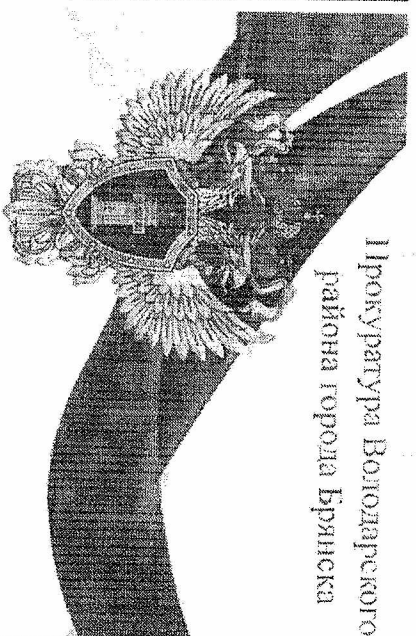


Схемы мошеннических действий в социальных сетях

Ежегодно в России ущерб от кибермошенников составляет десятки миллиардов рублей. Попадаются на уловки не только пожилые люди, но и молодежь, независимо от статуса и образования. Киберпреступления составляют половину от всех других преступлений, и, несмотря на все способы борьбы, мошенники продолжают наживаться на простых людях.

Одной из распространённых схем является использование злоумышленниками поддельных аккаунтов в социальных сетях и мессенджерах для связи с сотрудниками организаций. Указанные аккаунты содержат реальные данные руководителей (фамилия, имя, отчество, фото и т.п.) и выглядят максимально достоверно. Во всех случаях преступники действуют примерно по сходным сценариям. Сотрудник организации получает сообщение в социальной сети, мессенджере или по электронной почте якобы от своего руководителя. При этом злоумышленник обращается к сотруднику, используя его имя и отчество, чтобы вызвать доверие. В процессе общения злоумышленник предлагает о последующем телефонном звонке из какой-либо организации или правоохранительных органов и просит сотрудника организации никому о нем не сообщать, а после завершения — отчитаться о результатах разговора. После этого сотруднику организации поступает звонок, в ходе которого у него могут запрашивать различную конфиденциальную информацию и вынуждать совершать противоправные действия в пользу злоумышленников. Продолжая совершенствовать методы социальной инженерии, злоумышленники в ряде случаев проводят предварительную разведку и используют информацию о потенциальных жертвах, чтобы вызвать доверие.



Прокуратура Володарского
района города Брянска

«КАК НЕ СТАТЬ ПРЕСТУПНИКОМ В СОЦИАЛЬНЫХ СЕТЯХ»

Информационно-справочный буклет



В приведённом примере злоумышленники используют доверие сотрудников организаций к непосредственному руководителю и страх столкнуться с последствиями отказа выполнить его требования. С поддельных аккаунтов злоумышленниками рассылаются сообщения также и в адрес руководителей и работников других организаций с целью получения контактных данных лиц, необходимых мошенникам для дальнейшего взаимодействия и совершения противоправных действий.

Ещё одной из распространённых мошеннических схем является рассылка в социальных сетях и мессенджерах сообщений с предложением протолосовать по различным темам (участие в конкурсе, выбор музыкальной композиции, фильма и т.п.), содержащих ссылку, после перехода по которой легальный аккаунт пользователя перехватывается злоумышленниками. В этом случае необходимо при восстановлении доступа к аккаунту использовать платные механизмы социальной сети и мессенджера. Один из новых способов — дипфейки. Человек получает видеосообщение от родственника или знакомого, который просит денег в долг. Но на деле это оказывается созданное с помощью нейросети видео. Отличить его от оригинала могут не все, и те, кто не отличил, переводят деньги на счёт преступникам. В последнее время эта схема стала применяться все чаще.

Сейчас одним из распространённых способов обмана является хищение денег через токенизированные, то есть виртуальные банковские карты. Люди под воздействием мошенников привязывают к своему телефону чужую карту и потом через банкомат вносят на неё деньги.

Одним из самых популярных у кибермошенников приёмов — получение доступа к аккаунтам людей на Госуслугах.

