Если вы решили, что пластиковые карточки - как раз то, чего вам в этой жизни браковало, то вы должны знать: риски для вашего электронного бумажника тоже есть.

Среди наиболее распространенных способов его ограбления - подделка кредитки (по оценкам специалистов, этот вид преступления составляет 40 процентов).

С намагничиванием и эмбасированием особых проблем не есть. Человек, который решил, что карт-воровство, - ее хлеб, просто покупает на радиорынке по доступной цене (ориентировочно 100 долларов США) соответствующий прибор. На втором месте - кражи, связанные с похищением у владельцев кредиток (35 процентов). Наиболее простой способ - установление на клавиатуре банкомата специальной насадки, которая внешне повторяет оригинальные клавиши.

На ней вы набираете PIN-код и оставляете свои "пальчики".

Потом карточку у вас похищают, следовательно из вашего счета уже в любом банкомате снимают ваши деньги. Поэтому смотрите в первую очередь на клавиатуру банкомата, которым пользуетесь.

Еще одним из самых распространенных способов есть применение специального пластикового конверта, немного большего от пластиковой карточки, который закладывают в карт-приемного банкомата. Тогда банкомат не может ни прочитать данных из магнитной ленты, ни повернуть назад вашу кредитку. Потом к вам подходит законспирированный под такого, как и вы, неудачника, вор и говорит, что для того, чтобы повернуть карточку ("за легендой" ему это удалось), нужно ввести PIN-код и нажать служебные клавиши.

Конечно, это дело напрасно, и пока "клиент" бежит связываться с банком, вор достает специальными инструментами кредитку, после чего сразу же на месте, вводя подсмотренный PIN-код, снимает из нее наличность...

Другой способ тоже связан с подсматриванием PIN-кода и похищением кредитки. Для этого преступники устанавливают видеокамеру, которая соединена Bluetooth или другим беспроволочным способом. Преступнику достаточно быть от видеокамеры на расстоянии 10 метров...

Чтобы уберечься от видео-глаза, достаточно прикрыть клавиатуру во время набора другой рукой.

От еще одного способа рукой не закроешься, поскольку он связан с коррупцией, которая, кроме власти, бывает еще и в банках. Банковский служащий продает ваш PIN-код ворам, а дальше у вас из счета исчезают деньги - или при посредничестве похищенной карточки, или эмитированной в кустарных условиях злоумышленниками.

Однако специалисты соглашаются: это бывает крайне редко. Более дешево будет злоумышленникам подключиться к соответствующему кабелю, которым передают данные. Этим способом можно перехватить информацию, которую банкомат посылает в банк, чтобы убедиться, что сумма запроса есть на счете.

Пока еще мало популярным является способ, связанный с использованием интернета. Преступники пытаются получить реквизиты кредитки с целью их последующего использования для закупок в интернет-магазинах.