Алгоритм действий гражданина, при попытке совершения в отношении него преступлений с использованием
информационно-телекоммуникационных технологий (наиболее распространенные виды мошенничеств).

|  |  |  |
| --- | --- | --- |
| №п/п | Способ совершения преступления | Действия гражданина по предотвращению совершения в отношении него преступления |
| 1. | Поступление звонка на абонентский номер гражданина от сотрудников служб безопасности банков, должностных лиц министерств, ведомств Российской федерации | 1. Если звонящий начинает уточнять какие-либо персональные данные, в т.ч. конфиденциальную информацию, связанную с банковским счетом или банковской картой - прервать разговор;
2. Не сообщать звонящему коды из входящих СМС-сообщений;
3. Не устанавливать по рекомендации звонящего какие-либо приложения на свой мобильный телефон, такие как «AnyDesk», «TeamViewer», «Zoom» и т.п.;
4. Не впадать в панику и не пугаться угрозам, поступающим от звонящего, который может сообщить, что в отношении гражданина возбуждено уголовное дело (в том числе, якобы, из-за финансирования вооруженных сил Украины).

Если по какой-либо из причин гражданин не последовал указанным советам и злоумышленник совершил хищение денежных средств со счета, в кратчайший срок необходимо заблокировать банковскую карту, с целью предотвращения дальнейшего хищения денежных средств, посредством связи с банком-эмитентом карты. Контактный телефон банка, выпустившего карту, указан на ее оборотной стороне. |
| 2. | Поступление звонка на абонентский номер гражданина от сотрудников правоохранительных органов, под предлогом того, что родственник или знакомый стал виновником ДТП | 1. Даже при высказывании угроз со стороны звонящего, необходимо прервать разговор и связаться непосредственно с родственником или знакомым, якобы ставшим виновником ДТП, с целью проверки информации, поступившей от неизвестного.
2. В случае следования советам злоумышленника, при очередном прерывании с ним разговора, необходимо сообщить в полицию.
3. Ни в коем случае не открывать дверь и не передавать денежные средства неустановленным лицам,

прибывшим по месту жительства гражданина. |
| 3. | Поступление звонка на абонентский номер сотовой связи гражданина, якобы от сотрудников оператора мобильной связи Российской Федерации, с целью продления договора обслуживания и предотвращения блокировки СИМ-карты | При поступлении звонка с предостережением от неизвестного о том, что СИМ-карта оператора сотовой связи, находящаяся в пользовании гражданина, может быть заблокирована и необходимо осуществить подтверждение личности ее владельца:1. Ни в коем случае не сообщать неизвестному коды из входящих СМС-сообщений
2. Не устанавливать по рекомендации звонящего какие-либо приложения на свой мобильный телефон, такие как «AnyDesk», «TeamViewer», «Zoom» и т.п.;

Для подтверждения личности гражданина, операторы сотовой связи никогда не звонят абоненту, а только присылают СМС-сообщения с указанной информацией. При наличии в указанном СМС-сообщении какой-либо ссылки на Интернет-ресурс, настоятельно не рекомендуется по ней переходить, а лично обратиться в ближайший офис оператора связи для проведения указанной операции. |
| 4. | Поступление звонка на абонентский номер гражданина, якобы от сотрудника государственного портала «Госуслуги» | 1. Ни в коем случае не сообщать неизвестному коды из входящих СМС-сообщений
2. Не устанавливать по рекомендации звонящего какие-либо приложения на свой мобильный телефон, такие как «AnyDesk», «TeamViewer», «Zoom» и т.п.;
 |

|  |  |  |
| --- | --- | --- |
|  |  | 3. Для уточнения информации, предоставленной неизвестным, прервать разговор и позвонить по контактным абонентским номерам портала «Госуслуги» («8-800-100-70-10» или по телефону «115» (с абонентских номеров операторов сотовой связи). |
| 5. | Приобретение товара по цене ниже рыночной посредством торговых Интернет- площадок, таких как «А\ч1о» и «Юла». | 1. Всегда пользоваться услугой «Безопасная сделка», посредством собственноручного ее оформления при переходе по соответствующей ссылке, размещенной в объявлении продавца. Ни в коем случае не следовать советам продавца, который перенаправляет общение с ним в мессенджеры «WhatsApp», «Viber», «Telegram», а тем более в них присылает ссылку, якобы для оформления «безопасной сделки».
2. При возникновении сомнений в добропорядочности продавца, никогда не переводить денежные средства в полном объеме на предоставленные им номера банковских карт и счетов
3. Не сообщать продавцу конфиденциальную информацию по банковской карте или расчетному счету (такие как полный номер карты, месяц/год ее действия, CVV-код с ее оборотной стороны). Если все же они были предоставлены продавцу, не сообщать код из входящего СМС-сообщения на абонентский номер гражданина
4. Если же гражданин сообщил все указанные сведения продавцу, незамедлительно принять меры по блокировке банковской карты, с целью предотвращения дальнейшего хищения денежных средств и дистанционного оформления кредитов, посредством связи с банком-эмитентом карты. Контактный телефон банка, выпустившего карту, указан на ее оборотной стороне.
 |
| 6. | Приобретение товара посредством торговых Интернет-площадок, таких как «OZON>, «Wildberies», «Яндекс.Маркет» | 1. В случае приобретения товара на указанных маркетплейсах и последующем отказе в оформлении, под предлогом того, что товар закончился на складе, не начинать общение с неизвестным, от которого поступило предложение в мессенждерах «WhatsApp», «Viber», «Telegram» о заказе такого же товара с другого склада со скидкой.
2. Если же переписка с неизвестным состоялась, не переводить денежные средства на банковские реквизиты, которые он предоставил и не сообщать ему конфиденциальную информацию по банковской карте или расчетному счету (такие как полный номер карты, месяц/год ее действия, СУУ-код с ее оборотной стороны). Если все же они были предоставлены продавцу, не сообщать код из входящего СМС-сообщения на абонентский номер гражданина.
3. Не переходить по Интернет-ссылкам, предоставленным неизвестным.
 |
| 7. | Приобретение товара на различных Интернет-сайтах по продаже бытовой или сельскохозяйственной техники (в том числе таких как «М.Видео» и «Эльдорадо») | 1. Всегда обращать внимание на URL-адрес указанных сайтов. В них не должно быть каких-либо не логичных символов, которые отсутствуют в их официальных названиях. Также в URL-адресах сайтов крупных Интернет- магазинов всегда используется протокол «https://», вместо распространенного и не актуального в современном мире протокола «http://» На сайтах крупных торговых сетей оформление происходит только после регистрации личного аккаунта. В случае, если оплата заказа происходит путем перевода на банковскую карту, указанную на сайте - значит он принадлежит мошенникам. Ни в коем случае не осуществлять перевод денежных средств указанным способом. В случае, если все же перевод был осуществлен — необходимо сделать скриншот экрана указанного мошеннического сайта и, по возможности, запомнить полный номер банковской карты злоумышленника.
2. Перед совершением заказа на сайте, который вызывает сомнения, ознакомиться с отзывами по нему, размещенными в сети Интернет.
 |
| 8. | Поступление просьбы от родственника или знакомого в мессенджерах «WhatsApp», «Viber», «Telegram» , социальных сетях «В Контакте», «Одноклассники» | 1. Никогда не переводить денежные средства родственникам или знакомым на не знакомые банковские реквизиты, предоставленные в сообщениях, посредством указанных мессенджеров и социальных сетей. Всегда перед совершением перевода гражданином денежных средств, связываться с лицом путем совершения звонка, от которого поступила указанная просьба. |

