СЕЛЬСКОЕ ПОСЕЛЕНИЕ
БАХИЛОВО
МУНИЦИПАЛЬНОГО
РАЙОНА СТАВРОПОЛЬСКИЙ
САМАРСКОЙ ОБЛАСТИ

ОФИЦИАЛЬНАЯ ПУБЛИКАЦИЯ

ВЕСТНИК Бахилово

6+

№12 (328),
4 апреля 2025 г.

АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ БАХИЛОВО МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ № 22 от 01.04.2025 г.

ОБ УСТАНОВЛЕНИИ ОСОБОГО ПРОТИВОПОЖАРНОГО РЕЖИМА НА ТЕРРИТОРИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ БАХИЛОВО МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ

В соответствии со статьей 30 Федерального закона от 21.12.1994 № 69-ФЗ «О пожарной безопасности», постановлением Правительства Российской Федерации от 16.09.2020 № 1479 «Об утверждении Правил противопожарного режима», постановлением Правительства Самарской области от 20.03.2025 № 121 «Об особом противопожарном режиме на территории Самарской области», руководствуясь пунктом 3 части 4 статьи 36 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», пунктом 3 статьи 43 Устава сельского поселения Бахилово муниципального района Ставропольский Самарской области, принятого Решением Собрания Представителей сельского поселения Бахилово муниципального района Ставропольский Самарской области от 10.09.2019 № 180, в целях обеспечения пожарной безопасности в лесах и населенном пункте на территории сельского поселения Бахилово муниципального района Ставропольский Самарской области администрация сельского поселения Бахилово муниципального района Ставропольский Самарской области ПОСТАНОВЛЯЕТ:

1.Установить особый противопожарный режим на территории сельского поселения Бахилово муниципального района Ставропольский Самарской области с 01.04.2025 по 15.10.2025.

2.В период действия особого противопожарного режима на территории сельского поселения Бахилово муниципального района Ставропольский Самарской области:

- запретить разведение костров, сжигание мусора, сухой растительности и отходов на территории сельского поселения, организаций, индивидуальных предпринимателей, приусадебных участков;

- при наступлении IV-V классов пожарной опасности в лесах устанавливать запрет на посещение лесов;

- организовать на территории населенного пункта, а также на территории иных категорий земель специальные площадки для складирования сухой травянистой растительности, пожнивших остатков, валежника, порубочных остатков, мусора и других горючих материалов, в том числе организовать вывоз данных отходов;

- запретить применение пиротехнических изделий и огневых эффектов в зданиях и на открытых территориях.

3.Рекомендовать начальнику участка МУ МРС «СтавропольРесурсСервис», руководителю Бахиловского филиала ГБОУ СОШ с. Александровка, руководителю СПДС «Солнышко» ГБОУ СОШ с. Александровка, директору ГБУ СО «Солнечнополянский пансионат для инвалидов», врачу ОВП, заведующему клубом с. Бахилово, заведующему библиотекой с. Бахилово, мастеру филиала Ставропольское ДЭУ:

- установить строгий контроль за соблюдением мер особого противопожарного режима на подведомственных территориях;

-укомплектовать пожарные щиты специальным пожарным инвентарем, первичными средствами пожаротушения;

- вывесить наглядную агитацию о мерах пожарной безопасности, указать номер телефона местного пожарного депо, пожарной охраны города, района и порядок вызова пожарной охраны в случае возникновения пожара.

4. Ведущему специалисту администрации сельского поселения:

- вывесить наглядную агитацию в общественных местах о мерах пожарной безопасности, указать номер телефона местного пожарного депо, пожарной охраны города, района и порядок вызова пожарной охраны в случае возникновения пожара;

- обеспечить территорию населённого пункта связью, средствами звуковой сигнализации для оповещения людей в случае пожара;

- закрепить за каждым домовым хозяйством граждан один из видов противопожарного инвентаря, с которым они должны прибыть на тушение пожара (ведро, багор, лопата, лестница, топор из соотношения 6:1:1:1:1 на 10 домов);

- организовать патрулирование территории населенного пункта силами членов добровольных пожарных формирований с первичными средствами пожаротушения;

- определить допустимые места и (или) способы разведения костров, а также порядок сжигания мусора, травы, листвы и иных отходов, материалов и изделий, в том числе использования мангалов (жаровен);

- очистить территорию сельского поселения от сгораемого мусора, освободить проезды к зданиям и водоисточникам;

- обеспечить выполнение мероприятий по предотвращению распространения пожара на населенный пункт и отдельно расположенные объекты в части устройства минерализованных полос (опашка) вокруг населенного пункта, окашивания и своевременной уборки сухой травянистой растительности, тростниковых и камышовых зарослей, находящихся в границах населенного пункта;

- запретить сжигание сухой травы (сельскохозяйственных палов);

- организовать проверки территорий на предмет выявления фактов засеивания колосовых культур в границах полос отвода и охранных зон железных дорог, путепроводов и продуктопроводов, а также в границах отвода автомобильных дорог и информировать о таких фактах отдел по делам ГО и ЧС администрации муниципального района Ставропольский Самарской области.

