

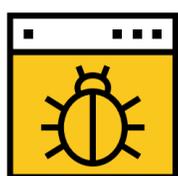


ВРЕДОНОСНОЕ ПО ДЛЯ
МОБИЛЬНОГО БАНКИНГА

ВРЕДОНОСНОЕ ПО МОЖЕТ ДОРОВОГО ВАМ ОБОЙТИСЬ

Вредоносное ПО для мобильного банкинга предназначено для хищения финансовой информации, хранящейся в вашем мобильном устройстве.

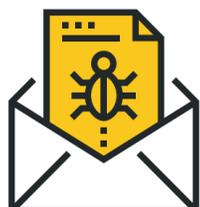
КАК ОНО РАСПРОСТРАНЯЕТСЯ?



При посещении вредоносных веб-сайтов



При загрузке вредоносных приложений



Посредством фишинга



КАКИЕ РИСКИ?



Сбор информации, удостоверяющей вашу личность



Несанкционированное снятие денег

ЧТО С ЭТИМ ДЕЛАТЬ?



<https://>

Загрузите официальное мобильное приложение вашего банка и каждый раз проверяйте, действительно, ли вы находитесь на настоящем сайте банка.



Избегайте автоматического входа в учётную запись на банковском сайте или в приложении.



Никому не передавайте и не разглашайте номер вашей банковской карты и пароль.



Если есть возможность, установите приложение мобильной безопасности, которое будет уведомлять вас о любой подозрительной активности.



Если вы потеряли свой мобильный телефон или сменили номер, свяжитесь со своим банком для обновления информации.



Не передавайте информацию о вашем счёте текстовыми сообщениями или электронной почтой.



При подключении к мобильной версии сайта или приложению своего банка всегда пользуйтесь защищённой сетью Wi-Fi. Никогда не делайте этого посредством открытой сети Wi-Fi!



Периодически проверяйте свои финансовые выписки.