Одна из наиболее распространенных схем кражи учетных записей — создание копии официального сайта социальной сети. Дизайны и URL-адрес поддельного сайта копируют официальный: многие с трудом могут распознать обман. Обычно злоумышленники пытаются заставить пользователей перейти по фишинговой ссылке, чаще всего отправленной по SMS от имени известных компаний, чтобы вызвать у жертвы доверие.

Еще один способ завладеть аккаунтами пользователей — заражение компьютера вредоносным ПО. Благодаря такой схеме кибермошенники получают доступ к роутеру жертвы, а уже чего подменяют домены социальных сетей таким образом, чтобы, пытаясь зайти на официальный сайт соцсети, пользователи попадали на заранее выбранную мошенниками страницу.

Как не стать жертвой?

1. Не ищите легких денег
В интернете нет легкого заработка. Дать вам миллион сразу обещают только мошенники. Лучше всего игнорировать объявления о заработках без вложений и сразу добавлять в черный список. Обычно таким способом пытаются заманить в финансовые пирамиды или мошеннические сети.

2. Не верьте странным сообщениям от друзей или родственников
Каждый сталкивался с получением SMS от родственников или друзей с просьбой о займе денег. Многие, сильно доверчивые люди, ведутся на уловки и переводят значительные суммы. Узнать мошенников можно — если вам говорят, что человек оказался за городом, без денег, без карты, у него изменился телефон и так далее, то лучше сначала позвоните ему и уточните, действительно ли это не фейк.

3. Подключайте VPN в незнакомых местах

С помощью локальной сети мошенники часто воруют личную информацию из социальных сетей или компьютера. Аферисты запросто могут подключиться к вашему ноутбуку или телефону, и скачать ваши фото/переписки, после чего начать шантажировать. Поэтому, лучше включать VPN в незнакомых для вас местах.

4. Придумайте надежный пароль

У многих пароли в социальных сетях не меняются по несколько лет. Есть и те, у кого один код на все времена, но так лучше не делать. В качестве пароля вы можете выбрать заглавные и прописные буквы, цифры и латиницу. Проще восстановить пароль, чем вернуть украденные деньги.

5. Не переходите по странным ссылкам

Вам могут написать с ненастоящего аккаунта или с профиля знакомого с просьбой перейти по ссылке и как можно быстрее. Кроме того, мошенники часто заманивают жертву с помощью упоминания в записке сообщества. Например, это может быть ссылка на фальшивый выигрыш. Если вы когда-либо размещали объявления на Avito, то мошенники могут включить ваш номер в SMS-рассылку. Лучше перепроверять непосредственно в приложении.

6. Покупка вещей

Чтобы не нарваться на мошенников, лучше не покупать товары с левых сайтов. Находите официальные интернет-страницы представителей брендов и заказывайте через них. Распознать афериста просто — он будет просить предоплату прямо на карту. В случае с реальным магазином, вы оплачиваете покупку и деньги списываются сразу, напрямую переходя в магазин.

7. Не доверяйте сотрудникам банка, которые просят какие-либо пароли
Часто мошенники звонят со знакомого номера — 900. В 99% случаев банк вам звонить не будет. Он просто не будет производить операцию, которую

вы осуществили и попросит вас повторно подтвердить ее.

Что делать, если все-таки наварались на мошенников? Если вдруг вы заподозрили, что стали жертвой мошенничества, то немедленно позвоните в банк и заблокируйте карту. После этого лучше сообщить о мошенниках, даже в том случае, если подозрительных активностей не было, но вы назвали номер своей карты. Банки могут отреагировать по-разному. В какое-то учреждение можно просто позвонить или написать, а в какое-то придется ехать.

Что делать, если Вы или Ваши близкие все-таки стали жертвами мошенников

Даже если Вас или Ваших близких обманули мошенники — обращайтесь в органы внутренних дел с заявлением. В заявлении следует максимально подробно изложить все обстоятельства произошедшего.

