Warszawa, 27.06.2019 r.

Informacja prasowa

**Płacisz telefonem lub zbliżeniowo? Czy to bezpieczne?**

**W dobie digitalizacji banki otwierają przed nami nowe możliwości. Dzięki temu możemy korzystać z płatności zbliżeniowych kartą lub za pomocą telefonu. Równocześnie podkreślają, że to bezpieczny i wygodny sposób dysponowania swoimi środkami w każdej sytuacji. Ekspert z ODO 24 wskazuje na co warto zwracać uwagę korzystając z płatności za pomocą urządzeń mobilnych by nasze dane osobowe nie wpadły w niepowołane ręce.**

**Jak płacą Polacy**

Wkrótce coraz mniej z nas będzie potrzebować tradycyjnego portfela. W 2018 roku Polacy posiadali 34,7 mln kart z możliwością płatności zbliżeniowej – wynika z danych Narodowego Banku Polskiego. Co więcej, ich liczba w ostatnim kwartale ub.r. stanowiła 84,1% wszystkich kart. Coraz chętniej płacimy również telefonem**.** Pod koniec marca 2019 roku dodaliśmy ponad 2,1 mln kart płatniczych do swoich urządzeń mobilnych, dzięki czemu mogą płacić np. telefonem (dane udostępnione przez portal cashless.pl).

Banki zauważając tendencję wzrostową odnośnie zainteresowania systemami mobilnymi wychodzą naprzeciw swoim użytkownikom wprowadzając coraz to nowsze możliwości płatności. *Sposobów dokonywania transakcji obecnie jest kilka. Pierwszą z nich jest skorzystanie z aplikacji banku, która jest połączona z odpowiednią usługą na naszym telefonie, np. Apple Pay, Google Pay czy HCE. Źródłem pieniędzy jest oczywiście karta bankowa skojarzona z aplikacją mobilną. Transakcja odbywa się na zasadzie standardowej płatności zbliżeniowej, gdzie telefon zastępuje nam kartę płatniczą. Kolejną opcją jest coraz popularniejszy BLIK. Zastępuje on zupełnie użycie karty płatniczej. Transakcji dokonuje się za pomocą kodu wyświetlanego w aplikacji. Dzięki niemu możemy realizować np. wypłaty z bankomatów, płatności w sklepach stacjonarnych, przelewy na numer telefonu (wybrane banki) –* wskazuje Barbara Matasek, specjalista ds. ochrony danych, ODO 24.

**Nowocześnie i bezpiecznie – jak faktycznie jest?**

Niektórzy nadal boją się, że bez problemu złodziej będzie mógł skopiować kartę zbliżeniową lub uzyskać dostęp do aplikacji na telefonie. Jednak jest to bardziej skomplikowane niż może się wydawać. Warto wiedzieć, że:

1. **Złodziej ma utrudnione zadanie chcąc skorzystać ze standardowego terminala płatniczego.** Żeby mógł on pobrać nasze pieniądze musiałby być podłączony do sieci płatności. Co więcej, konieczne byłoby podpisanie również umowy z firmą, która obsługuje terminale płatnicze. Przez co bez problemu można byłoby go namierzyć. Dla bezpieczeństwa należy jednak nie nosić portfela i telefonu w tylnej kieszeni spodni lub okrycia wierzchniego;
2. **Sklonowanie naszej karty również nie jest idealnym rozwiązaniem dla złodzieja.** Podczas każdej płatności zbliżeniowej generowany jest bowiem jednorazowy kod dCVV. W przypadku sklonowania kartyprzez złodziejabank zablokuje ją podczas próby ponownego wykorzystania wygenerowanego wcześniej kodu. Złodziej „sklonowaną” kartą będzie więc mógł posłużyć się tylko raz i zazwyczaj będą to zakupy na niedużą kwotę (w zależności od limitów w konkretnym banku). Niemniej trzeba jednak być czujnym i przede wszystkim chronić samą kartę przed zgubieniem. Na kartach znajdują się imiona i nazwiska oraz kody CVC2/CVV2. Oszust posiadając te informacje oraz numer karty bez problemu skorzysta z niej podczas płatności internetowej, które nie są zazwyczaj z góry ograniczone przez bank stosunkowo niskimi limitami jednorazowej płatności;
3. **Nasze urządzenia oferują dodatkowe funkcje, które chronią dane osobowe.** Począwszy od PIN-u, przez odcisk palca, kończąc na rozpoznawaniu twarzy. Korzystanie z nich znacząco minimalizuje utratę informacji, co nie jest zapewnione w przypadku dokumentów tradycyjnych;
4. **Dostępne są bardziej zaawansowane funkcje zabezpieczające.** Należy do nich m.in. szyfrowanie całego urządzenia bądź ograniczenie dostępu do poszczególnych aplikacji/folderów, które dodatkowo mogą być chronione osobnym hasłem. Dzięki temu zyskujemy dużą dozę pewności, że przechowywane w folderach dane, w tym dane na temat kart płatniczych, nie trafią w niepowołane ręce w przypadku kradzieży lub zagubienia nośnika.

*Reasumując większość nowoczesnych smartfonów, niezależnie od systemu operacyjnego, można tak skonfigurować, by dzięki aktywowanym na nich zabezpieczeniom, znacząco ograniczony został dostęp do zgromadzonych w nich danych. Samo uruchomienie płatności telefonem podczas zakupów w sklepie możemy również zabezpieczyć, w zależności od dostępnych na naszym urządzeniu opcji. Przykładowo możliwość dokonania płatności może zostać aktywowana dopiero po rozpoznaniu naszej twarzy czy odcisku palca* – podsumowuje Barbara Matasek, specjalista ds. ochrony danych, ODO 24.

Jesteśmy coraz bardziej świadomi niebezpieczeństw – według Raportu o dokumentach InfoDOK przygotowanego przez Związek Banków Polskich w I kwartale 2019 r mieliśmy do czynienia jedynie z 1 117 próbami wyłudzeń kredytów. Jest to jeden z najniższych wyników od początku publikacji raportu, czyli od 2008 roku. Dzięki rosnącej wiedzy i prowadzonym kampaniom edukacyjnym społeczeństwo coraz częściej zdaje sobie sprawę z różnych niebezpieczeństw oraz na co warto zwracać uwagę.

**ODO 24 sp. z o. o.** oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Kontakt dla mediów:

**Triple PR**

**Aneta Gałka**

tel. 570 533 678

aneta.galka@triplepr.pl