**Для размещения на сайте, в раздел Пресс-служба**

**Личная финансовая безопасность**



Под финансовой грамотностью населения допустимо понимать способность физических лиц оценивать финансовую ситуацию и принимать эффективные решения в отношении личных финансов, основываясь на информации, полученной из надёжных источников, то есть наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений.

В последнее время популярным и практическим способом хранения денежных средств являются банковские карточки, так как они всегда под рукой, а получить наличные или рассчитаться в магазине можно, только зная ПИН-код.

Мошенничество с банковскими картами стало популярным, поскольку мошенники постоянно придумывают новые уловки и махинации, целью которых является кража денег с личного счета.

Обхитрить банковскую систему безопасности не так просто, поэтому преступники стараются любыми способами узнать информацию о карте у самого держателя, поэтому они стараются использовать все возможные ресурсы — телефон, интернет-сайты, онлайн-банк, мобильный банк и прочие каналы.

Например:

Звонок на мобильный телефон (Данный вид мошенничества имеет различные вариации. Владельцу карты звонят с незнакомого номера и под любым предлогом просят сообщить её реквизиты, но всё не так просто, как может показаться на первый взгляд, так как чаще всего мошенники представляются сотрудниками банка, извещают клиента о том, что его карту пытались взломать и просят уточнить данные для исправления ситуации, либо же, о том, что в работе системы безопасности случился сбой, и на данный момент существует необходимость сообщить всю необходимую информацию для восстановления и т. п.);

Через отправку СМС-сообщений (Эта схема имеет много общего с предыдущим способом, разница лишь в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера, но мошенники как правило подписываются известной компанией);

Через интернет банкинг (Услуга «Мобильный банк» позволяет совершать операции с помощью СМС-команд, например, для того, чтобы перевести средства на другой счёт, достаточно отправить сообщение на короткий номер банка с того телефона, который привязан к карте).

Для преступников не всегда главной целью являются реквизиты карты. Самый простой способ незаконного обогащения — убедить клиента в том, что он должен перевести деньги самостоятельно.

Существуют способы хищения денежных средств через банкоматы. В этом случае используются такие способы, как:

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, советует ввести ПИН-код.

Известны случаи финансового мошенничества через интернет, а именно посредством продажи и покупки товаров на таких сайтах как Авито.

Самым древним способом незаконного финансового обогащения, связанного с банковской картой физического лица, является элементарное её хищение.

На основе вышеизложенного можно выделить ряд правил, которые помогут обезопасить свой финансовый капитал от действий мошенников, а именно:

Не размещать в свободном доступе и не передавать посторонним информацию о банковской карте. К такой информации относится: номер карты, анкетные данные, кодовое слово, пароль, CVV-код на обороте карты, фотография карты;

При получении СМС-сообщений от неизвестных номеров (как правило, от лжесотрудников банка) не стоит перезванивать или отвечать на подобные СМС-сообщения, а также переходить по прикреплённым ссылкам. Злоумышленники могут удаленно оформить интернет-заявку на получение кредита и воспользоваться одобренным кредитом. Лучшим решением в сложившейся ситуации будет удаление полученного сообщения и блокировка подозрительного номера отправителя;

Использовать для работы с банком только официальные банковские приложения, которые подтверждены лицензионно и имеют на своей странице полный перечень правил пользования сервисом. Как правило, при оформлении новой карты сотрудники банка сразу же предлагают клиенту подключить услугу интернет-банкинга и помогают с регистрацией; Не следует доверять незнакомым ресурсам в интернете, которые вызывают сомнение; Использовать услугу СМС-уведомлений для контроля за счётом. Эта функция значительно упростила жизнь владельцам банковских карточек, а также повысила уровень обеспечения безопасности, поскольку клиент всегда в курсе состояния своего финансового счёта и при возникновении подозрительной ситуации имеет возможность немедленного реагирования;

Следует хранить ПИН-код отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода, дабы стоящие за спиной люди не имели возможности узнать и в дальнейшем использовать полученную информацию;

Не лишним будет установить расходные лимиты в интернет-банке или мобильном приложении, так как чаще всего при оформлении заказов в интернет-магазинах пользователи не ощущают физической траты денежных средств и могут самостоятельно сократить свой бюджет, при чём в значительной степени;

Необходимо немедленно заблокировать карту в случае потери, кражи или захвата её банкоматом, а также при утере телефона, сопряжённого с картой. Для оплаты на торговых площадках (например, Авито или Юла) использовать исключительно официальные сервисы оплаты. Не оплачивать товары или оформлять возврат по ссылкам, которые были отправлены в переписке или мессенджерах;

Сервисы, которые обещают выигрыши, вознаграждения за пройденный опрос и другие компенсации являются довольно распространенной уловкой мошенников. Нужно обязательно проверять отзывы в интернете перед использованием таких сервисов; Предложение инвестировать деньги под необычайно высокий процент, пополняя инвестиционный счёт с карты — следует внимательно изучить историю и отзывы о таких компаниях, а лучше всего использовать официальные банки для таких целей. Инвестируя в интернете возникает огромный риск потери своих финансов.

Юрисконсульт филиала ФБУЗ «Центр гигиены и эпидемиологии в

Чувашской Республике – Чувашии в г. Новочебоксарске» К. А. Хораськин