5. Рекомендовать начальнику участка МУ МРС «СтавропольРесурсСервис»:

-обеспечить территорию населенного пункта водоснабжением для нужд пожаротушения;

- организовать подготовку водовозной техники к использованию для нужд пожаротушения.

6. Ведущему специалисту администрации сельского поселения совместно с старшим УУП О МВД России по Ставропольскому району (по согласованию):

- организовать информирование населения сельского поселения о правилах пожарной безопасности;

- организовать рейды по местам возможного нахождения лиц без определённого места жительства, мест проживания неблагополучных семей с целью пресечения возможных нарушений требований пожарной безопасности;

- организовать проведение сходов граждан с целью инструктажа населения по вопросам обеспечения пожарной безопасности;

- осуществить обходы жителей частного сектора с целью проведения разъяснительной работы по предупреждению пожаров, обращая внимание на места проживания малоимущих семей, социально не адаптированных групп населения и т.п..

7. Рекомендовать директору ГБУ СО «Солнечнополянский пансионат для инвалидов» в подведомственном учреждении с круглосуточным пребыванием людей обеспечить усиление дежурства дополнительным персоналом, а также организовать проверки соблюдения, в том числе и в ночное время, мер пожарной безопасности.

8. Рекомендовать начальнику участка МУ МРС «СтавропольРесурсСервис», директору ГБУ СО «Солнечнополянский пансионат для инвалидов»:

- провести проверку исправности и наличия приспособлений для забора воды пожарными автомобилями на случай пожара (пожарные гидранты, колодцы, водонапорные башни);

- обеспечить возможность круглосуточного использования водоисточников, места их расположения обозначить указателями согласно ГОСТ 12.4.0026-2015;

- обеспечить исправность и возможность круглосуточного использования бойлеров для подвоза воды к местам тушения пожаров.

9. Рекомендовать руководителям организаций, расположенным на территории сельского поселения, независимо от форм собственности:

- ограничить производство пожароопасных работ (за исключением аварийно - восстановительных работ);

- провести внеплановые противопожарные инструктажи работников и дополнительные практические занятия с работниками по отработке действий при возникновении пожара и эвакуации людей из зданий;

- привести в исправное состояние источники водоснабжения и первичные средства пожаротушения;

- содержать земельные участки, находящиеся в собственности, а также прилегающую к ним территорию, в соответствии с постановлением Правительства Российской Федерации от 16.09.2020 № 1479 «Об утверждении Правил противопожарного режима»;

- принять меры по недопущению складирования мусора, бытовых отходов.

10. Рекомендовать директору ООО «Волжские берега» запретить выжигание прошлогодней стерни, а также стерни после уборки урожая, произвести работы по устройству минерализованных полос (опашка) по границам полей.

11. Рекомендовать руководителю Бахиловского филиала ГБОУ СОШ с. Александровка, старшему воспитателю СПДС «Солнышко» ГБОУ СОШ с. Александровка:

- провести работу с педагогами, учащимися, родителями по разъяснению недопустимости палов сухой травы, разведения костров, сжигания мусора;

- в период подготовки к майским праздникам, перед окончанием учебного года и в период проведения летних оздоровительных лагерей запланировать и организовать проведение классных часов, утренников, инструктажей по тематике пожарной безопасности с целью предотвращения несчастных случаев и во избежание случайных или умышленных поджогов подростками;

- при проведении инструктажей уделить особое внимание осведомленности детей и подростков, добиться их понимания о необходимости незамедлительно сообщать старшим руководителям, воспитателям и родителям о возникновении источника задымления и пожара.

12. Постановление подлежит официальному опубликованию в газете «Вестник Бахилово» и на официальном сайте поселения на официальном сайте администрации сельского поселения Бахилово в сети Интернет http://bahilovo.stavrsp.ru.

13. Контроль за исполнением настоящего постановления оставляю за собой.

Глава сельского поселения Бахилово А.Н. Еремин

АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ БАХИЛОВО МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ № 23 от 04.04.2025 г.

