# ****Личная финансовая безопасность****

 Одним из наиболее эффективных способов защиты прав потребителей является обеспечение высокого уровня финансовой грамотности самих граждан. Финансово образованный потребитель наилучшим образом способен понимать раскрываемую информацию и оценивать риски и выгоды, связанные с каждым видом предлагаемой финансовой услуги. Начиная с выбора банка или иного кредитного учреждения, заключения договоров и заканчивая защитой прав потребителей в суде,  обеспечить максимально полезный результат в интересах потребителя возможно только если он сам будет обладать хотя бы минимальными знаниями в сфере предоставления финансовых услуг.

Финансовая безопасность напрямую зависит от ежедневно принимаемых решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтениеусловий договоров, отсутствие финансовой дисциплины и – как следствие – неисполнение своих обязательств и неприятная финансовая ситуация.

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления  доверием и других манипуляций с  целью незаконного обогащения.

Существуют  несколько видов мошенничества:

●Мошенничество  с использованием банковских карт;

● Мобильные и Интернет- мошенничества.

# *****Мошенничество с использованием банковских карт*****

Банковская карта – удобный инструмент повседневных расчетов.

Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча  во время операций  с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение.

Основные приемы, которые используют злоумышленники:

• скимминг или установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте;

• Траппинг – установка на банкомат устройства, которое блокирует карту и не выдает  ее обратно, а «добрый прохожий», якобы пытающийся помочь, подглядывает пин-код и после вашего ухода,  забирает карту из банкомата и снимает с нее деньги;

• Магазинные мошенничества, когда во время оплаты покупки или услуги данные карты могут быть считаны и зафиксированы ручным скиммером;

• Фишинг – рассылка электронных писем, в которых от имени банка сообщается об изменениях, производимых в системе его безопасности. При этом пользователей просят возобновить информацию о карте, в том числе указать ее номер и пин-код;

•  Мошенничество с помощью телефона – когда клиенту поступают звонки с просьбой погасить задолженность по кредиту, который клиент не брал, и в ходе разговора уточняются данные карты.

Во  избежание вероятности хищения средств с вашей карты соблюдайте следующие правила:

• При использовании банкомата внимательно осмотрите поверхность над пин-клавиатурой и устройство для приема карты на предмет нахождения посторонних прикрепленных предметов;

• Закрывайте рукой клавиатуру при вводе пин-кода;

• Не передавайте банковскую карту посторонним;

• Требуйте проведения операций с картой только в личном присутствии;

• Никому не сообщайте ваш пин-код или код из смс-сообщения.

Помните: кредитные организации и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов!

• Сообщайте банку актуальные контактные данные;

• Подключите услугу SMS-уведомлений, всегда имея при себе телефон круглосуточной службы поддержки владельцев карт банка, вы обеспечите эффективную профилактику риска несанкционированных операций по ней.

• ХранитеПИН-код отдельно от карты и не записывайте его на карте. При его потере ил краже немедленно заблокируйте карту.

Уберегите себя также и от неприятных последствий собственной невнимательности:

• Своевременно оплачивайте кредит и не превышайте лимит кредитования – это убережет от штрафов;

• Не теряйте карту – перевыпуск ее может стоить дополнительных средств;

• Не снимайте с карты деньги полностью – оставьте некоторую сумму для оплаты комиссий или  автоматических платежей;

• При использовании карты зарубежом, помните о курсовой разнице во избежание нежелательного  «овердрафта».