Адрес и телефоны прокуратуры Володарского района города Брянска: 241020, г. Брянск, ул. Пушкина, д. 33, тел. +7(4832) 26-11-38

Адрес и телефоны УМВД России по Брянской области: 241001, г. Брянск, ул. Советская, д. 102, тел. Дежурной части +7(4832) 66-70-90, телефон доверия +7(4832) 72-22-33; телефон полиции — 02, с мобильных любых операторов - 102

Будьте бдительны! Предупредите своих родственников и знакомых, не поддавайтесь на уловки мошенников!

Одна из наиболее распространенных схем кражи учетных записей — создание копии официального сайта социальной сети. Дизайн и URL-адрес поддельного сайта копируют официальные; многие с трудом могут распознать обман. Обычно злоумышленники пытаются заставить пользователей перейти по фишинговой ссылке, чаще всего отправленной по СМС от имени известных компаний, чтобы вызвать у жертвы доверие. Еще один способ завладеть аккаунтами пользователей — заражение компьютера вредоносным ПО. Благодаря такой схеме кибермошенники получают доступ к роутеру жертвы, а уже чето подменяют домены социальных сетей таким образом, чтобы, пытаясь зайти на официальный сайт соцсети, пользователи попадали на заранее выбранную мошенниками страницу.	3. Подключайте VPN в публичных местах С помощью локальной сети мошенники часто воруют личную информацию из социальных сетей или компьютера. Аферисты запросы могут подключиться к вашему ноутбуку или телефону, и скачать ваши фото/переписки, после чего начать шантажировать. Поэтому, лучше включать VPN в публичных местах. 4. Придумайте надежный пароль У многих пароли в социальных сетях не меняются по несколько лет. Есть и те, у кого один код на все времена, но так лучше не делать. В качестве пароля вы можете выбрать заглавные и прописные буквы, цифры и латиницу. Проще восстановить пароль, чем вернуть украденные деньги.	вы осуществили и попросит вас повторно подтвердить ее. Что делать, если все-таки навались на мошенников? Если вдруг вы заподозрили, что стали жертвой мошенничества, то немедленно позвоните в банк и заблокируйте карту. После этого лучше сообщить о мошенниках, даже в том случае, если подозрительных активностей не было, но вы назвали номер своей карты. Банки могут отреагировать по-разному. В какое-то учреждение можно просто позвонить или написать, а в какое-то придется ехать.
1. Не ищите легких денег В интернете нет легкого заработка. Дать вам миллион сразу обещают только мошенники. Лучшее всего информировать объявления о заработках без вложений и сразу добывать в черный список. Обычно таким способом пытаются заманить в финансовые пирамиды или мошеннические сети. 2. Не верьте странным сообщениям от друзей или родственников Каждый сталкивался с получением SMS от родственников или друзей с просьбой о займе денег. Многие, сильно доверчивые люди, ведутся на уловки и переводят значительные суммы. Узнать мошенников можно — если вам говорят, что человек оказался за городом, без денег, без карты, у него изменился телефон и так далее, то лучше сначала позвоните ему и уточните, действительно ли это не фейк.	5. Не переходите по странным ссылкам Вам могут написать с ненастоящего аккаунта или с профиля знакомого с просьбой перейти по ссылке и как можно быстрее. Кроме того, мошенники часто заманивают жертву с помощью упоминания в записи сообщества. Например, это может быть ссылка на фальшивый выигрыш. Если вы когда-либо размещали объявления на Avito, то мошенники могут вложить ваш номер в SMS-рассылку. Лучше переписываться непосредственно в приложении. 6. Покупка вещей Чтобы не нарваться на мошенников, лучше не покупать товары с левых сайтов. Находите официальные интернет-страницы поставщиков брендов и заказывайте через них. Распознать афериста просто — он будет просить предоплату прямо на карту. В случае с реальным магазином, вы оплачиваете покупку и деньги списываются сразу, напрямую переходя в магазин. 7. Не доверяйте сотрудникам банка, которые просят какие-либо пароли Часто мошенники звонят со знакомого номера — 900. В 99% случаев банк вам звонить не будет. Он просто не будет производить операцию, которую	Что делать, если Вы или Ваши близкие все-таки стали жертвами мошенников Даже если Вас или Ваших близких обманули мошенники — обращайтесь в органы внутренних дел с заявлением. В заявлении следует максимально подробно изложить все обстоятельства произошедшего. Адрес и телефоны прокуратуры Болодарского района города Брянска: 241020, г. Брянск, ул. Пушкина, д. 33, тел. +7(4832) 26-11-38 Адрес и телефоны УМВД России по Брянской области: 241001, г. Брянск, ул. Советская, д.102, тел. Дежурной части +7(4832) 66-70-90, телефон доверия +7(4832) 72-22-33; телефон полиции — 02, с мобильных любых операторов - 102 Будьте бдительны! Предупредите своих родственников и знакомых, не поддавайтесь на уловки мошенников!