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПОСТАНОВЛЕНИЕ АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ БАХИЛОВО ОТ 01.04.2025 Г. №22 «ОБ УСТАНОВЛЕНИИ ОСОБОГО ПРОТИВОПОЖАРНОГО РЕЖИМА НА ТЕРРИТОРИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ БАХИЛОВО МУНИЦИПАЛЬНОГО РАЙОНА СТАВРОПОЛЬСКИЙ САМАРСКОЙ ОБЛАСТИ»

В соответствии со статьей 30 Федерального закона от 21.12.1994 № 69-ФЗ «О пожарной безопасности», постановлением Правительства Российской Федерации от 16.09.2020 № 1479 «Об утверждении Правил противопожарного режима», постановлением Правительства Самарской области от 20.03.2025 № 121 «Об особом противопожарном режиме на территории Самарской области», руководствуясь пунктом 3 части 4 статьи 36 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», пунктом 3 статьи 43 Устава сельского поселения Бахилово муниципального района Ставропольский Самарской области, принятого Решением Собрания Представителей сельского поселения Бахилово муниципального района Ставропольский Самарской области от 10.09.2019 № 180, в целях обеспечения пожарной безопасности в лесах и населенном пункте на территории сельского поселения Бахилово муниципального района Ставропольский Самарской области администрация сельского поселения Бахилово муниципального района Ставропольский Самарской области ПОСТАНОВЛЯЕТ:

1. Внести в постановление администрации сельского поселения Бахилово от 01.04.2025 г. №22 «Об установлении особого противопожарного режима на территории сельского поселения Бахилово муниципального района Ставропольский Самарской области» (далее- Постановление) следующие изменения: .

1.1. Пункт 2 Постановления дополнить абзацем следующего содержания:

«- проводить мониторинг земель сельскохозяйственного назначения на предмет выявления возгораний сухой травы, стерни на ранней стадии.»

2. Постановление подлежит официальному опубликованию в газете «Вестник Бахилово» и на официальном сайте поселения на официальном сайте администрации сельского поселения Бахилово в сети Интернет http://bahilovo.stavrsp.ru.

3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава сельского поселения Бахилово А.Н. Еремин

ЗАПРЕТ НА ПРОДАЖУ БЕЗАЛКОГОЛЬНЫХ ТОНИЗИРУЮЩИХ НАПИТКОВ

Законом Самарской области от 14.03.2025 № 29-ГД (http://publication.pravo.gov.ru/document/6300202503180005) с 1 сентября 2025 года на территории Самарской области вводится запрет на продажу безалкогольных тонизирующих напитков (в том числе энергетических) в зданиях, строениях, сооружениях, помещениях, используемых для непосредственного осуществления образовательной деятельности, медицинской деятельности, деятельности в области культуры, физической культуры и спорта.

Нарушение установленного запрета продажи безалкогольных тонизирующих напитков (в том числе энергетических) влечет наложение административного штрафа:

- на граждан в размере от одной тысячи до двух тысяч рублей;
- на должностных лиц - от пяти тысяч до семи тысяч рублей;
- на юридических лиц - от десяти тысяч до двадцати тысяч рублей.

Те же правонарушения, совершенные повторно в течение года, влекут наложение административного штрафа:

- на граждан в размере от двух тысяч до пяти тысяч рублей;
- на должностных лиц - от десяти тысяч до пятнадцати тысяч рублей;
- на юридических лиц - от двадцати тысяч до тридцати тысяч рублей.

ПАМЯТКА ПО ПРОФИЛАКТИКЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

На сегодняшний день информационно-телекоммуникационные технологии затрагивают все сферы жизни человека. Наряду с этим, стремительно возрастает количество преступлений, которые совершаются с использованием данных технологий.

На территории Российской Федерации распространено дистанционное мошенничество, к которому относятся:

1. «Фишинг» – вид дистанционного мошенничества посредством разговора по телефону или направления электронного письма или смс-сообщения, при котором злоумышленники получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств.

2. «Фарминг» – направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг;

3. «Двойная транзакция» - «ошибка» при оплате товаров или услуг с предложением повторить операцию, в дальнейшем денежные средства списываются дважды по каждой из проведенных операций;

4. «Траппинг» - манипуляция с картридером банкоматов, позволяющая не возвращать карту владельцу или списывать все данные карты для дальнейшего их использования.

Чтобы обезопасить себя и своих близких от различных схем мошенников необходимо запомнить и выполнять следующие рекомендации:

1. Установить на телефон или компьютер современное лицензированное антивирусное программное обеспечение;

2. Не устанавливать и не сохранять без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников;

3. Не использовать пароли, связанные с персональными данными;

4. Необходимо убедиться в достоверности информации, полученной в ходе телефонного разговора и интернет-переписки с неизвестными. Мошенники могут представляться сотрудниками правоохранительных органов, представителями операторов сотовой связи и банковских учреждений, знакомыми и даже вашими родственниками. Следует связаться с теми, от чьего имени действуют незнакомцы и убедиться в правдивости информации. Не стоит бояться прервать разговор;

5. Ни при каких обстоятельствах не следует сообщать реквизиты своих банковских счетов и карт (номер карты, срок её действия, секретный код на оборотной стороне карты). Сотрудники банка никогда не просят сообщить данные вашей карты или пройти к банкомату;

6. Никогда нельзя переводить денежные средства, если об этом вас просит ваш знакомый в социальной сети. Возможно, мошенниками был взломан аккаунт, сначала необходимо связаться с этим человеком и узнать, действительно ли он просит у вас деньги;

7. Поставить лимит на сумму списаний или перевода в личном кабинете банка;

8. В случае возникновения вопросов обращаться в банк, выдавший карту;

9. Не перезванивать по номерам и не переходить по ссылкам, которые приходят на e-mail или по SMS.

