Как защититься от мошенников и держать средства в сохранности.

Ознакомьтесь с основными правилами и рекомендациями по кибербезопасности и соблюдайте их для сохранения своих средств, т.к. безопасность счета зависит прежде всего от вас самих.

Для получения доступа к чужим деньгам злоумышленники используют все более новые и изощренные способы. В результате люди страдают от их действий, теряя свои накопленные деньги. Зная и соблюдая основные правила можно сохранить средства в безопасности. В этом разделе ЗАО МДО «Имон ИНТЕРНЕШНЛ» представляет основные рекомендации по защите от возможных сценариев получения доступа к вашим средствам со стороны мошенников. Злоумышленники, используя методы социальной инженерии (психологическое воздействие на человека таким образом, чтобы он предоставил свои личные конфиденциальные данные), всячески пытаются выманить у жертвы ценные данные с последующем списанием денег с его счетов. Обращаем ваше внимание, что сотрудники компании:

- НЕ осуществляют звонки с просьбой предоставления персональных данных, номеров карт, одноразовых паролей из СМС для подтверждения финансовых операций
- НЕ просят коды из СМС для отмены совершённых «мошеннических операций»
- НЕ просят у вас коды безопасности с обратной стороны карты (CVV/CVC), логин/пароль/пин-код от ИМОНЛАЙН, коды из СМС, номер банковской карты

Основные правила:

- Никогда и ни при каких условиях не сообщайте никому свои пароли, ПИН-коды и CVV-коды и коды из смс-подтверждения, даже сотрудникам банков.
- Не переходите по подозрительным ссылкам. Злоумышленник может направить вас на фишинговый (поддельный) сайт и украсть ваши конфиденциальные данные.
- Используйте только одобренные и официальные приложения из AppStore, Google Play. Не устанавливайте приложения из недостоверных источников.
- Используйте антивирусное ПО и регулярно обновляйте базы сигнатур.
- Сообщите организации о смене номера мобильного, т.к. есть риск того что ваши данные попадут новому пользователю.
- Проверяйте реквизиты платежей и переводов, которые приходят в СМС от организации
- Регулярно меняйте код, пароль и другие персональные идентификационные данные, не используйте легкие пароли, как имя или дата рождения. Пароль должен содержать не менее 8 знаков комбинацию из букв (прописных и заглавных), специальных символов и цифр;
- Не используйте один и тот же пароль для доступа на разные сервисы;

Как безопасно пользоваться приложением ИМОНЛАЙН:

Никому не говорите пароль, ПИН-код для входа в приложение.

Не устанавливайте приложения по ссылкам из СМС-сообщений или электронной почты, даже если в сообщении указано что оно из банка.

Установите сложный пароль на своем смартфоне.

При утере телефона обратитесь в организацию для блокировки кошелька.

Проверяйте выписки с банковских счетов, отслеживайте оповещения об операциях.

Сохраняйте чеки о любых операциях и движениях по счетам, сообщайте организации о любых несоответствиях.

Как безопасно пользоваться банкоматами:

Прикрывайте клавиатуру рукой, когда вводите ПИН-код.

Не принимайте помощь от незнакомцев, находясь у банкомата, и не совершайте операции под диктовку.

Перед использованием осмотрите банкомат и местность и убедитесь, что на нём нет подозрительных устройств. Если банкомат повреждён или находится в сомнительном месте, лучше перестраховаться и не пользоваться им.

Как безопасно пользоваться платежными картами:

Не передавайте данные карты (ПИН-код, CVV-код) другим лицам и нигде не записывайте.

Не оставляйте карту без присмотра и не передавайте её никому.

Не совершайте покупки в сомнительных интернет-магазинах, с общедоступных компьютеров или с использованием бесплатного интернета. Делайте покупки только на проверенных сайтах. Лучше завести отдельную карту для онлайн-покупок и пополнять только на ту сумму которая нужна для оплаты.

При утере карты срочно заблокируйте её. Для этого позвоните в контакт-центр организации на номер 1122 с мобильного телефона, либо посредством мобильного кошелька ИМОНЛАЙН.

Проверяйте выписки с банковских счетов, отслеживайте оповещения об операциях

Сохраняйте чеки о любых операциях и движениях по счетам, сообщайте организации о любых несоответствиях.

Куда обращаться?

В случае возникновения сомнений либо подозрительной операции немедленно обратитесь в справочно-информационную службу по номеру: 1122

Примеры мошеннических схем для выманивания конфиденциальных данных:

1. Злоумышленник звонит жертве с номера похожего на номер контакт-центра банка (наподобие 1122, 808 и др.), представляется сотрудником банка и сообщает о якобы выигранном денежном призе от проведенного розыгрыша (когда действительно многие банки проводят реальные розыгрыши) и просит предоставить данные карт (ПАН номер и CVV) для зачисления выигранной суммы.
2. Мошенник звонит по случайному номеру из сайта размещения бесплатных объявлений (сомон.тч и др.) и интересуется товаром у владельца. Мошенник утверждает, что живет в другом городе/районе и предлагает перевести сумму на мобильный кошелек владельца, а товар отправить через курьера либо на такси. После соглашения мошенник пытается получить доступ к мобильному кошельку владельца посредством ввода номера телефона владельца на свой телефон. Система отправляет смс-код для входа на номер владельца, и мошенник просит продиктовать этот код объясняя это тем, что для того, чтобы деньги поступили на счет он должен ввести этот код у себя на кошельке, но на самом деле он получает доступ к кошельку владельца.
3. Мошенник отправляет на почту о крупных скидках на какие-то товары и ссылку на поддельный сайт (идентичный известным сайтам как Алиэкспресс, Волна, Амазон и др.) для заказа товара со скидкой (жертва вводит свои данные от платежной карты что в итоге эти данные попадают в руки мошенника).
4. Преступники рассылают в популярных группах и социальных сетях посты, в которых говорится что они готовы помочь лицам пострадавшим от рук мошенников за небольшую плату вернуть украденные деньги. После того как жертва поверит и обращается к ним, у него просят данные карты. Получив требуемые данные, мошенники крадут оставшиеся средства и дальше блокируют жертву.
5. На телефон звонит мошенник и представляется сотрудником сотового оператора и сообщает что есть возможность быстрого прохождения процедуры перерегистрации сим-карты без очередей (актуальная тема с симкартами). Для завершения процедуры мошенник просит смс-код,

отправленный на телефон жертвы. На самом деле этот код используется для доступа к личному кабинету или мобильному кошельку жертвы.

6. Мошенники на местах скопления большого количества людей раздают бесплатные сим-карты. Эти симкарты затем будут использоваться для контроля над вами и вашим аккаунтом в каком-либо сервисе. Мошенник могут перевыпустить сим-карту и после все звонки и смс будут поступать на новую симкарту.
7. Преступники звонят жертве и сообщают что на их имя оформили кредит. Предложат отменить заявку, выманивают данные о жертве, затем оформляют настоящий кредит. Впоследствии зачисленные деньги крадут.
8. В период определенных событий, например подача заявок на грин-карты активизируются мошенники. Создают ярлыки на поддельные сайты заполнения данных на компьютеры в интернет-кафе. Помимо других данных добавляют поля ввода данных карт и банкинга жертвы.
9. Мошенники рассылают по смс ссылку на скачивание полезного приложения, что в свою очередь собирает информацию о жертве.
10. Преступник звонит жертве и представляется сотрудником техподдержки банка и сообщает что только что восстановили работоспособность сервисов по мобильному кошельку и карточкам и просит продиктовать данные от карты и мобильного банкинга для якобы повторной активации услуг.