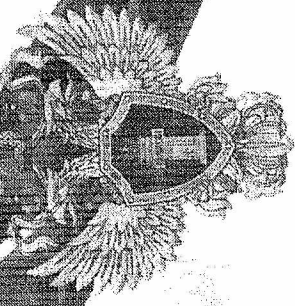
Схемы мошеннических действий в социальных сетях

Ежегодно в России ущерб от кибермошенников составляет десятки миллиардов рублей. Попадают на уловки не только пожилые люди, но и молодежь, независимо от статуса и образования. Киберпреступления составляют половину от всех других преступлений, и, несмотря на все способы борьбы, мошенники продолжают наживаться на простых людях.

Одной из распространённых схем является использование злоумышленниками поддельных аккаунтов в социальных сетях и мессенджерах для связи с сотрудниками организаций. Указанные аккаунты содержат реальные данные руководителей (фамилия, имя, отчество, фото и т.п.) и выглядят максимально достоверно. Во всех случаях преступники действуют примерно по сходным сценариям. Сотрудник организации получает сообщение в социальной сети, мессенджере или по электронной почте якобы от своего руководителя. При этом злоумышленник обращается к сотруднику, используя его имя и отчество, чтобы вызвать доверие. В процессе общения злоумышленник предупреждает о последующем телефонном звонке из какой-либо организации или правоохранительных органов и просит сотрудника организации никому о нем не сообщать, а после завершения — отчитаться о результатах разговора. После этого сотрудник организации поступает звонок, в ходе которого у него могут запрашивать различную конфиденциальную информацию и вынуждать совершать противоправные действия в пользу злоумышленников.

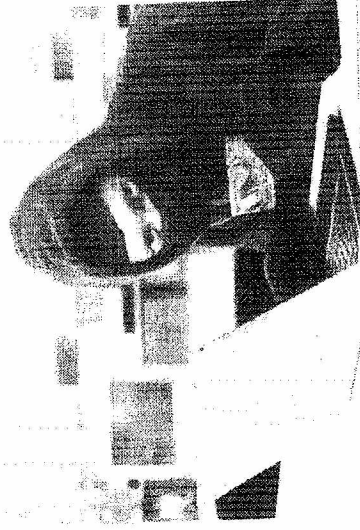
Продолжая совершенствовать методы социальной инженерии, злоумышленники в ряде случаев проводят предварительную разведку и используют информацию о потенциальных жертвах, чтобы вызвать доверие.

Прокуратура Володарского
района города Брянска



«КАК НЕ СТАТЬ ПРЕСТУПНИКОМ В СОЦИАЛЬНЫХ СЕТЯХ»

Информационно-справочный буклет



В приведённом примере злоумышленники используют доверие сотрудников организаций к непосредственному руководителю и страх столкнуться с последствиями отказа выполнить его требования. С поддельных аккаунтов злоумышленниками рассылаются сообщения также и в адрес руководителей и работников других организаций с целью получения контактных данных лиц, необходимых мошенникам для дальнейшего взаимодействия и совершения противоправных действий.

