1.1 Масштаб происшествий

Мошенники за год, через интернет-банки украли со счетов россиян 99 млн руб. Об этом говорится в докладе компании Group-IB, занимающейся предотвращением и расследованием мошенничества с использованием высоких технологий.

В общей сложности, за один день мошенники похищали у россиян 398 тыс. руб. За год количество ежедневных хищений средств у физлиц выросло в три раза. Как это отразилось на объемах похищенных средств, компания не указывает.

Но основной целью хакеров остаются по-прежнему юридические лица. За год у них похищено 1,9 млрд руб. Еще 638 млн руб. киберпреступники похитили через целевые атаки на банки. Всего объем хищений денежных средств в российском сегменте интернет-банкинга за год составил более 2,6 млрд руб. — это в 3,7 раза меньше, чем годом ранее.

* 1. Как происходит преступление

Прежде всего, преступникам нужен номер карты и данные для аутентификации (Номер карты, пароль и номер телефона от банковского аккаунта, CVV1/CVV@ и т.п.). Часто мошенники покупают базу данных в “Даркнете” (Тёмный интернет, закрытая сеть, автоматически скрывающая ваше местоположение) и проверяют актуальность информации в ней или же подбирают пароли с помощью брутфорса (Математический подбор пароля) или других методов.

В даркнете **купить данные карты можно за 300-500 рублей**. Кроме того, кардеры оплачивают VPN с возможностью выбора сервера (желательно с точностью до штата или хотя бы до страны) и другие средства анонимизации.

После удачного “получения” данных банковских карт, преступник покупает ликвидные для продажи вещи, в иностранных интернет магазинах, на иностранный адрес. При получении товара, мошенник через сторонних людей продаёт вещи с огромной скидкой

Другой вариант – организация фишинговой кампании. Копируется страница банка с формой для входа в аккаунт или создаётся фальшивое приложение, с помощью спама распространяется ссылка на него.

Пользователь, обеспокоенный тем, что его карту могут заблокировать; банк просит подтвердить операцию; поступил перевод неизвестно от кого – идёт на фальшивый сайт или запускает поддельное приложение. Кардер забирает введённые данные и переводит все деньги себе. Или ждёт больших поступлений, чтобы выгрести по максимуму.

1.2 Метод борьбы органов власти

Отслеживание сомнительных операций, корпоративная академия, где готовы обучать конкурентов, продвижение идеи международного обмена информацией – действия, которые предпринимает государство в противостоянии с киберпреступностью.  Также спецслужба ФСБ, проводит слежку, обыски и поимку мошенников на территории РФ.

1.3 Личная безопасность

Самые главные меры для своей безопасности.

1) Всегда проверяйте сайты на предмет их достоверности. Это несложно - главное использовать современные браузеры со специальными системами защиты личных данных, а также автоматически сверяющиеся с сертификатами подлинности сайтов.

2) Не стоит хранить реквизиты карты на компьютере или пересылать их с помощью мессенджеров или электронной почты. Не отдавайте карту сторонним лицам, даже официантам и кассирам. Не пополняйте и не снимайте деньги в уличных банкоматах, в них могут находиться скрытые камеры и накладные клавиатуры, запоминающие отпечатки.

3) Не отвечайте на сомнительные письма, и уж тем более не переходите по содержащихся в них ссылкам. Ни один серьёзный банк не будет отправлять такие сообщения своим клиентам.

Ни в коем случае не вводите данные карт на сайтах с сомнительной репутацией.

1.4 Вывод

**Несмотря на все ухищрени кибермошенников, обезопасить себя и близких от их деятельности довольно просто - достаточно быть более внимательным. С каждым днём мошенники придумывают новые способы взлома данных, но и органы по борьбе с этим тоже не дремлют.**