|  |  |  |
| --- | --- | --- |
|  | об оказании финансовой помощи, или осуществления голосования, путем перехода по Интернет-ссылке | 2. Без предварительной телефонной беседы со знакомым или родственником, не переходить по высланным с их аккаунтов Интернет-ссылкам, если ранее такие просьбы с их стороны не поступали, или сам URL-адрес указанной Интернет-ссылки кажется подозрительным. |
| 9. | Соискание работы посредством сети Интернет на сайтах «hh.ru» или на аналогичных ему | 1. В случае переписки с потенциальным работодателем, ни в коем случае не совершать переводы денежных средств под различными предлогами на предоставленные банковские реквизиты.
2. Также категорически не рекомендуется без предварительной встречи отправлять незнакомцу фотографии документов личности (паспорт, водительское удостоверение, военный билет, загранпаспорт).
 |
| 10. | Поступление звонка гражданину с предложением участия в торгах ценными бумагами и фьючерсами | Звонящий всегда представляется биржевым аналитиком, осуществляющим сопровождение сделок на различного рода биржевых платформах. Как правило, после согласия гражданина на участие в торгах, предоставляет URL-адрес самого биржевого сервиса, на котором, как и на официальных биржевых сервисах «Forex», «Binance», размещены правоустанавливающая документация на проведение финансовых операций на территории Российской Федерации от имени Центрального банка России, а также информация о возможных рисках потери денежных средств гражданином при ведении биржевой деятельности.Категорически не рекомендуется начинать деятельность, если неизвестный:1. Переадресовывает общение с ним в такие мессенджеры, как «Skype» или «WhatsApp»
2. С целью пополнения кошелька Интернет-ресурса по биржевой торговле, предоставляет гражданину номера счетов банковских карт неустановленных лиц
3. Требует оформления кредитов в кредитных учреждениях, предоставляет гражданину займ на ведение биржевой торговли, требует фотокопии документов, удостоверяющих личность

Перед осуществлением деятельности в биржевой торговле настоятельно рекомендуется ознакомиться с отзывамипо предоставленному неизвестным URL-адресу сервиса брокерской деятельности посредством сети Интернет. Какправило, там всегда размещена информация обо всех брокерских сервисах мошенников. |
| 11. | Получение дополнительной прибыли с помощью лиц, чьи страницы размещены в социальной сети «Instagram» а также мессенджере «Telegram» ипропагандирующие заработок денег по схеме «сегодня переведи мне 10 рублей, завтра получи 100 рублей». | Не рекомендуется связываться с указанными лицами, с целью получения дополнительного заработка денежных средств. Как правило, неизвестные требуют перевода денег на счета банковских карт неустановленных лиц, под предлогом осуществления ими ставок на различного рода спортивные события. Данные лица не осуществляют какого- либо рода деятельность по заработку денег, а всего лишь производят сбор денежных средств с обманутых граждан, для дальнейшего их хищения. |
| Во всех случаях, за исключением предусмотренных законодательством Российской Федерации, категорически не рекомендуется предоставлять незнакомым лицам возможность ознакомления с личным паспортом гражданина РФ, в том числе делать его фотокопии, ксерокопии, во избежание оформления кредитныхобязательств в микрофинансовых организациях. |
| При совершении в отношении гражданина одного из вышеуказанных видов мошеннических действий, необходимо безотлагательно сообщать в полицию по абонентскому номеру «02», Дежурная часть УМВД России по г. Владимиру +7 (492) 232-64-05 (со стационарных телефонов связи), «102», «112»(с телефонных номеров операторов сотовой связи Российской Федерации) |