Ещё одной из распространённых мошеннических схем является рассылка в социальных сетях и мессенджерах сообщений с предложением проголосовать по различным темам (участие в конкурсе, выбор музыкальной композиции, фильма и т.п.), содержащих ссылку, после перехода по которой легальный аккаунт пользователя перехватывается злоумышленниками. В этом случае необходимо при восстановлении доступа к аккаунту использовать штатные механизмы социальной сети и мессенджера. Один из новых способов — дипфейки. Человек получает видеосообщение от родственника или знакомого, который просит денег в долг. Но на деле это оказывается созданное с помощью нейросети видео. Отличить его от оригинала могут не все, и те, кто не отличил, переводят деньги на счёт преступникам. В последнее время эта схема стала применяться все чаще.

Сейчас одним из распространённых способов обмана является хищение денег через токенизированные, то есть виртуальные банковские карты. Люди под воздействием мошенников привязывают к своему телефону чужую карту и потом через банкомат вносят на нее деньги. Один из самых популярных у кибермошенников приемов — получение доступа к аккаунтам людей на Госуслугах.

Типовые схемы телефонного

мошенничества:

Жертвам поступают звонки от имени операторов связи и под предлогом необходимости продления договора обслуживания, или в связи с вынужденной сменой абонентского номера просят сообщить данные паспорта или номера СНИЛС.

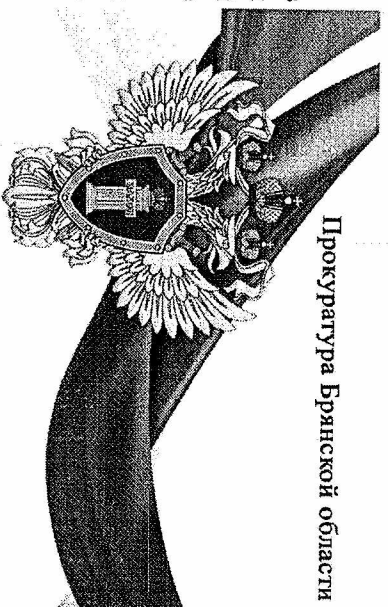
Спустя непродолжительный период времени гражданам поступают звонки от имени сотрудников правоохранительных органов, сервиса «Госуслуги», которые сообщают недостоверные сведения о совершенном ими преступлении («государственной измене»), финансировании противоправной деятельности или попытках оформления кредита на основании ранее сообщенных данных.

В ходе общения преступники выясняют у жертв наличие у них денежных средств. Затем, действуя от имени представителей Центробанка предлагают в целях подтверждения правомерного выдачи ими «задекларировать» денежные средства, путем их передачи «курьеру» или осуществить их перевод на «безопасный счет», уверяя при этом вернуть в течение непродолжительного периода времени.

Также мошенники в ходе телефонных разговоров представляются работниками почты и сообщают потерпевшим сведения о поступлении заказного письма.

Затем жертва по указанию злоумышленников, используя приложение «Почта России», по предоставленному ему трек-номеру обнаруживает наличие почтового отправления на его имя, но по вымышленному адресу.

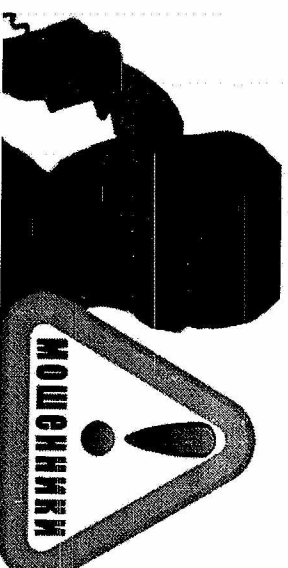
В этот же день на адрес электронной почты гражданина поступает «фейковое» уведомление от



Прокуратура Брянской области

#КладитТрубку

Информационно-справочный буклет



БРЯНСК

2026

имени портала «Госуслуги», в котором указано, что в его личный кабинет осуществлен неправомерный доступ, в связи с чем необходимо связаться с оператором «горячей линии» по указанному номеру телефона, после звонка на который, пострадавшему сообщают, что у него похищены личные документы и необходимо продолжить общение в интернет-мессенджере.

