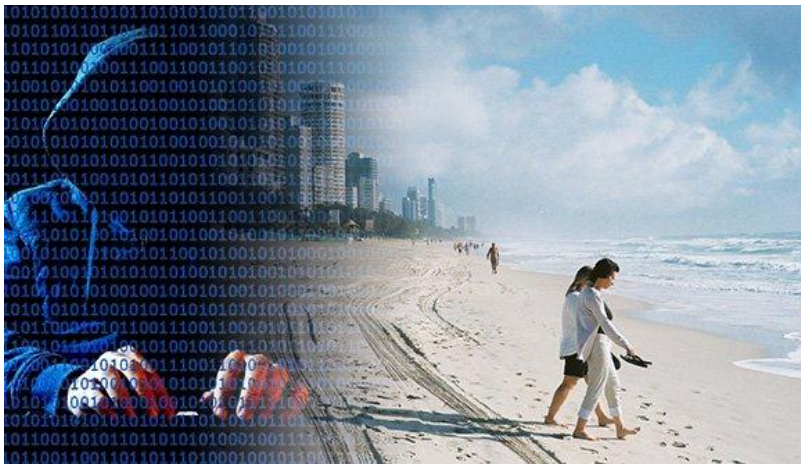
kpt. Grzegorz Data
OISW Rzeszów

Cyber(i nie tylko)bezpieczeństwo na wakacje



Sezon urlopowy w pełni, w tym czasie warto pamiętać o kilku zasadach, które pozwolą cieszyć się wolnym czasem nie przejmując się problemami związanymi ze sferą informatyczną. Oto kilka rad, które przydadzą się nie tylko w okresie wakacyjnym, ale również w codziennym korzystaniu z dobrodziejstw sprzętu komputerowego i sieci Internet.

SIECI WIFI

Udając się na wymarzone wakacje najczęściej nie chcemy tracić kontaktu z naszymi miejscami w sieci. Wiedzą o tym organizatorzy wypoczynku oferując darmowy dostęp do Internetu poprzez sieci WIFI. Niestety wiedzą również o tym przestępcy, dlatego:

- Jeśli to tylko możliwe, unikaj publicznych sieci WiFi, gdyż mogą być to sieci „podstawione" przez cyberprzestępców;
- Laptop, tablet lub też telefon podłączony do fałszywej sieci może zostać zainfekowany złośliwym oprogramowaniem wykradającym dane lub szyfrującym zawartość dysków lub – częściej – mogą zostać podsłuchane Twoje hasła i loginy uwierzytelniające w serwisach społecznościowych, aukcyjnych, poczcie elektronicznej lub banku;

- Jeżeli nie posiadasz innego dostępu do Internetu poza siecią np. hotelową ogranicz do minimum korzystanie z usług, do których trzeba się zalogować;
- Najbezpieczniejsze jest używanie Internetu poprzez sieć komórkową.

TELEFONY i TABLETY

Korzystając z urządzeń mobilnych pamiętaj:

- Używaj oprogramowania antywirusowego;
- Zabezpiecz telefon kodem PIN lub odciskiem palca;
- Wykonaj kopię wszystkich danych przechowywanych w telefonie;
- Usuń dane niepotrzebne lub takie, które mogłyby Cię skompromitować w przypadku kradzieży lub zagubienia telefonu;
- Używaj funkcji monitorujących położenie Twojego telefonu, dzięki temu będziesz mógł go odleźć lub zablokować w przypadku kradzieży lub zagubienia:
  ANDROID: Wejdź na android.com/find i zaloguj się na konto Google – możesz odnaleźć położenie swojego telefonu, odtworzyć dźwięk, zablokować lub wykasować na nim dane;
  APPLE: Zaloguj się na stronie icloud.com/find na komputerze. Będziesz mógł zobaczyć położenie telefonu na mapie a także zablokować go kodem PIN włączając tryb „Utracony”;
  MICROSOFT: Przejdź na stronę account.microsoft.com/devices. Jeśli zostanie wyświetlony monit o zalogowanie się, użyj tego samego konta Microsoft, które zostało użyte do zalogowania się na telefonie. Wybierz telefon, który chcesz znaleźć, a następnie kliknij pozycję Znajdź mój telefon. Istnieje także możliwość zadzwonienia na telefon bądź zablokowania hasłem a także wymazania;
- Instaluj aplikacje z zaufanych źródeł, sklepu Gogle Play lub oficjalnego sklepu Apple, instalując zweryfikuj ustawienia prywatności, o które będzie pytać podczas instalacji – czy np. aplikacja musi mieć dostęp do listy Twoich znajomych z informacjami kontaktowymi;
- Przy sprzedaży lub oddaniu telefonu usuń wszystkie dane poprzez opcje: APPLE : Ustawienia/Ogólne/Wyzeruj/Wymaż zawartość i ustawienia ANDROID: Ustawienia/Kopie i kasowanie danych/Ustawienia Fabryczne

