Ostrożnie z publicznym Wi-Fi. Jak korzystać bezpiecznie?

skrót artykułu krakow.wyborcza.pl

Ada Chojnowska
05.12.2016 10:00

W ostatnich latach policjanci przestrzegali przed skimmingiem, czyli wyłudzającymi dane nakładkami na bankomatach. Oszuści mają jednak o wiele więcej sposobów - pieniądze możemy stracić, korzystając np. z otwartych sieci internetowych.

- Gdybym chciał dokonać ataku na czyjeś konto bankowe, najpierw zorientowałbym się, do której kawiarni chodzi. Następnie zbudowałbym własnego hotspota z podłączeniem do internetu o dokładnie takiej samej nazwie jak ta kawiarnia. Taki hotspot z modemem komórkowym to koszt 100-150 zł. Ustawiłbym go bez hasła i czekałbym, aż moja ofiara z tego hotspota skorzysta. W tym momencie pojawia się już mnóstwo mniej lub bardziej wyrafinowanych sposobów na to, by wykraść dane - mówi Mariusz Kochański z krakowskiej firmy Veracomp, która od 25 lat dystrybuuje różnego rodzaju rozwiązania IT, między innymi z zakresu sieci bezprzewodowych i bezpieczeństwa.

Stworzenie własnego hotspota to zresztą niejedyne rozwiązanie. Sposobów na przechwycenie danych, które przesyłamy, korzystając z otwartych, publicznych sieci, jest naprawdę mnóstwo. Tym bardziej że często nasze smartfony czy laptopy po jednym skorzystaniu z takiego Wi-Fi później łączą się z nim już automatycznie.

Od cyfrowego świata odwrotu nie ma

Z opublikowanego przez Accenture raportu "Igniting Growth in Consumer Technology" wynika, że w Polsce nasycenie smartfonami wynosi już 75 proc. i ciągle wzrasta. Niedługo będzie to już 80-90 proc. Niemal każdy użytkownik smartfona od czasu do czasu łączy się z internetem. Do tego przez smartfony jesteśmy w stanie załatwić coraz więcej spraw, a w telewizji nie brak reklam usług bankowych, z których możemy szybko i łatwo skorzystać przez telefon z dostępem do internetu.

[…]

- Nigdy nie możemy mieć pewności, do kogo należy dana sieć Wi-Fi, a także kto się do niej podłączył. Techniki podsłuchiwania i przechwytywania sygnału są rozmaite. Trzeba być tego świadomym - przestrzega Kochański.

Czy to wszystko oznacza, że z otwartych sieci nie powinniśmy korzystać wcale? Niekoniecznie. Z zasady samo połączenie przez publiczne Wi-Fi jest bezpieczne, trzeba tylko uważać, jak z niego korzystamy. - Przeglądanie stron internetowych, korzystanie z gier online - to wszystko można robić bez obaw. Jednak w momencie, kiedy musimy przekazać jakieś dane wrażliwe, zalogować się na stronie bankowej, kupić coś w sklepie internetowym czy nawet skorzystać z poczty elektronicznej, **powinniśmy być zdecydowanie ostrożniejsi** - zaleca Kochański.

Sposoby na ochronę

Co oznacza ostrożniejsi? Jednym ze sposobów jest zestawienie tzw. połączenia VPN (Virtual Private Network, czyli Wirtualna Sieć Prywatna). Jest to technologia tworząca bezpieczny pomost pomiędzy dowolnym urządzeniem podłączonym do internetu a siecią prywatną czy firmową. Zestawione łącze jest szyfrowane, co oznacza, że przesyłane dane są chronione, mamy również możliwość ukrycia naszego adresu

IP przed hakerami i programami szpiegującymi.

- Na rynku jest wiele różnego rodzaju programów, także darmowych, które z powodzeniem może u siebie zainstalować przeciętny konsument. Używane umiejętnie, znacznie podnoszą poziom naszego bezpieczeństwa - radzi ekspert.