Будьте бдительны и не поддавайтесь на уловки мошенников! Способы и методы совершения краж и мошеннических действий постоянно меняются. В случае малейших подозрений на обман незамедлительно сообщайте об этом в правоохранительные органы по телефону «02» или «112».

ИНФОРМАЦИЯ

о возможности установления гражданином запрета (ограничения) на онлайн-операции, в том числе на заключение кредитными организациями с ним договоров потребительского займа (кредита), в целях предупреждения мошеннических действий со стороны третьих лиц

Пунктом 7.1. Положения «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», разработанного Центральным банком Российской Федерации от 17 апреля 2019 г. № 683-П определено: *«В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) договора об использовании электронного средства платежа, на основании их заявлений устанавливают в отношении операций, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций через информационно-телекоммуникационную сеть «Интернет», ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе видов операций».*

Центробанк обязал банки с 1 октября 2022 года предоставить клиентам возможность собственноручно накладывать запрет на онлайн-операции и ограничивать их параметры (как при кредитовании, так и при денежных переводах).

Самозапрет на кредиты, что это?

Это ограничение, которое банк по заявлению клиента накладывает на операции, осуществляемые с помощью удаленного доступа через интернет. Запретить можно как отдельно кредитование, так и другие банковские операции или установить максимальную сумму.

Принят федеральный закон[1], по которому граждане могут устанавливать самозапрет на выдачу кредитов, который начнет действовать с 1 марта 2025 года. Можно будет устанавливать запрет на заключение договоров потребительского займа с банками и микрофинансовыми организациями (МФО). Гражданам дадут право подать во все квалифицированные бюро кредитных историй заявление через единый портал госуслуг, а также запросить информацию о наличии в кредитной истории сведений о таком ограничении. К заявлению нужно будет прикрепить данные СНИЛСа.

Снять запрет можно будет в любое время, но взять кредит получится только после того, как данные попадут в кредитную историю. Депутаты считают, что такой «период охлаждения» позволит исключить риск мошенничества с одномоментным снятием запрета и заключением кредитного договора.

В каких случаях стоит оформить самозапрет на кредит?

Категорий людей, которым рекомендуют оформить такой самозапрет, нет. В настоящее время юристы рекомендуют делать это лично, в присутствии сотрудника банка и самого клиента, с обычной подписью (целесообразно написать заявления о запрете во все крупные банки, а как минимум в те, где вы когда-либо обслуживались по дебетовой карте, кредитной карте, кредиту.

Как оформить самозапрет на кредиты через «Госуслуги»?

С 1 марта 2025 года самозапрет на кредиты можно будет выставить на «Госуслугах», с 1 сентября 2025 года – в МФЦ. Эти данные автоматически попадут в бюро кредитных историй. Банки, которые запрашивают информацию в бюро, увидят выставленные ограничения на кредитование. Пока эта опция недоступна.

Можно ли оформить самозапрет через банки, микрофинансовые и другие организации?

Пока это единственный вариант и он уже вступил в силу и действует с октября 2022 года.

В отдельных банках можно написать заявление о запрете онлайн-кредитования конкретно в них. Такая опция есть практически во всех крупных банках, но есть те, которые будут против (к ним необходимо относится скептически, т.к. они не соответствует рекомендациям Центробанка что повышает риски заемщика).

Условия и порядок оформления такого запрета сегодня устанавливает банк.

Аналогичные запреты можно направить и в микрофинансовые организации, но технически сделать это будет сложнее т.к. их слишком много, зарегистрированы они в разных регионах, а о существовании некоторых можно просто не знать.

Можно ли снять самозапрет?

Да. Можно запретить выдавать кредиты на свое имя, потом отозвать запрет, потом запретить снова. Центробанк никак не ограничивает количество таких процедур.

Плюсы и минусы самозапрета на кредиты.

Плюс очевиден – самозапрет на кредиты поможет защититься от мошенников. А возможно, и от спонтанных покупок – кредиты выдаются онлайн за несколько минут. Но если придется ехать в банк, чтобы снимать самозапрет, велик шанс передумать.

Минус только в том, что если вы сами соберетесь взять кредит, то придется потратить время и сходить в отделение банка. Большой проблемы в этом нет, особенно если вы живете в городе, где есть отделение банка. Но если вы проживаете в маленьком городке, где отделений нет и не хочется никуда ехать, то это проблематично.