Pamiętaj, iż dane na kartach pamięci SD nie zostaną usunięte. Kontakty także mogą pozostać na karcie SIM jeśli jej nie usuniesz

ZAKUPY

Wakacje to także czas zwiększonych zakupów online. Obok czasu świątecznego, wakacje to czas zwiększonej fali oszustw dokonywanych przy zakupach internetowych. Pamiętaj:

- Sprawdź czy podany na stronie adres i istnieje a numer telefonu odpowiada, porozmawiaj z kimś ze sprzedaży lub wsparcia;
- Zwróć uwagę na błędy gramatyczne lub ortograficzne na witrynie;
- Wpisz w wyszukiwarce nazwę sklepu i sprawdź opinie, nie kieruj się opiniami na stronie sklepu – mogą być fałszywe. Brak opinii to też informacja - strona może być nowa. Opinie sprzedawca może sobie zamówić w specjalizowanych serwisach. A może najpierw warto kupić jakieś drobne akcesoria by sprawdzić wiarygodność sklepu;
- Zachowaj ostrożność jeżeli witryna przypomina wyglądem stronę internetową innego sklepu lub dostawcy, a jej adres niewiele różni się od adresu znanej firmy jedynie jedną literą znakiem lub wyrażeniem (np. NNN-24.pl). jeśli masz jakieś wątpliwości poszukaj innej oferty;
- Uważaj na podejrzanie niskie ceny, marże sklepów nie są aż tak wysokie by sprzedawać towar za połowę wartości;
- Samych zakupów dokonuj z domu lub sprawdzonej sieci. Pamiętaj, iż przestępcy mogą przejąć twoją sesję płatności kartą lub przelewem;
- Przy płatności kartą kredytową sprawdzaj cyklicznie wyciągi, jeśli bank posiada usługę powiadamiania o płatnościach SMS – włącz ją, przy podejrzanej płatności zawsze będziesz mógł ją wstrzymać lub reklamować. Dobrą praktyką jest posiadanie osobnej karty tylko do płatności online. Ustal dzienne limity na transakcje;
- Rozważ płacenie za zakupy za pomocą serwisów PayPal lub PayU. – są znacznie bezpieczniejsze;
- Przyglądaj się bankomatowi, z którego korzystasz wypłacając pieniądze. Sprawdź czy nie ma ruchomych lub odklejających się nakładek przy otworze na kartę lub klawiaturze. Bankomat celowo wysuwa kartę ze zmienną prędkością tak aby utrudnić odczytanie danych z paska magnetycznego. Podczas każdej wypłaty warto zasłonić się ręką lub portfelem. Zmniejszasz w ten sposób ryzyko, że ktoś podejrzy twój kod. Śledź też transakcje, które pojawiają się w historii rachunku. Jeśli zauważymy operację, której nie wykonaliśmy, powinniśmy zastrzec kartę i zareklamować operację w banku. Korzystaj z bankomatów w miejscach uczęszczanych, tego typu miejsca są rzadziej odwiedzane przez przestępców, którzy nie chcą być przyłapani na instalowaniu nakładek.