Впоследствии жертве сообщают недостоверные сведения о совершении в отношении нее противоправных действий и убеждают перевести имевшиеся денежные средства на «безопасный счет».

В ходе телефонных разговоров злоумышленники представляются сотрудниками правоохранительных органов и сообщают гражданам недостоверные сведения о совершенном ими или их родственниками преступлениях (порожнотранспортных происшествий, финансировании незаконных вооруженных формирований и т.д.). При этом в ходе общения выясняют у жертвы наличие денежных средств, а также не представляли возможности позвонить своим родным под различным предлогом.

После чего предлагают передать денежные средства через своих сотрудников – курьеров или водителей за непривлечение к уголовной ответственности, а также для возмещения причиненного вреда.

!!! Необходимо помнить, что представители органов государственной власти в ходе общения с гражданами не выясняют сведения о наличии у них денежных средств, а тем более не требуют подтверждений правомерности их владения !!!

В сети «Интернет» размещаются объявления о **продаже автомобилей, дачи, другого имущества** («Авто ру», «Авито» и т.д., а также в различных социальных сетях). Подробно описывается товар, выкладываются его фотографии и все это по очень привлекательной цене. Низкую стоимость злоумышленники объясняют вполне различными жизненными ситуациями. Желаяшему приобрести товар предлагается внести задаток, поскольку на него нашлось множество покупателей или продавец находится за пределами города или даже страны, но готов вылететь для оформления сделки. Деньги злоумышленники просят перечислить переводом через банк либо на абонентский номер телефона.

Также в интернет-мессенджерах размещаются объявления об оказании содействия в получении дополнительного заработка («пассивного дохода») - путем инвестирования на рынках ценных бумаг и «криптовиржах», для участия в котором необходимо совершить переводы денежных средств.

Получив желаемое, мошенники отключают телефон и на связь с обманутой жертвой больше не выходят.

!!! Для совершения каждого из подобных преступлений используются абонентские номера и банковские карты, полученные мошенниками с нарушением требований действующего законодательства.

При этом с 2025 года за участие в подобной деятельности на территории Российской Федерации введена уголовная ответственность !!!

Как не стать обманутым:

- не давать свой телефон кому-либо постороннему с целью позвонить (якобы у незнакомца закончились деньги на телефоне);
- никогда и ни при каких обстоятельствах никому не сообщать свои персональные данные или конфиденциальную информацию: паспортные данные, PIN-код, CVV-код и другие реквизиты банковской карты, номер счета, логин и пароль от страниц в социальных сетях, на интернет-сайтах и прочее, личного кабинета на «Госуслугах»;

- задавать вопросы. Если звонящий представляется сотрудником полиции, банка, доктором поликлиники, страховым агентом, первое, что необходимо сделать, попытаться узнать как можно больше информации о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации, как найти официальный сайт, как и откуда узнал номер телефона и прочее, в том числе упоминание об уголовной ответственности за мошенничество, настоящего сотрудника не смутят, а мошенников заставят занервничать. При этом говорить необходимо негромким спокойным голосом, чтобы обманщик понял, что его разоблачили;

- не переходить по ссылкам, якобы присылаемым от банка;
- не спешить переводить или отдавать деньги.

Требование внести денежную сумму, например, в качестве залога при розыгрыше призов или пополнить «контрольный» счет банка должно сразу насторожить;

- не откликаться на просьбу положить на счет деньги, так как по ошибке человек перевел деньги на Ваш номер;

- не перезванивать на номер, если он не знаком (если звонить оператору банка – то на номер, указанный на обороте банковской карты);

- закончить разговор в тот момент, когда только возникнет подозрение, что Вами пытаются манипулировать.

Что делать, если Вы или Ваши близкие все-таки стали жертвами

мошенников:

Даже если Вас или Ваших близких обманули мошенники – обращайтесь в органы внутренних дел с заявлением. В заявлении следует максимально подробно изложить все обстоятельства произошедшего. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника и в Ваш банк. Принятие оператором и банком экстренных мер может позволить заблокировать перевод и вернуть деньги.