В принципе, онлайн-кредит – это удобно, но система будет хороша только тогда, когда каждый гражданин будет обладать своей квалифицированной электронной цифровой подписью. Не простой, а именно квалифицированной, как, например, у судей.

Обезопасит ли самозапрет полностью от мошенников?

Полностью – нет, однако он существенно усложнит мошенникам задачу и как минимум защитит от некоторых схем и от потери крупных сумм.

Как обезопасить себя, пока закон не начал действовать?

Если вы хотите оформить именно самозапрет на кредитование или переводы, это можно сделать непосредственно в банке. Конечно, потребуется время, чтобы обратиться во все кредитные организации, но для начала можно подать заявления в банки, услугами которых вы когда-либо пользовались.

Сейчас у некоторых банков есть специальная последовательность действий для онлайн-кредитования, чтобы избежать мошенничества. Например, счет заемщика могут заблокировать, если он пытается сразу же после получения кредита снять или перевести деньги. Для разблокировки счета придется связаться с банком или посетить отделение лично.

Рекомендации:

Юристы советуют раз в год или полгода запрашивать отчет из бюро кредитных историй. Это уже сейчас можно сделать на «Госуслугах» - через сайт заказать выписку из всех БКИ, в которых содержится информация о клиенте.

Также можно периодически проверять себя через систему судебных приставов на сайте ФССП. Достаточно указать ФИО, дату рождения и выбрать регион, по которому будет производиться проверка.

Не пересылайте никогда фотографии паспорта – в некоторых случаях займ могут оформить по фото или копии документа. Если куда-то нужно отправить данные, лучше не поленитесь и перепишите их. Если вам стало известно, что эти данные уже куда-то попали целесообразно менять паспорт. При этом, если паспорт украли или вы его потеряли, следует обратиться в полицию.

Возьмите там справку о том, что паспорт утерян, с указанием даты. Если паспорт попадет в руки мошенников, эта справка будет основным доказательством того, что кредит или займ брали не вы.

Иногда мошенникам достаточно только паспортных данных, поэтому их тоже стоит беречь. Не сообщайте данные по телефону или в соцсетях, не вводите данные на непроверенных и незащищенных сайтах (в адресной строке должно быть изображение закрытого замка). В случае звонка «из банка» не разговаривайте со звонящими – общайтесь в чате поддержки на официальном сайте или в приложении либо перезвоните в банк самостоятельно

[1] Федеральный закон от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)» (вступает в силу 01.03.2025)

ИНФОРМАЦИЯ

о популярных сценариях мошенничества с использованием цифровых технологий и рекомендуемых инструментах защиты

Кибератаки на компании, факты **дистанционных хищений денежных средств** у граждан фиксируются все чаще, при этом криминальные схемы, в том числе по выводу незаконно полученных доходов, постоянно меняются. За последние пять лет количество противоправных деяний в указанной сфере в целом по России возросло в два раза и сейчас составляет треть от всех зарегистрированных преступлений. Больше половины из них относится к категории тяжких и особо тяжких. Основной массив приходится на кражи и мошенничества.

Происходят **утечки персональных данных**, которые используются для формирования так называемых «цифровых портретов» в противоправных целях. Отмечается рост киберхищений, связанных с применением метода социальной инженерии, когда граждане, как правило, пенсионного возраста, сами сообщают сведения о себе лицам, представляющимся сотрудниками государственных органов или банковского сектора. Самые распространенные способы неправомерного завладения денежными средствами сопряжены с созданием фальшивых сайтов, а также получением доступа к конфиденциальным данным пользователей.

В основном такая вариативность реализации преступных намерений исходит из-за рубежа, включая **кол-центры, находящиеся на территории Украины**. Кроме того, киевскими спецслужбами используются схемы запугивания жертв несуществующим уголовным преследованием либо долговой финансовой зависимостью. Это заканчивается совершением последними преступлений против общественной безопасности. Фигурантами по таким делам нередко становятся высокообразованные люди, которые сами призваны формировать законопослушное поведение.

Как показало собственное исследование группы компаний «Сбер», проведённое в 2023 году, на Украине действовало более тысячи мошеннических колл-центров, в которых задействовано порядка 100 тысяч человек. Примерно 300 таких колл-центров сосредоточены в Днепре – так называемой «столице» телефонного мошенничества. По данным банка, 92% звонков преступников направлены на Россию, а оставшиеся 8% получают жители других стран, преимущественно Польши, Германии и Казахстана. Доходы идут на личное обогащение и закупку вооружения против России.

Обнаруженная «Сбером» база данных показала, что 212 колл-центров (на тот момент) управлялись тремя головными центрами по модели франшизы, а инфраструктура для их деятельности сосредоточена в Нидерландах и Германии. Преступники используют профессиональные CRM-системы для управления звонками и фиксируют в них суммы украденного.

