OUCH!
Biuletyn Bezpieczeństwa Komputerowego

# Bezpieczeństwo podczas okresu świątecznego

## Wstęp

Okres świąteczny zbliża się wielkimi krokami, wielu z nas ruszy w podróż do swoich najbliższych aby ich odwiedzić i spędzić święta w rodzinnym gronie. Poniżej przedstawiamy kilka wskazówek, które pomogą zwiększyć bezpieczeństwo w tym okresie. Jeśli należysz do tej grupy podróżników, zapoznaj się z nimi.

- **Urządzenia mobilne**: Zabierz ze sobą tylko potrzebne urządzenia. Zabierając ze sobą tylko niezbędne urządzenia, ograniczasz możliwość zgubienia bądź kradzieży któregoś z nich. Czy wiesz, że prawdopodobieństwo zgubienia urządzenia mobilnego jest znacznie większe niż prawdopodobieństwo jego kradzieży? Za każdym razem, gdy opuszczasz pokój hotelowy, restaurację, taksówkę, pociąg lub samolot, upewnij się, że niczego nie pozostawiłeś i masz wszystkie swoje urządzenia. Jeśli podróżujesz z dziećmi, pomyśl za nich i sprawdź czy nie zostawiły urządzenia na siedzeniu w pociągu czy krześle restauracyjnym.

  Natomiast jeśli chodzi o samo urządzenie, które zdecydujesz się zabrać ze sobą, upewnij się, że ma wgrane najświeższe aktualizacje bezpieczeństwa. Włącz blokadę ekranu, która utrudni osobom postronnym wgląd do urządzenia. Jeśli urządzenie posiada możliwość zdalnego śledzenia, włącz tę opcję. Z pewnością będzie pomocna z sytuacji jego kradzieży lub zgubienia. Ponadto wiele urządzeń posiada opcję zdalnego wymazania danych z pamięci urządzenia, warto to wiedzieć i o tym pamiętać, a w koniecznym momencie z niej skorzystać. Tym sposobem jeśli z jakiegoś powodu utracisz urządzenie, będziesz mógł skasować z niego poufne dane, zabezpieczając się tym samym przed przechwyceniem ich przez osoby postronne. Pamiętaj o zrobieniu kopii zapasowej danych urządzenia, które zabierasz ze sobą w podróż. Tylko w ten sposób łatwo będzie odzyskać dane przechowywane w pamięci urządzenia w razie jego utraty.

- **Sieć Wi-Fi**: Podczas podróży może zajść potrzeba połączenia się z publiczną siecią Wi-Fi. Miej na uwadze, że nie wiesz kto konfigurował tę sieć, kto ją monitoruje oraz kto jeszcze jest do niej podłączony. Zamiast łączyć się z publiczną siecią Wi-Fi, bezpieczniejszą opcją jest utworzenie osobistego hotspotu w swoim smartfonie. Tylko wtedy będziesz miał pewność, że połączenie internetowe jest bezpieczne. Jeśli natomiast nie jest to możliwe, a musisz połączyć się z publiczną siecią Wi-Fi (np. na lotnisku, w hotelu lub kawiarni), skorzystaj z wirtualnej sieci prywatnej, często nazywanej VPN (ang. Virtual Private Network). Jest to oprogramowanie instalowane na laptopie lub urządzeniach przenośnych, które pomaga chronić i ukrywać połączenie Wi-Fi. Niektóre rozwiązania VPN zawierają ustawienia umożliwiające automatyczne włączenie sieci VPN podczas łączenia się z niezaufanymi sieciami Wi-Fi.

- **Publiczne komputery**: Stanowczo unikaj korzystania z publicznych komputerów, takich jak te w hotelowych lobby lub w kawiarniach, do logowania się na jakiekolwiek konta lub uzyskiwania dostępu do poufnych informacji. Nie wiesz, kto korzystał z tego komputera przed Tobą i czy przypadkiem nie zainfekował go szkodliwym oprogramowaniem, takim jak rejestrator naciśnięć klawiszy. Korzystaj tylko z tych urządzeń do których masz zaufanie i pewność.

- **Media społecznościowe**: Mamy skłonność do informowania wszystkich o naszych podróżach i przygodach za pośrednictwem mediów społecznościowych, ale nie zawsze wiemy do kogo finalnie trafi ta informacja. W miarę możliwości staraj się unikać nadmiernego dzielenia swoimi zdjęciami podczas wyjazdu i zastanów się, czy nie poczekać z tym do powrotu. Pamiętaj również że wrzucone zdjęcia karty pokładowej, prawa jazdy, paszportu czy karty płatniczej są łakomym kąskiem dla złodziei. Nie rób tego nigdy.

- **Praca**: Jeśli będziesz pracować podczas urlopu (co stanowczo odradzamy!), sprawdź z wyprzedzeniem, jakie są zasady dotyczące podróży służbowych. Upewnij się jakie urządzenia i dane możesz zabrać ze sobą oraz w jaki sposób bezpiecznie łączyć się zdalnie z siecią służbową.

Okres świąteczny powinien być czasem, który wspólnie spędzimy w gronie rodzinnym. Pamiętaj jednak o czyhających niebezpieczeństwach, które opisaliśmy w tym wydaniu biuletynu bezpieczeństwa komputerowego.

## Redaktor gościnny

Princess Young jest starszym analitykiem w Southwest Airlines i kieruje działaniami edukacyjnymi i szkoleniowymi w zakresie bezpieczeństwa cybernetycznego dla 60 tys. pracowników w całym kraju. Princess lubi współpracować z pracownikami w sposób dający im współodpowiedzialności za bezpieczeństwo cybernetyczne, niezależnie od ich roli czy stanowiska.

## Źródła

**Bezpieczeństwo urządzeń mobilnych:** https://www.sans.org/newsletters/ouch/securing-mobile-devices/
**Moc aktualizacji:** https://www.sans.org/newsletters/ouch/the-power-of-updating/
**Wirtualne Sieci Prywatne (VPN):** https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
**Czy robisz kopie zapasowe:** https://www.sans.org/newsletters/ouch/got-backups/

**Polski przekład CERT Polska:** Bartłomiej Wnuk, Aleksandra Węgrzynowicz