Адрес и телефоны прокуратуры Брянской области: 241023, г. Брянск, ул. А.М. Рекунова, д.1; телефон +7 (4832) 65-42-05, +7 (4832) 65-42-06.

Адрес и телефоны УМВД России по Брянской области: 241001, г. Брянск, ул. Советская, д. 102, тел. дежурной части +7 (4832) 66-70-90, телефон доверия +7 (4832) 72-22-33; телефон полиции – 02, с мобильных любых операторов – 102.

В сети «Интернет» размещаются объявления о **продаже автомобилей, дачи, другого имущества** («Авто ру», «Авито» и т.д., а также в различных социальных сетях). Подробно описывается товар, выкладываются его фотографии и все это по очень привлекательной цене. Низкую стоимость злоумышленники объясняют вполне различными житейскими ситуациями. Желающему приобрести товар предлагается внести задаток, поскольку на него нашлось множество покупателей или продавец находится за пределами города или даже страны, но готов вылететь для оформления сделки. Деньги злоумышленники просят перечислить переводом через банк либо на абонентский номер телефона.

Также в интернет-мессенджерах размещаются объявления об оказании содействия в получении дополнительного заработка («пассивного дохода») - путем инвестирования на рынках ценных бумаг и «криптовбиржах», для участия в котором необходимо совершить переводы денежных средств.

Получив желаемое, мошенники отключают телефон и на связь с обманутой жертвой больше не выходят.

!!! Для совершения каждого из подобных преступлений используются абонентские номера и банковские карты, полученные мошенниками с нарушением требований действующего законодательства.

При этом с 2025 года за участие в подобной деятельности на территории Российской Федерации введена уголовная ответственность !!!

Как не стать обманутым:

- не давать свой телефон кому-либо постороннему с целью позвонить (якобы у знакомого закончились деньги на телефоне);
- никогда и ни при каких обстоятельствах никому не сообщать свои персональные данные, конфиденциальную информацию: паспортные данные, PIN-код, CVV-код и другие реквизиты банковской карты, номер счета, логин и пароль от страниц в социальных сетях, на интернет-сайтах и прочее, личного кабинета на «Госуслугах»;
- задавать вопросы. Если звонящий представляется сотрудником полиции, банка, доктором поликлиники, страховым агентом, первое, что необходимо сделать, попытаться узнать как можно больше информации о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации, как найти официальный сайт, как и откуда узнал номер телефона и прочее, в том числе упоминание об уголовной ответственности за мошенничество, настоящего сотрудника не смутят, а мошенников заставят занервничать. При этом говорить необходимо негромким спокойным голосом, чтобы обманщик понял, что его разоблачили;
- не переходить по ссылке, якобы присылаемым от банка;
- не спешить переводить или отдавать деньги. Требование внести денежную сумму, например, в качестве залога при розыгрыше призов или пополнить «контрольный» счет банка должно сразу насторожить;

- не откликаться на просьбу положить на счет деньги, так как по ошибке человек перевел деньги на Ваш номер;

- не перезванивать на номер, если он не знаком (если звонить оператору банка – то на номер, указанный на обороте банковской карты);

- закончить разговор в тот момент, когда только возникнет подозрение, что Вами пытаются манипулировать.

Что делать, если Вы или Ваши близкие все-таки стали жертвами мошенников:

Даже если Вас или Ваших близких обманули мошенники – обращайтесь в органы внутренних дел с заявлением. В заявлении следует максимально подробно изложить все обстоятельства произошедшего. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника и в Ваш банк. Принятие оператором и банком экстренных мер может позволить заблокировать перевод и вернуть деньги.

Адрес и телефоны прокуратуры Брянской области: 241023, г. Брянск, ул. А.М. Рекунова, д.1; телефон +7 (4832) 65-42-05, +7 (4832) 65-42-06.

Адрес и телефоны УМВД России по Брянской области: 241001, г. Брянск, ул. Советская, д. 102, тел. дежурной части +7 (4832) 66-70-90, телефон доверия +7 (4832) 72-22-33; телефон полиции – 02, с мобильных любых операторов – 102.

