścia na fałszywą stronę. Pamiętaj, zastanów się, zanim wykonasz jakiegokolwiek działanie. Zwróć uwagę na gramatykę, interpunkcję lub brak polskich znaków w komunikacie. Sprawdź adres internetowy umieszczając kursor na danej ikonce, łączy. Wyświetli Ci się na pasku w lewym dolnym rogu.

Kolejną metodą, dość popularną w ostatnim czasie, jest oszustwo „na bon turystyczny”. To forma wsparcia finansowego polskich rodzin z dziećmi, a także krajowej branży turystycznej.

Został wprowadzony w związku z trudną sytuacją tego sektora wywołaną epidemią Covid-19. Cyberprzestępcy nie przepuszczą takiej okazji, na ich celowniku znajdują się m.in. rodzice małoletnich dzieci. Jak podaje Komenda Główna Policji, sprawcy dzwonią do potencjalnych ofiar i podając się za np. pracowników Ministerstwa Rozwoju, zachęcają do skorzystania ze "specjalnej oferty na voucher urlopowy" informując, że warunkiem przysłania vouchera, jest wpłacenie na podane konto pieniędzy za dodatkowe 4 dni pobytu na wakacjach (rzekomo 3 dni są za darmo w ramach bonu). Zanim podejmiesz decyzję powinieneś sprawdzić tę informację na oficjalnej stronie instytucji, w tym przypadku Ministerstwa Rozwoju i Polskiej Organizacji Turystycznej lub skorzystać z pomocy policji. (źródło: <https://www.policja.pl/pol/aktualnosci/191636,Uwaga-Oszustwa-metoda-na-bon-turystyczny.html>)

Jak uniknąć pułapek phishingowych? Zachowaj czujność!

1. Sprawdź, czy adres strony nie budzi Twoich podejrzeń.
2. Jeżeli nie masz pewności co do wiarygodności adresata nie klikaj na nadesłane linki i nie odpowiadaj.
3. Zastanów się, czy na pewno chcesz udostępnić informacje, jakich wymaga strona (np. PESEL, numer konta bankowego).
4. Możesz wyposażyć się w dodatkowe narzędzia ochrony, takie jak oprogramowanie antywirusowe.
5. Zobacz film kampanii „Bankowcy dla edukacji”, którą realizuje Warszawski Instytut Bankowości pt. „Cyberbezpieczeństwo w praktyce. Rodzaje cyberzagrożeń” – link: <https://youtu.be/7Huv9lIQlo>

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę [www.bde.wib.org.pl](http://www.bde.wib.org.pl)