Средний колл-центр похищает 40 тысяч долларов в месяц, а совокупный ущерб от деятельности 212 колл-центров, работающих по франшизе, в 2023 году достиг 100 миллионов долларов. Типовой колл-центр совершает 70 тысяч звонков в день и насчитывает до 100 «операторов» в одну смену.

Мониторинг мошеннических схем и способов защиты от них

Чтобы не стать жертвой телефонного или интернет мошенничества необходимо своевременно отслеживать используемые злоумышленниками мошеннические схемы, а также предлагаемые специалистами банковского сектора, правоохранительных органов и юристов инструменты защиты своих сбережений.

Вашему вниманию предлагаются наиболее распространённые в 2022-2023 годах такие сценарии.

«Валютные ограничения»

Последние два года мошенники запугивали своих потенциальных жертв не только несанкционированными переводами или оформлением кредитов, но и привязывались ко всем новостным поводам. Говорили об угрозе в связи с отключением от системы «Свифт», об уходе Visa и Mastercard, о дефиците валюты, об угрозе деньгам на вкладах, т.е. использовали все возможные информационные поводы.

Мошенники звонили потенциальным жертвам, представлялись работниками банков или обменных пунктов и сообщали, что евро и доллары вот-вот перестанут выдавать или изымут из обращения. Людям предлагали перевести деньги на некий «специальный счет», но для этого нужно было сказать по телефону банковские данные, с помощью которых мошенники потом переводили средства на свои счета.

Помните, что банки не запрашивают финансовую информацию клиентов по телефону, поэтому самое лучшее решение в этой ситуации – бросить трубку и найти всю информацию самостоятельно. У Банка России нет планов изымать сбережения ни в рублях, ни в валюте.

Обо всех валютных ограничениях можно узнать на сайте финансового маркетплейса Банки.ру, а если возникнут сомнения, то прежде чем совершать операцию, можно уточнить информацию на «горячей линии».

«Мобилизация»

Одновременно с нагнетанием истерии о возможной мобилизации распространялись две схемы мошенничества – поддельные документы и фишинг.

В первом случае в интернете даже появились сайты, которые маскируются под видом сервисов по изготовлению документов. Кроме того, тем, кого могли мобилизовать, писали в мессенджерах с похожими предложениями.

За медицинскую отсрочку или справку с «бронью» мошенники предлагали заплатить от 20 до 65 тыс. рублей. После оплаты поддельный документ могут не отправить вовсе, но даже если он придет, пользоваться такими справками уголовно наказуемо.

Кроме того, регистрировались случаи, когда мошенники приходили домой к потенциальным жертвам якобы с повесткой. Человеку предлагали за деньги не вручать ее, а иначе придется явиться в военкомат. Правда, массовой эта практика так и не стала.

В случае с фишингом собирались личные данные. Сразу после объявленной мобилизации в Интернете появилась якобы база данных граждан, которых государство планирует мобилизовать. На самом деле подобного списка в открытом доступе нет. Мошенники манипулируют страхом и выдают ложные данные за действительные, предлагая за деньги «исключение из списков мобилизованных».

Второй метод: дать ссылку на якобы полный список, а на сайте уже запросить личные данные и банковскую информацию у потенциальной жертвы. Переводить деньги и переходить по таким ссылкам не стоит.

«Мошенничество под видом государственных органов»

Это многоуровневые схемы звонков с участием якобы правоохранительных органов, Банка России и кредитных учреждений.

Чаще всего говорят о некоем безопасном счете в Центробанке, на который нужно срочно перевести средства, которым якобы грозит хищение. Кроме того, для убедительности присылают человеку в мессенджер или на электронную почту документы или удостоверения с логотипом и печатью Банка России. Также аферисты могут прислать скан-копию заявления о заявке на кредит якобы от лица жертвы с его ФИО и поддельной подписью. Со стороны все это выглядит очень правдоподобно. Критическое мышление у жертв при использовании таких приемов снижается.

Помните: Банк России не работает напрямую с физлицами. По своей инициативе его сотрудники не звонят гражданам, не рассылают им электронные письма и СМС-сообщения. Регулятор не обслуживает и не открывает счета физлиц.

В таких случаях необходимо сразу класть трубку, а также не называть свои личные и банковские данные вне зависимости от того, как представился человек по телефону.

«Брачные мошенничества»

С использованием сети Интернет (преимущественно на сайтах знакомств) преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов.

Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предлогами прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

При покупке в интернет-магазинах, граждане часто невнимательны, чем и пользуются мошенники. Обычно схема мошенничества выглядит так: создаётся сайт-одностраничник, на котором выкладываются товары одного визуального признака.

Цена на товары обычно весьма привлекательная, ниже среднерыночной. Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные данные. Чаще всего такие интернет-магазины работают по 100% предоплате. Переписка о приобретении товаров ведется с использованием электронных почтовых ящиков.