Типовые схемы телефонного мошенничества:

Жертвам поступают звонки от имени операторов связи и под предлогом необходимости продления договора обслуживания, или в связи с вынужденной сменой абонентского номера просят сообщить данные паспорта или номера СНИЛС.

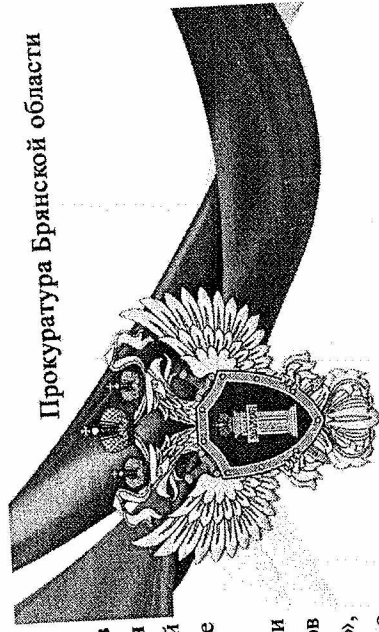
Спустя непродолжительный период времени гражданам поступают звонки от имени сотрудников правоохранительных органов, сервиса «Госуслуги», которые сообщают недостоверные сведения о совершенном ими преступлении («государственной измене»), финансировании противоправной деятельности или попытках оформления кредита на основании ранее сообщенных данных.

В ходе общения преступники выясняют у жертв наличие у них денежных средств. Затем, действуя от имени представителей Центробанка предлагают в целях подтверждения правомерного владения ими «задекларировать» денежные средства, путем их передачи «курьеру» или осуществить их перевод на «безопасный счет», уверяя при этом вернуть в течение непродолжительного периода времени.

Также мошенники в ходе телефонных разговоров представляют себя работниками почты и сообщают потерпевшим сведения о поступлении заказного письма.

Затем жертва по указанию злоумышленников, используя приложение «Почта России», по предоставленному ему трек-номеру обнаруживает наличие почтового отправления на его имя, но по вымышленному адресу.

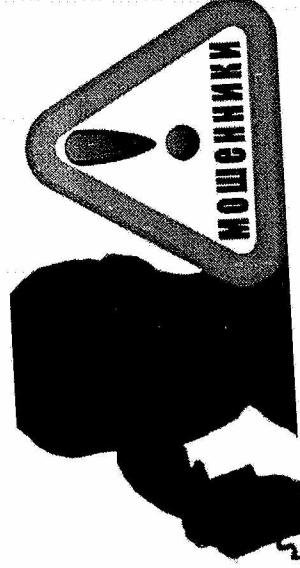
В этот же день на адрес электронной почты гражданина поступает «фейковое» уведомление от



Прокуратура Брянской области

#КладиТрубку

Информационно-справочный буклет



БРЯНСК

2026

имени портала «Госуслуги», в котором указано, что в его личный кабинет осуществлен неправоммерный доступ, в связи с чем необходимо связаться с оператором «горячей линии» по указанному номеру телефона, после звонка на который, пострадавшему сообщают, что у него похищены личные документы и необходимо продолжить общение в интернет-мессенджере.

Впоследствии жертве сообщают недостоверные сведения о совершении в отношении нее противоправных действий и убеждают перевести имевшиеся денежные средства на «безопасный счет».

В ходе телефонных разговоров злоумышленники представляют себя сотрудниками правоохранительных органов и сообщают гражданам недостоверные сведения о совершенном ими или их родственниками преступлениях (дорожно-транспортных происшествий, финансировании незаконных вооруженных формирований и т.п.). При этом в ходе общения выясняют у жертвы наличие денежных средств, а также не предоставляют возможности позвонить своим родным под различным предлогом.

После чего предлагают передать денежные средства через своих сотрудников – курьеров или водителей за непривлечение к уголовной ответственности, а также для возмещения причиненного вреда.

!!! Необходимо помнить, что представители органов государственной власти в ходе общения с гражданами не выясняют сведения о наличии у них денежных средств, а тем более не требуют подтверждения правомерности их владения !!!