Czwarty Cyber Poradnik poświęcamy bezpiecznym podróżom XXI wieku, kiedy każdy wyposażony jest w smartfon, tablet czy też laptopa.

Sezon świąteczny większości z nas upływa pod znakiem podróży. Końcówka grudnia oraz początek nowego roku to dla nas czas powrotów do domu rodzinnego czy sylwestrowych wyjazdów. W tym czasie musimy pamiętać o wielu rzeczach – wybór ostatnich prezentów, pakowanie walizek, sprint, żeby zdążyć na pociąg czy autobus. W całym tym ferworze łatwo zapomnieć o bezpieczeństwie naszych urządzeń w podróży. Chwila nieuwagi wystarczy, aby ułatwić cyberprzestępcom dostęp do naszego urządzenia oraz naszych danych dostępowych. W dzisiejszym Cyber Poradniku nasi eksperci przygotowali kilka praktycznych wskazówek jak zadbać o bezpieczeństwo nowoczesnych technologii, które towarzyszom nam w podróży. Powiemy Ci jak przygotować się do wyjazdu ze smartfonem (lub innym urządzeniem), wyjaśnimy co zrobić jeśli go zgubisz oraz rozwiejemy wszelkie wątpliwości na temat publicznych sieci Wi-Fi.

Zanim wyjedziesz – przygotuj się!

Przed każdym wyjazdem pamiętaj o wcześniejszych przygotowaniach. To tyczy się również

Twoich sprzętów. Aby mieć pewność, że jesteś przygotowany na każdą okoliczność sprawdź jakie porady mają dla Ciebie specjaliści ds. bezpieczeństwa systemów i sieci z S.M.S.!

- **Hasła, hasła i jeszcze raz hasła.** Pewnie się powtarzamy, ale silne i odpowiednio skomplikowane hasło może okazać się Twoim wybawicielem. Pamiętaj o zastosowaniu małych i dużych liter, cyfr oraz znaków specjalnych. Stosuj inne hasła dla każdego ze swoich profili społecznościowych, aplikacji bankowych czy innych kont użytkownika. Jeśli to możliwe ustaw uwierzytelnianie dwuskładnikowe przy logowaniu.
- **Informacje na urządzeniu.** Pamiętaj, że informacje mają swoją wartość. Dlatego zwracaj uwagę jakie dane przechowujesz na swoich urządzeniach oraz czy na pewno jest to konieczne. Przed wyjazdem przejrzyj urządzenia oraz przenieś bądź usuń informacje, które nie są Ci w tym momencie potrzebne, a mogą być łakomym kąskiem dla cyberprzestępcy.
- **Kopia zapasowa.** Tak, tak wiemy, że często powtarzamy Ci również jak istotne jest tworzenie kopii zapasowych. Ale wyobraź sobie, że dzisiaj tracisz swój smartfon lub laptop, a wraz z nim wszystkie przechowywane tam dane. Urządzenie będziesz w stanie odkupić, ale informacji, dokumentów czy zdjęć nie będziesz w stanie odzyskać. W takiej sytuacji posiadanie kopii zapasowej może Cię uchronić od utraty wszystkiego.
- **Aktualizacje.** Pamiętaj o zaktualizowaniu wszystkich oprogramowań i aplikacji do najnowszych wersji. Zwykle ataki cybernetyczne wymierzone są w urządzenia działające na nieaktualnych systemach.
- **Lokalizator.** Niektóre urządzenia są wyposażone w lokalizator urządzenia (np. Apple ma opcję „Znajdź mój iPhone/iPad”, Google umożliwia zlokalizowanie urządzenia, na którym jest zalogowany użytkownik z jego kontem). Pamiętaj, aby uruchomić tę opcję przed wyruszeniem w podróż.

Zgubiłem smartfon i co dalej?

Oprócz zabezpieczenia systemu i urządzenia pamiętaj, że bezpieczeństwo fizyczne jest również istotne. Dzięki temu uchronisz się przed zgubieniem lub kradzieżą. Jednak jeśli spotkała Cię któraś z tych sytuacji to standardowo polecamy nie panikować. Jeśli skorzystałeś z naszych rad odnośnie lokalizatora możesz namierzyć swoje urządzenie. Wykonanie kopii zapasowej uchroni Cię natomiast przed utratą danych. Sprawdź także, czy po prostu nie odłożyłeś urządzenia w inne miejsce niż zwykle. Przejrzyj kieszenie, torby lub plecaki, schowki w samolocie bądź samochodzie, poproś swoich współpasażerów o pomoc.

Wi-Fi w miejscach publicznych

Największym zagrożeniem dla użytkownika w podróży są publiczne sieci Wi-Fi. Po pierwsze nie wiemy, kto taką sieć stworzył ani jakie ma zamiary wobec innych użytkowników, którzy są skłonni do niej podłączyć. To, że sieć nazywa się „WiFi Orange", „Warszawa" itp. nie znaczy, że ich właścicielem jest dana firma czy urząd miasta. Tym samym nigdy nie mamy pewności, kto odpowiada za ich zabezpieczenia. Po drugie nigdy nie jesteśmy w stanie stwierdzić, kto razem z nami korzysta. W jednym z naszych artykułów przedstawialiśmy dokładniej zagadnienia bezpieczeństwa Wi-Fi od strony technicznej (w tym szczegółowo opisaliśmy metodologię oraz etapy ataku typu Man In The Middle), więc serdecznie zapraszamy Was do przypomnienia sobie tego tekstu. Dlatego zalecamy, aby sieci Wi-Fi, do których mamy dostęp w sferze publicznej traktować jako niezaufane. Dlatego ważne jest, aby odpowiednio zabezpieczyć swoje urządzenie jeśli zdecydujemy się korzystać z takiego połączenia podczas podróży. Dodatkowo możesz również rozważyć korzystanie z wirtualnej sieci prywatnej (z ang. VPN – virtual private network), która zapewnia bezpieczeństwo przesyłania danych. Pamiętaj również, aby ograniczyć korzystanie z kluczowych aplikacji czy usług (bankowość elektroniczna, poczta e-mail czy korespondencja urzędowa) w przypadku, jeśli korzystasz z publicznej sieci Wi-Fi.

Mamy nadzieję, że teraz wiesz już jak bezpiecznie korzystać ze swoich urządzeń podczas podróżowania. Zachęcamy Cię do odwiedzenia naszych profili w mediach społecznościowych

(Facebook oraz Twitter) , gdzie możemy podyskutować na temat bezpieczeństwa w sieci.

Czytałeś już nasze wcześniejsze numery **Cyber Poradnika**? Jeśli nie to serdecznie zachęcamy Cię do ich lektury i podnoszenia świadomości nt. cyberbezpieczeństwa.

Cyber Poradnik nr 1 – Bezpieczne zakupy

Cyber Poradnik nr 2 – Co zrobić, gdy padniesz ofiarą cyberprzestępcy?

Cyber Poradnik nr 3 – Phishing