По договоренности с продавцом деньги перечисляются, как правило, за границу через «Western Union» на имена различных людей, после чего псевдо-продавец исчезает.

«Крик о помощи»

Один из самых циничных и распространённых способов хищения денежных средств.

В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Здесь важно прежде чем переводить свои деньги, проверить – имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

«Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на «сайт-двойник» такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

«Нигерийские письма»

Также один из самых распространённых видов мошенничества, когда жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки.

Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

«Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В частности имеется информация о таких недобросовестных брокерских компаниях, как: «MXTrade» и «MMCIS».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам – трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Важно! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.

Способы защиты от мошенничества

Доля возврата средств банками клиентам, когда последние самостоятельно переводят деньги аферистам или открывают им доступ к своему счету.

Сейчас банки по закону «О национальной платежной системе» не обязаны возвращать деньги в этих случаях. Банк России вместе с участниками рынка и экспертами предлагает внести изменения в законодательство, чтобы люди могли рассчитывать на возврат средств даже тогда, когда их обманули с помощью социальной инженерии.

Банк России ведет базу о случаях и попытках перевода денежных средств без согласия клиентов. В ней аккумулируются данные из банков, в том числе содержатся сведения о дропперских счетах, которые злоумышленники используют для вывода и снятия похищенных средств.

Механизм возмещения гражданам похищенных злоумышленниками средств

Если банк-отправитель получил информацию из базы ФинЦЕРТа, но не учел ее в своих бизнес-процессах и совершил перевод на такой счет, то он будет обязан вернуть клиенту похищенную сумму, даже в случаях, когда хищение произошло с использованием методов социальной инженерии.

Кроме того, Банк России внедряет так называемый «период охлаждения», когда у гражданина будет время обдумать и оценить совершаемые действия. Банк-плательщик будет обязан на два дня приостанавливать зачисление денег на счет, информация о котором содержится в базе Банка России. Формально банк не нарушит права добросовестных граждан и законодательство, приостанавливая перевод, поскольку по закону перевод совершается в срок до трех рабочих дней

Кроме того, проверять операцию на признаки мошенничества должен и банк-получатель. Если он видит, что деньги перечисляют на счет, содержащийся в базе регулятора, то у банка должно быть право приостанавливать доступ владельца такого счета к дистанционному обслуживанию. То есть получатель подозрительного счета не сможет сразу же удаленно распорядиться деньгами, перевести их на любой другой счет, что обычно сразу делают мошенники. Чтобы разблокировать эту возможность, владельцу счета придется прийти в отделение банка с паспортом, на что вряд ли пойдут дропперы. В то же время будут соблюдены все гражданские права добросовестных банковских клиентов.

Банк России повышает требования к банковским полисам страхования от мошенников, чтобы в страховки были включены случаи возврата средств при атаках социальных инженеров. Речь о любых случаях, когда клиент добровольно переводит деньги мошенникам или раскрывает им банковские сведения, то есть при атаках телефонных мошенников, онлайн-мошенников. Все эти случаи должны включаться в страховое покрытие. При этом из покрытия планируется исключить случаи, по которым банки обязаны возмещать средства клиентам по закону «О национальной платежной системе». Это все случаи, когда мошенники похитили средства, используя какие-то технологические приемы, например, без непосредственного участия человека.

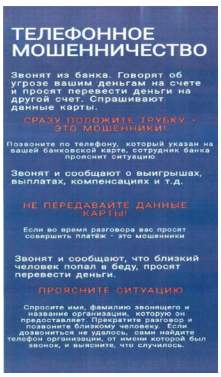
В октябре 2023 года вступил в силу закон об оперативном взаимодействии между Банком России и МВД. Сотрудники полиции получили доступ к базе ФинЦЕРТ, которая в свою очередь пополняется сведениями от МВД. Эти данные помогут банкам эффективнее вести борьбу с мошенническими списаниями средств с банковских карт, в том числе с использованием методов социальной инженерии. Раньше при рассмотрении дел о мошенничестве много времени уходило на запросы данных и переписку между правоохранительными органами и банками. Теперь обмен данными будет проходить оперативно».

В структуре **МВД России** создано специализированное подразделение – **Управление по борьбе с противоправным использованием информационно-коммуникационных технологий**, сотрудниками которого на постоянной основе проводится мониторинг ситуации.

В ходе мониторинга сети устанавливаются Интернет сайты, форумы, закрытые чаты, используемые для организации и реализации вышеуказанных преступных схем.

