К сожалению, со временем появились и многочисленные способы мошенничества с картами. Как выясняется, даже простое снятие наличных денег в банкомате может закончиться плачевно. Поэтому лучше предвидеть возможные уловки аферистов и противостоять им, чем в один прекрасный день расстаться со своими деньгами. Угроза эта реальна, и только от вас и вашего отношения к банковской карте зависит, воплотится ли эта угроза в жизнь. Карточные воры в своей среде называют друг друга кардерами, а своих жертв холдерами (от англ. cardholder- владелец карты). Существует несколько основных способов хищения денег. Самый распространённый-подделка, когда полученная незаконным путём информация в чужой карте эмбассируется (наносится) на пластик (белый пластик) или записывается на магнитную полосу подделки или подлинной карты.

Устройство для перехвата информации с магнитной ленты пластиковых карт называется скиммер. Слово скиммер происходит от английского «skim»-снимать.

В данном случае речь идёт о снятии (сливок) с вашего банковского счёта. Скиммер-это накладка на банкомат, которая принимает вашу карточку и считывает с неё данные.

На втором месте хищения, ставшие возможными по причине кражи-утери владельцами пластиковых карт с их незамедлительным последующим использованием похитителями. Поэтому при обнаружении пропажи карты необходим моментальный звонок в банк для блокировки кредитки.

С развитием Интернета, появлением «виртуальных магазинов» и возможностью заказывать товары по почте с персонального компьютера поле для махинаций с пластиковыми карточками ещё более расширилось. Дело в том, что для оплаты заказанного товара достаточно указать реквизиты карточки. Следовательно, любая информация о карточке для владельца может обернуться невосполнимыми потерями. А способов выманивания реквизитов карточек у владельцев –великое множество. С помощью Интернета производится более тридцати видов мошеннических действий.

Сравнительно недавно в Интернете появился новый вид финансового мошенничества-фишинг, так называемая интернет-рыбалка или, в вольном переводе, закидывание удочки. Технология выуживания личных ПИН-кодов достаточно проста. Вы получаете по электронной почте письмо из банка, в котором держите свои деньги, с просьбой сверить пароли и номер счёта или же обновить свои данные по той или иной причине. Но банк никогда не запрашивает конфиденциальную информацию по почте, а вот умелые мошенники, подделав сайт банка, рассылают такие письма в надежде попасть на доверчивых клиентов. В такой ситуации лучше всего позвонить в банк и всё узнать.

Как же уберечь собственные сбережения? Конечно, банки совершенствуют оборудование и тоже заботятся о безопасности. Появились банкоматы со специальной защитой от скиммеров, с более усовершенствованными модификациями картридера, так называемыми джиттерами (от англ. jitter-дрожание). Благодаря им банкомат «глотает» карточку не плавно, как обычно, а толчками: сначала втягивает карту в приёмное устройство, затем частично выталкивает её наружу, и уже затем окончательно поглощает в своём нутре. Такая процедура сбивает последовательность считывания информации скиммером и делает процесс копирования данных невозможным. Старайтесь выбирать такие банкоматы, т.к. гарантии безопасности у них выше.

Самое главное оружие в борьбе со скиммерами - это бдительность держателей банковских карт.

При работе с банкоматом следует учесть ряд простых правил:

- Если Вы, подойдя к банкомату, на месте углубления картоприёмника видите выпуклость или какое-то иное «новшество дизайна» - звоните в банк, выясняйте подробности дизайна данного банкомата. Как правило, любые усовершенствования банкоматов никак не затрагивают лицевую панель;
- Перед использованием банкомата осмотритесь вокруг, не следует использовать «пластик» в присутствии подозрительных людей, или если банкомат выглядит небезопасно или слишком изолированно;
- Ни в коем случае не сообщайте ПИН-код к своей пластиковой карте, ни сотруднику банка, ни отзывчивому прохожему, который изъявляет желание помочь вам с банкоматом, в случае возникновения у вас каких-либо проблем;
- Воспользуйтесь другим банкоматом, если требуется усилие для погружения карты в отверстие банкомата, или в случае, если вы чувствуете, что банкомат работает не так, как обычно;
- В некоторых случаях целесообразнее заплатить комиссию за снятие наличных средств в чужом банкомате, нежели пользоваться сомнительными устройствами для получения наличных;
- Почаще проверяйте баланс, и если начали исчезать какие-либо суммы, даже очень маленькие – звоните в банк;

У многих банков существуют специальные службы, которые в буквальном смысле этого слова круглосуточно сидят и отслеживают операции по пластиковым картам с целью обеспечения их безопасности.