Препоръки за сигурност за приложението за мобилно банкиране „Fibank”

- Мобилното банкиране на – Fibank (Първа инвестиционна банка) може да изтеглите от специализираните мобилни приложения за смарт устройства – телефони, таблети и др. Приложенията са достъпни за операционните системи Android и iOS;
- Fibank разпространява приложенията за смарт устройствата само чрез официалните маркети. Използвайте за инсталиране на приложенията Google Play (за Android) и iTunes (за iOS). Бутони за дотъп до Google Play и iTunes са достъпни и на уебсайтовете на Fibank и Виртуален банков клон на адреси www.fibank.bg и https://e-fibank.bg;

За паролата:

- Достъпът до мобилното приложение “Fibank” се извършва с персоналното потребителско име и паролата, които ползвате и за стандартното интернет банкиране (e-fibank или my-fibank). За допълнителна сигурност приложението не запаметява Вашата парола за достъп;
- Запомнете Вашата парола или ПИНт код и не ги записвайте в паметта на мобилния телефон, компютъра или на хартиен носител;
- Сменяйте периодично Вашата парола/ПИНт код за достъп;
- От съображения за сигурност не използвайте за парола някое от следните: име и рождена дата; поредица от числа/букви в ред (12345,abcd и други), повторение на знаци като ааа111;
- Използвайте т.н. „силна” парола, която да съдържа комбинация от главни, малки букви и цифри и да бъде поне с 8 символа;
- Не предоставяйте Вашето потребителско име, пароли и ПИНт код на други лица, включително и на членове на семейството;
- Не използвайте една и съща парола за достъп/ПИНт до различни акаунти за интернет банкиране, имейли и други;
- Всеки път след приключване на работа с мобилното приложение „Fibank” излизайте през менюто „Изход от профила” и затваряйте приложението;

За работа със смарт устройството:

- Обмислете поставянето на допълнителна защита на смарт устройството като: парола за отключване, разпознаване на лицеви черти, пръстов отпечатък, жестове и други в зависимост от модела и функционалностите на мобилното устройство. По този начин ще увеличите сигурността си при физическа кражба на устройството;
- Не предоставяйте мобилното устройство на трети лица;
- При загуба/кражба на мобилното устройство се свържете с банката за блокиране на регистрацията Ви за мобилното приложение;
- При съмнение за хакерска атака и кражба на лични данни, включително пароли/ПИНт, потребителско име уведомете своевременно банката ;
- Fibank Ви уверява, че не изисква от своите клиенти кодове за достъп до услуги, пароли, номера на банкови карти или друга конфиденциална информация чрез електронна поща;
- Инсталирайте антивирусен софтуер предоставен от надеждни производители на антивирусни програми и използвайте официалните маркети за инсталирането му;

- Не инсталирайте и не използвайте софтуер/приложения със съмнителен произход;
- Винаги актуализирайте операционната система на смарт устройството до последната възможна. Чрез тези актуализации производителите отстраняват откритите уязвимости в по-ранните версии на системата. Изпълнявайте стриктно инструкциите на производителя;
- Не банкирайте активно от смарт устройства, които са с права на супер потребител (т.нар root) или с разширени права (т.нар jailbreak). Получаването на администраторски права предоставя възможност от злонамерени лица да получат пълен и неоторизиран достъп до цялото Ви устройство;
- Деактивирайте регистрацията на мобилното приложение от всички устройства, от които вече не работите. Ако има мобилни смарт устройства, на които сте инсталирали предишни версии на мобилното приложение и вече не работите с тях поради преинсталация на приложението или друга причина , деактивирайте тези устройства по един от определените от банката начини.

Функции на приложението, в полза на сигурността:

- През меню „Настройки", „Времетраене на сесията" променяйте периода на продължителност на работата Ви в приложението в зависимост от справките/операциите, които ще желаете да осъществите. Не поставяйте неоснователно голямо времетраене;
- Използвайте меню „Настройки", „Политика на потвърждаване" и определете настройката с най-висока степен на сигурност. Fibank препоръчва използването на Токън устройство за извършване на всички видове операции, дори и на тези, за които не се изисква потвърждение с Токън устройство.
- От съображение за сигурност, за извършване на активни банкови операции през мобилното приложение „Fibank", е необходимо да регистрирате своето смарт устройство, както и всяко ново смарт устройство по определените от банката начини.