RANSOMWARE

Ostatnimi czasy coraz częściej słychać o złośliwych programach szyfrujących dyski w komputerach lub zawartość telefonów. Aby zminimalizować ryzyko takiego zdarzenia, należy pamiętać o kilku zasadach:

- Rób kopie bezpieczeństwa Twoich ważnych danych. W razie zaszyfrowania po prostu je łatwo odzyskasz;
- Nie klikaj w linki i nie uruchamiaj załączników, które otrzymałeś w wiadomościach mailowych od nieznanych osób;
- Aktualizuj system operacyjny oraz aplikacje. Im bardziej oprogramowanie jest aktualne, tym trudniej jest przestępcy zainfekować je. Najlepiej jest włączyć automatyczne aktualizacje;
- Korzystając na co dzień z komputera nie loguj się z uprawnieniami użytkownika mającego prawa administratora – dużo trudniej jest wtedy zainfekować komputer i zaszyfrować wszystkie dane na nim przechowywane;
- Zainstaluj i aktualizuj oprogramowanie antywirusowe;
- Nie płać okupu. Nie masz gwarancji, że odzyskasz swoje dane (wg. badań odzyskuje je mniej niż 20%);
- Jeżeli już Twoje pliki zostały zaszyfrowane i nie posiadasz ich kopii nie kasuj ich, najczęściej po jakimś czasie ukazują się narzędzia, które odszyfrowują te dane. Najłatwiej odnajdziesz je szukając rozszerzenia zaszyfrowanego pliku, bądź treści komunikatu informującego o zaszyfrowaniu.

OCHRONA TOŻSAMOSCI

Aby po urlopie do Twoich drzwi nie zapukała firma windykacyjna z informacją, iż zalegasz za raty kredytu, którego nie brałeś, zapoznaj się z kilkoma poradami:

- Nigdy nie dawaj dowodu osobistego, bądź innego dokumentu potwierdzającego Twoją tożsamość w zastaw. Przetrzymywanie cudzego dowodu osobistego jest wykroczeniem;

- Okazuj dowód osobisty tylko osobom uprawnionym – funkcjonariuszom służb, strażnikom miejskim, a także w sklepie w celu udowodnienia posiadania 18 lat albo dla potwierdzenia tożsamości przy weryfikacji karty płatniczej;
- Nie zgadzaj się na kopiowanie dowodu osobistego – jeśli nawet musisz przedstawić na żądanie w celu np. wynajęcia apartamentu, nie oznacza to, że można wykonać jego kserokopię;
- Jeśli przekazujesz skan dowodu osobistego zawsze zamieść na nim adnotację dotyczącą celu sporządzenia skanu. Dzięki temu będzie można go używać tylko w tym jednym konkretnym celu;
- Nie podawaj danych z dowodu osobistego osobom trzecim;
- W przypadku zgubienia lub kradzieży bezzwłocznie zastrzeż dokument tożsamości. Możesz to zrobić w dowolnym banku należącym do systemu "Dokumenty Zastrzeżone", telefonicznie lub online poprzez Biuro Informacji Kredytowej - jeśli ma się tam założone konto. Pamiętaj, że zgłoszenie zagubienia lub kradzieży dokumentu na posterunku policji nie jest równoznaczne z zastrzeżeniem go (funkcjonariusze Policji nie mają możliwości zastrzegania dokumentu);
- Na publikowanie zdjęć znajomych i bliskich w portalach społecznościach powinieneś mieć ich zgodę – szczególną rozwagę miej przy publikowaniu zdjęć dzieci. Pamiętaj, że zdjęcia mogą być udostępniane dalej i wizerunek może zostać podany w negatywnym kontekście, zdjęcia można zmodyfikować i udostępnić w postaci memów, a w skrajnych przypadkach ukraść tożsamość a zdjęcia dzieci mogą stać się przedmiotem zainteresowania pedofilów.
- Nie zamieszczaj w Internecie informacji kiedy i gdzie wyjeżdżasz – to zaproszenie dla złodzieja.