ЛИЧНАЯ ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

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

МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

- **Скимминг** – это установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте: накладная клавиатура или миниатюрная камера, которая заснимет процесс ввода ПИН-кода, и устройство для считывания данных карты. Перед пользованием банкоматом внимательно осмотрите его на предмет наличия посторонних предметов.
- **«Магазинные мошенничества».** Данные карты могут быть считаны и зафиксированы ручным скиммером. Поэтому не передавайте карту или ее данные посторонним, требуйте проведения операций с картой только в личном присутствии.
- **Траппинг.** На банкомат устанавливаются устройства, которые блокирует карту. На помощь человеку приходит мошенник, который подглядывает ПИН-код и после ухода человека достает карту из банкомата. При вводе ПИН-кода закрывайте рукой клавиатуру.
- **Фишинг.** Рассылка электронных писем о якобы производимых изменениях в системе безопасности банка. Мошенники просят дать информацию о карте, в том числе указать номер кредитки и ее ПИН-код отправив ответное письмо или заполнив анкету на сайте, похожем на сайт банка-эмитента. Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте его.
- **Вишинг** (голосовой фишинг). Сбор информации о номерах карт и счетов при помощи моделирования звонка автоинформатора.
- Звонки мошенников с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.

Банки не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Меры безопасности:

- Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете
- Сохраняйте документы до окончания проверки правильности списанных сумм
- Сообщайте банку актуальные контактные данные
- Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки

В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

ИНТЕРНЕТ-МОШЕННИЧЕСТВА

- **Покупки через интернет.** Продавец просит оплатить товар через систему денежных переводов, используя фальшивое или недействительное удостоверение личности. Получая деньги, он исчезает.
- **Составление гороскопа.** Пользователю предлагается заполнить анкету, после чего на электронный адрес отправляется не сам гороскоп, а письмо с указанием отправить по

указанному номеру СМС-сообщение. Стоимость такого сообщения может составлять несколько сотен рублей.

- **Письма платежных систем,** к которым прилагается вирус, замаскированный под вложение – файл или ссылку. Его задача – собрать данные о ваших аккаунтах в платежных системах и данные банковских карт.
- **Нигерийские сюжеты.** Некое высокопоставленное лицо из африканской страны просит помочь в выводе значительной суммы денег за процент. При этом клиента просят перечислять незначительные суммы для оформления перевода и других действий, пока клиент не осознает, что его обманули.

Способы защиты

- Не открывайте сайтов платежных систем по ссылке в письмах, проверяйте URL в адресной строке, посмотрите, куда ведет ссылка.
- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах.
- Не сообщайте ваши пароли, вводите их только на сайтах платежных систем.
- Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации, делайте несколько копий таких файлов.
- Не оплачивайте никаких взносов, при трудоустройстве на удаленную работу.
- Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» как правило от организаторов финансовых пирамид.
- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

МОБИЛЬНЫЕ МОШЕННИЧЕСТВА

- **«Вы выиграли приз».** Мошенник привлекает жертву дорогим подарком, который он «выиграл», при этом просит прислать подтверждающую СМС, внести регистрационный взнос и т.п. Получив деньги, мошенник исчезает.
- **«Мама, я попал в аварию».** Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.
- **«Ваша карта заблокирована».** На мобильный телефон приходит соответствующая СМС с указанием телефона для разблокировки, по которому мошенник предлагает жертве совершить несколько операций с банкоматом под диктовку. Деньги с карты перейдут на счет мошенников.
- **Вирус**. Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

Способы защиты

- Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов.
- При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию.
- Не отправляете СМС на короткие номера, заранее не узнав его стоимости.
- Не сообщайте никаких персональных данных. Попросите представиться, назвать ФИО, звание должность, наименование организации… Узнайте телефон этой организации в справочных базах и перезвоните.

- Если вам сообщают, что ваш родственник или знакомый попал в беду и за него нужно внести деньги - позвоните ему напрямую.
- Ценную информацию не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВОЙ ПИРАМИДЫ:

- Не поддавайтесь на агрессивную рекламу и обещания гарантированной доходности выше ставки банковского депозита.
- Обратите внимание на признаки финансовых пирамид: высокая доходность за счет непрозрачных сверхприбыльных проектов в другой стране, сокрытие организаторами информации о себе, отсутствие лицензий, обещание вознаграждения за приведенных друзей.
- Принимайте взвешенные решения, не поддавайтесь эмоциям.

Если деньги уже вложены в сомнительные проекты, постарайтесь максимально оперативно изъять не только полученную прибыль, но и основные вложения.

ФОРЕКС

Компании, предлагающие услуги на рынке Форекс, в основном получают доход от кредитования (предоставления займов) своих клиентов – физических лиц. Такие кредиты обычно называются «плечами», величина которого может достигать 1/100 (то есть на каждый рубль собственных средств можно совершать сделки на 100 рублей).

Такой кредит преподносится как возможность много заработать с минимальной суммой собственных денег. Но при наличии кредитного плеча, равного 100, движение рынка против игрока всего лишь на 1% означает полную потерю им 100% собственных средств! Если человек соглашается сотрудничать с кем-то из посредников, действующих на этом рынке, все риски он берет исключительно на себя.