



## КАК ЗАЩИТИТЬ МОБИЛЬНОЕ УСТРОЙСТВО

- использовать ПИН-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.);
- современно обновлять операционную систему устройства, антивирус;
- устанавливать приложения из PlayMarket, AppStore или только из проверенных источников;
- обращать внимание, к каким функциям гаджета запрашивает доступ приложение;
- включить встроенные функции устройства для определения его местонахождения;
- в случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы;
- при смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру;
- перед продажей устройства произвести его сброс до заводских настроек.

Источник: МВД Беларуси.

## РАЗНОВИДНОСТЬ КИБЕРПРЕСТУПЛЕНИЙ - КРАЖА ДЕНЕГ АБОНЕНТОВ СОТОВОЙ СВЯЗИ ЧЕРЕЗ МОБИЛЬНЫЙ БАНКИНГ.

- Злоумышленники идут жертве в общественных местах или обращаются к знакомым и просят телефон, чтобы сделать звонок.
- Делая вид, что набирает номер, при помощи USSD-запроса или выхода в интернет преступник активирует услугу мобильного банкинга. С ее помощью можно совершить платежные операции с лицевого счета абонента и получить у оператора сотовой связи лимитированный микрозайм.
- Сумма, поступившая хозяину гаджета, и средства с баланса телефона переводятся на абонентские номера или банковские счета злоумышленника.

## ЧЕГО ДЕЛАТЬ НЕЛЬЗЯ

- передавать незнакомым мобильный телефон или сим-карту, а в случае передачи - контролировать все действия, которые производятся с устройством;
- устанавливать приложения с низким рейтингом и отрицательными отзывами;
- перезванивать на неизвестные иностранные номера;
- хранить важную информацию на мобильном устройстве;
- делать полное снятие ограничений на устройстве.

© Инфографика **BEETA**