На информационном ресурсе данного органа можно получить необходимую методическую помощь, а также сообщить о злоумышленниках, распространяющих запрещенную или деструктивную информацию

На сайте **ГУ МВД России по г.Санкт-Петербургу и Ленинградской области** размещён доступный для восприятия тематический видео контент, содержащий как комплекс профилактических мер, так и разъясняющий способы противодействия злоумышленникам. Официальный сайт: www.78.mvd.ru. Аналогичные страницы есть в социальной сети «Вконтакте», https://vk.com/spb_police и в мессенджере «Телеграм», где размещены циклы видео-роликов, связанные со звонками со стороны лиц, действующих от имени служб безопасности банков, приобретением в сети Интернет туристических путевок и приобретением или продажей товаров и услуг на электронных торговых площадках (Авито, Юла и др.).



!!! ПОМНИТЕ !!!
Не существует 100% методик защиты от телефонного и интернет мошенничества.

Если Вы не уверены в правильности своих действий при сомнительных телефонных контактах и интернет-коммуникациях:

1) Не отвечайте на неизвестные Вам номера телефонных вызовов и СМС(ММС) запросов;

2) Не переходите по неизвестным Вам интернет-ссылкам и контактам;

3) Не пользуйтесь интернет соединением, когда он Вам не нужен на смартфоне и компьютере;

4) Не передавайте и не оставляете свои персональные данные на общедоступных ресурсах не проходите сомнительных анкетирований.

ПАМЯТКА
по профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий

К наиболее распространенным видам дистанционных мошенничеств, совершенных на территории г. Санкт-Петербурга и Ленинградской области, относятся:

- «фишинг» – вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

- «фарминг» - процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер, сайты по продаже билетов на ж/д и авиатранспорт и др.);

- «двойная транзакция» (при оплате товаров и услуг продавец сообщает об ошибке, предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций)

- «трэппинг» (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).

I. Основные схемы телефонного мошенничества:

1. Обман по телефону.

Мошенник звонит с незнакомого номера и представляется родственником (знакомым) и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвиняется в совершении того или иного преступления (это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство). Далее в разговор вступает якобы сотрудник правоохранительных органов, который уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перевести на определенный расчетный счет или передать какому-либо человеку. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам, но нередко человек, которому звонит мошенник, сам случайно подсказывает имя того, кому нужна помощь.

Аналогичным образом могут звонить мошенники сотрудникам государственных органов либо предпринимателям и, представляясь, например, руководителем какого-либо государственного органа (правоохранительного, надзорного, контролирующего), под предлогом приезда комиссии проверяющих требуют организовать либо «теплый прием» в форме бесплатного предоставления услуг (питание, подарки, организация отдыха и т.д.), либо перечислить определенную сумму денежных средств на указанный расчетный счет для организации досуга проверяющих или достижения необходимых положительных результатов проверки.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, нужно связаться с его коллегами, друзьями и родственниками для уточнения информации. Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он

правоохранительного органа (другого ведомства). После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

Само требование взятки должностным лицом является преступлением

2. SMS-просьба о помощи.

SMS-сообщения позволяют упростить схему обмана по телефону. Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

На SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

3. Телефонный номер-грабитель.

На телефон приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счета списаны крупные суммы. Существуют сервисы с платным звонком, как правило это развлекательные сервисы, которым услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

Единственный способ обезопасить себя от телефонных мошенников – не звонить по незнакомым номерам.

4.Телефонные вирусы.

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло ММС-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона.

Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

5. Выигрыш в лотерее или какого-либо приза.

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей. На Ваш мобильный телефон – как правило, в ночное время – приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего упоминаются известные иностранные модели и марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации». Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

7. Простой код от оператора связи.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения

связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Перезвонить своему мобильному оператору для уточнения условий, а также узнать какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

9. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

1. Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание

карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

Злоумышленникам нужен лишь номер Вашей карты и ПИН-код, как только Вы их сообщите, деньги будут сняты с Вашего счета.

Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

2. Если Вы утратили карту немедленно ее блокируйте.

3. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

4. Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

5. Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.

6. В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

7. Хищения с карт, подключенных к опции бесконтактных платежей. Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Как обезопасить себя от мошенников:

1. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
2. Не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
3. Используйте пароли не связанные с Вашими персональными данными.
4. Не сообщать данные карты, пароли и другую персональную информацию.
5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.
6. По всем возникающим вопросам обращаться в банк, выдавший карту.
7. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.
8. Не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.
9. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки).
10. Не перезванивать по номерам которые приходят на e-mail или по SMS.

Будьте бдительны!

Издание **«Вестник Бахилово»** 6+
№12 (328), 4 апреля 2025 г.

Учредитель: Администрация сельского поселения Бахилово муниципального района Ставропольский Самарской области.

Главный редактор: Гвоздева Юлия Владимировна.

Адрес издателя, редакции, типографии:
445020, РФ, Самарская область, г. Тольятти, ул. Ленинградская, 16, оф. 309. Тел. 37-80-07.
Тираж — 30 экз. **Бесплатно.**