Об электронных способах оплаты.

Основные виды мошенничества

Фрод – вид мошенничества в области информационных технологий, представляющий собой несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи.

Кардинг – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через вирусные программы: «трояны» и «черви»).

Фишинг – создание мошенниками сайта, который будет пользоваться доверием у пользователя, например, сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт.

Скимминг – использование злоумышленниками скиммера – инструмента для считывания, магнитной дорожки платёжной карты. Скиммер представляет собой устройство, устанавливаемое в картоприёмник, и картридер на входной двери в зону обслуживания клиентов в помещении банка.

Основная задача скимминга – считать необходимые данные магнитной полосы карты для последующего воспроизведения ее на поддельной. Таким образом, при оформлении операции по поддельной карте авторизационный запрос и списание денежных средств по мошеннической транзакции будут осуществлены со счета оригинальной, «скиммированной» карты.

После копировании информации с карты, мошенники изготавливают дубликат карты и, зная ПИН, снимают все деньги в пределах лимита выдачи. Видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру ввода в виде козырька банкомата либо посторонних накладок, например, рекламных материалов – используется вкупе со скиммером для получения ПИН-кода держателя, что позволяет получать наличные в банкоматах по поддельной карте.

Варианты GSM фрода

- При подписке на какой-то контент, за условную плату клиенту в договор включают очень высокий тариф на отписку, а после делают всё возможное, чтобы клиент решил отписаться.

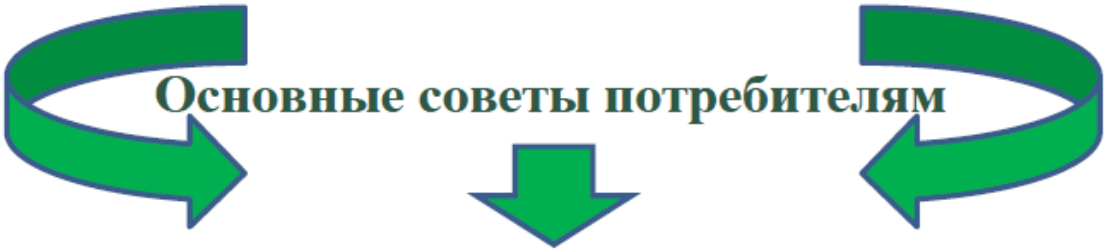
- Невозвраты по SIM-картам кредитных тарифных планов.

- Оформление SIM-карт на потерянные документы с тем, чтобы полученные SIM-карты с роумингом использовать за границей. При этом счета за разговоры местный оператор отсылает оператору, выпустившему SIM-карту, с некоторой задержкой, а пока платит за разговоры самостоятельно.

- Откровенный обман, когда звонящий говорит, что, переводя небольшую сумму на его телефон, вы помогаете своемуродственнику, попавшему в аварию или в другую затруднительную ситуацию.

- Возможен вариант открытия платного сервиса, со способом оплаты посредством SMS-сообщений. При этом технически возможно получение отрицательного баланса на SIM-карте с дебетным тарифным планом.

- Превышение лимита количества отправляемых SMS-запросов, обусловленный техническими возможностями платформы ОСС, приводящий к получению абонентом заказываемых услуг без фактической их оплаты.



- Не скачивать файлы сомнительного характера. Лучше всего использовать официальные сайты программного обеспечения, если вы не хотите заразить свой компьютер вирусами.

- Регулярно обновлять антивирус. О необходимости этого даже не нужно объяснять, чем лучше защищен ваш собственный компьютер, тем меньше шанс получить вредоносную программу.

- Не выключать брандмауэр. Некоторые сервисы, онлайн-игры и другие сайты для корректной работы просят вас отключать встроенную систему интернет-защиты (брандмауэр). Мы советуем этого не делать и избегать такого рода проекты.

- Регистрировать e-mail на надежных сервисах.

- Не читать спам и не открывать письма с прикрепленными файлами. Из самого понятия спама понятно, что он не содержит осмысленной информации и его лучше регулярно удалять.

Эти общие нормы главным образом направлены на защиту вашего персонального компьютера от заражения вирусами.