Co jeszcze można zrobić, żeby się zabezpieczyć? **W ustawieniach naszego komputera możemy wyłączyć udostępnianie plików na naszym komputerze i jego widoczność dla obcych, potwierdzić nazwę sieci u obsługi kawiarni czy w miejscu publicznym, w którym się znajdujemy, oraz unikać automatycznego łączenia się z siecią Wi-Fi.** Takie ustawienie pozwala na to, by smartfon lub tablet nie podłączał się samodzielnie do każdej napotkanej sieci lub do tych, z których kiedyś już korzystaliśmy.

Warto też zwrócić uwagę na to, **by nie łączyć się przez sieć publiczną, kiedy korzystamy z usług bankowych** niewymagających uwierzytelnienia, np. w postaci SMS-a. Ewentualnie dokonywać płatności jedynie, jeśli korzystamy z VPN. To tym ważniejsze, że kłopot z odzyskaniem skradzionych z naszej karty kredytowej pieniędzy może być naprawdę poważny.

- O ile w krajach anglosaskich bank od razu po zgłoszeniu zwraca nam pieniądze i dopiero później sprawdza, czy nie jesteśmy oszustami, o tyle w Polsce jest na odwrót - pieniądze zostaną nam zwrócone dopiero po zakończeniu postępowania prokuratorskiego i wykryciu sprawcy - ostrzega Kochański.

Hub cyberbezpieczeństwa

Korzystanie z publicznych sieci to tylko jedno z zagrożeń. Nawet korzystając z sieci w naszym domu, zostawiamy wiele danych wrażliwych, które oczywiście mogą być wykorzystane w różnych celach. O dane jesteśmy proszeni coraz częściej. Podpisy elektroniczne, skrzynki ePUAP, profile zaufane, nawet rekrutacja do przedszkoli i szkół - wszystko to wymaga podania naszych danych. W tym wypadku za ich bezpieczeństwo odpowiadają urzędnicy i na szczęście, jak mówią eksperci, ze swojego zadania wywiązują się dobrze.

- W wielu zagadnieniach nie ma innej możliwości niż przeprowadzenie głosowania internetowego. By nie dochodziło do nadużyć, konieczne jest podanie swoich danych. Tak jest choćby w przypadku budżetu obywatelskiego. Ludzie z coraz większą nieufnością podchodzą do podawania swoich danych w internecie, dlatego muszą mieć przekonanie, że nikt tych danych nie wykorzysta w innym celu i nic się z nimi nie stanie. Jeśli to przekonanie będzie, na pewno wzrośnie też liczba głosujących - podkreśla Rafał Kulczycki, dyrektor Wydziału Rozwoju Miasta w krakowskim magistracie. - Oczywiście, nie ma systemu, którego nie da się złamać. Ze strony miasta mogę jednak powiedzieć, że robimy wszystko, co możliwe, by wszystkie te dane jak najmocniej zabezpieczyć - dodaje.

To jednak nie wszystko. Jak mówi Kulczycki, urzędnicy chcą, by Kraków stał się swego rodzaju hubem cyberbezpieczeństwa. Miejscem, w którym wspólnie pracować nad tymi zagadnieniami będą wszyscy interesariusze, począwszy od instytucji publicznych, przez firmy, instytucje finansowe, po środowiska startupowe. - W Ministerstwie Cyfryzacji są na to odpowiednie środki, musielibyśmy tylko pokonać konkurencję innych miast. Dla nas jest to kwestia priorytetowa - zaznacza Kulczycki.

Od najmłodszych lat

Jak zwraca uwagę Kochański, jest jeszcze jeden element, o który powinniśmy zadbać, tym razem w kontekście długofalowym - edukacja. I to już od najmłodszych lat. - Nauka bezpiecznego korzystania z internetu powinna być prowadzona tak jak obecnie uczy się dzieci bezpiecznego przechodzenia przez jezdnię - mówi. - Chodzi tu zarówno o zagrożenia związane z kontaktem z obcymi, publikowaniem różnego rodzaju rzeczy w sieci, jak i możliwości zostania zhakowanym. Oczywiście, w przyjazny, niezbyt skomplikowany sposób. To podstawowe zagadnienia w erze społeczeństwa informacyjnego, w którym teraz wszyscy żyjemy.