

Всегда следует придерживаться главных правил:

1. Не записывайте пин-код на карте или в легко-доступных местах.

Почти 90% хищений денежных средств с пластиковых банковских карт – по причине халатного отношения к сохранению тайны пин-кода.

На магнитной полосе пин-код не записан в зашифрованном виде. Если у вас пропали деньги с карты и банк заявляет, что снятие было с использованием кода – сразу вспоминайте, кто мог видеть ваш пин-код, или, где вы могли его записать, кому-то сообщить.

Если операция проводилась с вводом пин-кода (банк это видит в отчётах) и в банкомате отсутствует система видеонаблюдения, у вас практически нет шансов вернуть ваши деньги.

По правилам платёжных систем, такие операции нельзя опротестовать. Банк имеет полное право отказать в рассмотрении жалобы о краже денег, и будет совершенно прав.

Поэтому, запоминайте пин-код или записывайте его так, чтобы никто не понял, что это он. Например, пин-коды можно хранить в качестве мобильных номеров вымышленных людей, зная, что пин – это первые четыре цифры номера Иванова И.И. и т.д.

2. Не передавайте никому реквизиты своей карты. Если конкретнее – номер карты, срок действия, имя и фамилия. По большому счёту, этого может быть достаточно для снятия денег с карты, даже без её физического

присутствия. Не надо оставлять её на столе, т.к. даже за 10 секунд можно сфотографировать карту с двух сторон, чего будет достаточно, для снятия с них денежных средств.

3. Если расплачиваетесь карточкой в магазине, ресторане, гостинице и т.д., не допускайте, чтобы карточка пропадала из виду. Например, официант может сказать, что терминал находится там-то и ему нужно отойти, чтобы прокатать вашу карту. В этом случае вы имеете полное право требовать, чтобы он взял вас с собой. Никто ведь не знает, что он там собрался с ней делать. При помощи нехитрого технического устройства можно запросто сделать клон вашей карты и попытаться ей расплачиваться в торговых сетях.

4. Никто не должен знать баланс вашей карты.

Проверка баланса где-либо – это самая рискованная электронная операция по карте. Мошенники охотятся за балансами карт, а не за самими картами. Никогда не выбрасывайте балансовые чеки, не рассказывайте направо и налево, что у вас там куча денег и т.п.

5. Заведите себе отдельную карту для банкоматов и кладите на нее только нужную сумму.

Не вздумайте копить деньги на карте, которую вы каждый день носите с собой. Откройте для этих целей любую карту уровня VisaElectron, MasterCardElectronic, CirrusMaestro. Эти карты открываются бесплатно либо за символическую плату. Обслуживание, как правило, тоже стоит копейки. При этом, желательно подобрать банк с бесплатным

интернет — банкингом. Тогда будет удобно переводить деньги с накопительной карты на зарплатную.

6. Будьте предельно осторожны с кредитными (на которых есть кредитный лимит) карточками.

Не используйте их в «сомнительных» местах. Проблема в том, что при потере денег с карты, вы теряете деньги банка. Как следствие – на вас будет висеть долг, да ещё под проценты.

7. Держите в своем мобильном телефоне номер сервисного центра банка, где выдали Вам карточку.

Этот номер записан на самой карте. И мы привыкли искать его именно там. Однако если карту похитили – начинаются беспорядочные метания в поисках нужного телефона. **Вывод:** карту украли – сразу звоним в банк и блокируем.

Безопасность в Интернете.

Чтобы сразу понять всю логику, вот вступительный ликбез: для того, чтобы снять деньги с вашей карты в Интернете, необходимо знать: номер карты, срок годности, имя, фамилию владельца, CVV код (эти 3 цифры можно увидеть на обратной стороне карты справа от полосы для подписи).

Немного о самом CVV коде. Этот код является неким аналогом пин-кода, который предназначен исключительно для Интернета. Берегите эти цифры, т.к. это онлайн-ключ к вашей карте.

Советы:

1. Самый первый принцип – не оставляйте реквизиты своей карты на малознакомых сайтах (да и вообще, никуда их не пишите,

если Вас об этом не просят). Наиболее яркие элементы, которые должны вызывать подозрение:

- когда сайт сделан не качественно;
- весь сайт наполнен рекламой, всплывающими окнами;
- форма для реквизитов карточки находится на незащищённой странице (адрес защищённой страницы должен обязательно начинаться на <https://>).

2. Выберите себе несколько сайтов, которыми Вы будете пользоваться всё время. Не нужно посещать множество сайтов, пытаясь найти ту или иную услугу/товар на пару рублей дешевле. Лучше не рисковать.

3. Хороший вариант, когда для ввода реквизитов карты, Вас перебрасывают на сайт биллинговой системы, а не просят вбивать реквизиты карты прямо на сайте. Вы ведь не знаете, куда потом сайт отправляет ваши данные и насколько хорошо там отлажена система безопасности. По крайней мере, на сайте биллинговой системы вбивать реквизиты несколько безопасней.

4. Заведите для онлайн операций отдельную карту.

P.s: Помните, то за преступления с использованием похищенных банковских платежных карточек предусмотрена ответственность, установленная ст. 212 УК Республики Беларусь, которая предусматривает наказание вплоть до лишения свободы на срок от 3 до 15 лет.



1). Злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты. При этом хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу», очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона либо пытаются похитить со счета деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы. Практически во всех случаях

хищения денежных средств со счетов мобильных телефонов потерпевшие сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон.

2). Злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям.

В случае обнаружения «взлома» аккаунта, прежде всего следует попытаться восстановить доступ наиболее привычным

способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого, следует оповестить друзей и знакомых об инциденте,

используя иные социальные сети и мессенджеры.

Также, чтобы в какой-то мере обезопасить себя от взлома, специалисты рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты. Помимо этого, в

настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа». При этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который автоматически будет выслан на указанный при регистрации страницы номер.

Кроме этого, следует помнить, что если реквизиты карты сохранены в смартфоне или каком-либо аккаунте, то в случае установки платного приложения с изначально бесплатным пробным периодом, после истечения указанного периода, платная подписка продлится автоматически и денежные средства спишутся со счета.

