# Банковские троянцы

**Банковские троянцы** – специализированные программы, созданные для похищения личных данных пользователей. В особенности они заточены на воровство логинов и паролей пользователей интернет-банкинга. Троянцы также могут перехватывать SMS с секретными кодами, которые присылает банк, и перенаправлять их злоумышленникам. Кроме того, они способны также непосредственно воровать деньги со счета – все сразу или постепенно небольшими переводами.

**Наиболее вероятные пути заражения.** Путь заражения компьютера пользователя троянской программой, как правило, происходит одинаково: она маскируется под безобидные, а часто и очень известные приложения. Самыми распространенными вариантами являются загрузка обновления программы не с официального сайта разработчика, а со стороннего ресурса, который имитирует оригинальный. Пользователь скачивает, казалось бы, известную программу, а внутри нее прикреплен троян, который заражает ПК. Кроме того, троянцев могут загружать на ПК другие трояны и вредоносное ПО, которым заражен компьютер. Не менее актуальным способом распространения банковских троянцев можно назвать СПАМ-рассылку. Этот метод усиливается технологиями социальной инженерии, которые строятся на психологии поведения и заставляют пользователя открыть прикрепленный документ или перейти по ссылке на зараженный сайт.

Банковские троянцы являются причиной 80% случаев кражи денег с банковских счетов. Банковские троянцы – довольно опасный хакерский инструмент. В «умелых» руках он может нанести ощутимый ущерб финансам жертв.

**Лучшей защитой от троянских программ, является осмотрительность.** Зная и используя несколько базовых правил кибербезопасности, можно свести к минимуму вероятность заражения:

1. Не открывайте письма от неизвестных адресатов с вложенными архивами и текстовыми документами.
2. Если открыли такое письмо, не открывайте файлы.
3. Удалите такое письмо.
4. Не используйте установочные файлы известных программ из сторонних источников.
5. Пользуйтесь антивирусом, как на ПК, так и на мобильном устройстве.
6. Регулярно делайте копии важной информации.
7. Реквизиты банковской карты должны запрашиваться при каждой повторной покупке в интернет-магазине. В противном случае, необходимо обратиться к менеджеру банка.
8. Помните: для входа в интернет-банкинг НЕ требуется ввод PIN-кода вашей карты.