Załącznik do Zarządzenia nr 53/2019
Burmistrza Miasta Tuszyna
z dnia 07 lutego 2019 roku

Procedury bezpiecznego użytkowania urządzeń mobilnych

Pracownicy Urzędu Miasta w Tuszynie używający urządzeń mobilnych typu telefon komórkowy – smartphone, laptop itp., są zobowiązani do przestrzegania poniższych zasad.

1. **Nie należy stosować łatwych do odgadnięcia kodów PIN** (np. 0000, 1111, 1234).
2. **Należy stosować blokadę dostępu** do urządzenia mobilnego hasłem lub kodem PIN.
3. **Należy zainstalować** na urządzeniu mobilnym aplikację antywirusową oraz zaporę sieciową,
4. **Należy aktualizować systematycznie system operacyjny** urządzenia mobilnego
5. **Należy być świadomym użytkownikiem Internetu** w urządzeniu mobilnym – nie wchodzić na podejrzane, nieznane strony WWW, nie pobierać żadnych plików ani załączników e-mailowych, których pochodzenia i zawartości nie jest się pewnym, nie pobierać bądź nie instalować aplikacji z nieautoryzowanych źródeł, nie zweryfikowanych pod kątem bezpieczeństwa i ochrony prywatności.
6. **Należy unikać oddawania urządzenia innemu użytkownikowi** – przekazując urządzenie mobilne np. do serwisu należy pamiętać, aby przed tym usunąć ewentualne maile odebrane z konta pocztowego, SMSy otrzymane od Banku, pliki tymczasowe, oraz historię przeglądarki, ponieważ mogą zawierać poufne informacje. Należy wylogować się ze wszystkich aplikacji do obsługi bankowości mobilnej i płatności mobilnych, jeżeli się z takich korzysta.
7. **Nie należy pobierać aplikacji z nieoficjalnych źródeł.** Należy pobierać aplikacje z centralnego, stale monitorowanego źródła, co znacznie zmniejsza ryzyko pobrania i zainstalowania szkodliwego oprogramowania (poza przypadkami, gdy ktoś w jakiś sposób ominie weryfikację przeprowadzaną przez ich operatorów). **Domyślne ustawienie systemów, dopuszczające instalację aplikacji z innych źródeł, powinno zostać wyłączone.**

8. **Należy sprawdzać poziom uprawnień, jakiego żądają aplikacje.** Należy zawsze uważnie przeglądać uprawnienia, o które prosi aplikacja oraz zdecydować, czy zakres wymaganych uprawnień odpowiada teoretycznemu działaniu aplikacji. Wymaganie uprawnień zupełnie nieprzystających do przeznaczenia aplikacji powinno zapalić w głowie użytkownika lampkę alarmową. Należy zrezygnować z zainstalowania takiej aplikacji.

9. **Należy patrzeć, w jakie linki się klika.** Należy bezwzględnie uważać na wiadomości tekstowe zawierające odsyłacze do stron WWW, rozpoczynających pobieranie szkodliwej aplikacji. Najlepiej powstrzymać się od korzystania z odsyłaczy pochodzących z nieznanego lub niezaufanego źródła. Co istotne, warto sprawdzać adres odwiedzanej strony nawet wtedy, gdy odsyłacz pochodzi z zaufanego źródła.

10. **Należy uważać na niezabezpieczone i publiczne sieci bezprzewodowe.** Należy zachować szczególną ostrożność podczas korzystania z niezabezpieczonych i publicznych sieci bezprzewodowych. Każda osoba obserwująca ruch w takiej sieci zobaczy wszystkie nieszyfrowane dane – w tym również nazwy użytkownika i hasła – przesyłane w postaci otwartego tekstu. Należy korzystać wyłącznie z serwisów i usług szyfrujących ruch z wykorzystaniem protokołu HTTPS. Protokół ten powoduje szyfrowanie wszystkich danych przesyłanych między smartfonem a miejscem docelowym, w związku z czym osoba podglądająca sieć nie zdoła ich odczytać.

11. **Należy blokować niechciane reklamy. Należy zainstalować oprogramowanie blokujące wyświetlanie reklam, na przykład AdBlocka.** Oprogramowanie to blokuje cały ruch związany z reklamami, chroniąc w ten sposób wrażliwe dane użytkownika.

12. **Należy pamiętać o wylogowaniu się z serwisów WWW.** Trzeba zawsze wylogowywać się z serwisu WWW po zakończeniu korzystania z niego. Spowoduje to usunięcie danych logowania (przechowywanych np. w postaci plików cookie), zmniejszając podatność użytkownika na ataki tego rodzaju.

13. **Należy zainstalować antywirusa.** Przed pobraniem mobilnego antywirusa należy upewnić się (np. czytając fora internetowe lub opinie o produkcie), czy nie jest on aby złośliwym robakiem wyłudzającym od nas pieniądze w zamian za możliwość odblokowania niezbędnych nam usług (które sam uprzednio zablokował).

14. **Należy mieć świadomość ataków przeprowadzanych przez porty USB.** Nawet jeśli chce się tylko naładować baterię, można paść ofiarą cyberataku. Dobrym i niedrogim sposobem zabezpieczenia się przed tym zagrożeniem jest korzystanie z „prezerwatyw USB" (ang. *USB Condoms*, http://www.usbcondoms.com/), które zapobiegają odczytywaniu danych z

telefonu i zapisywaniu ich na nim. Rozwiązanie to gwarantuje, że połączenie USB zostanie użyte wyłącznie w celu naładowania baterii.

15. **Należy aktualizować system operacyjny** - poza usprawnieniem działania i uzyskaniem dostępu do nowych funkcji użytkownik zwiększa w ten sposób również poziom bezpieczeństwa swojego smartfona.
16. **Należy blokować ekran.** Należy ustawić choćby najbardziej podstawową blokadę ekranu w ustawieniach systemowych (np. odblokowanie tylko nam znanym gestem ekranowym).

BURMISTRZ
Małecki
mgr inż. Witold Małecki