«Основные способы мошенничеств, совершенных с применением информационно-коммуникационных технологий»

МВД по Республике Бурятия

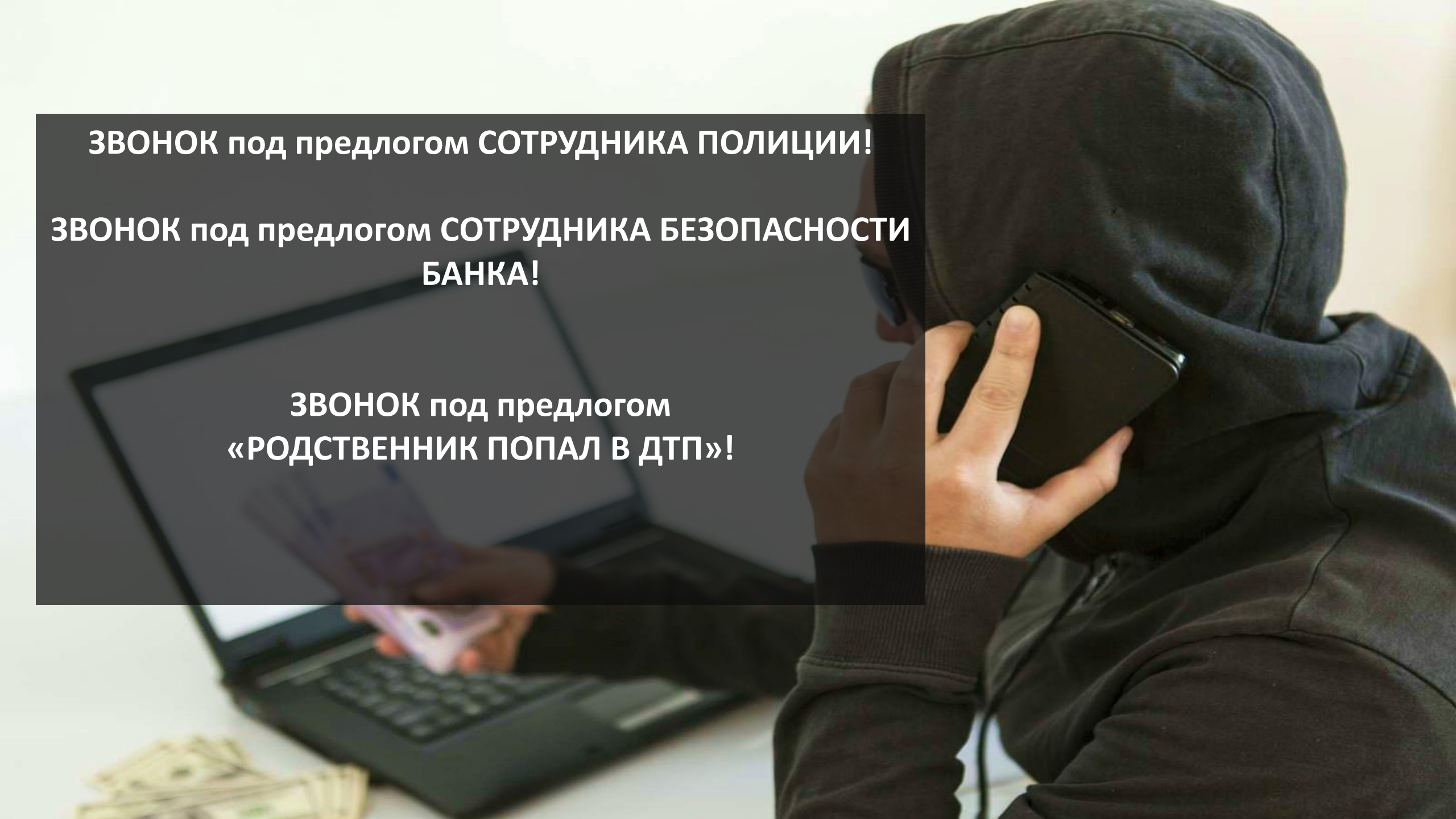
1. Телефонные мошенничества –
мошенничества с использованием средств сотовой связи, совершающиеся путем сообщения гражданам заведомо ложной информации.

2. Кибермошенничества –
вирусное заражение смартфона для получения доступа к данным, системам онлайн банкинга для последующего похищения денежных средств со счета.

3. Мошенничества, совершаемые в сети интернет –
мошенничества при покупках или продажах через сеть Интернет (онлайн магазины, соц.сети), оказание услуг, а также финансовые пирамиды, фиктивные инвестиции.

Телефонное мошенничество:

Обман в ходе телефонного разговора



ЗВОНОК под предлогом СОТРУДНИКА ПОЛИЦИИ!

ЗВОНОК под предлогом СОТРУДНИКА БЕЗОПАСНОСТИ БАНКА!

ЗВОНОК под предлогом «РОДСТВЕННИК ПОПАЛ В ДТП»!

ФОРМУЛА УСПЕХА ТЕЛЕФОННЫХ МОШЕННИКОВ

эффект неожиданности

+

яркие эмоции

+

психологическое давление, паника

+

актуальная тема

Увы, мы готовы сделать ВСЁ, что просят от нас мошенники

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ОТРИЦАТЕЛЬНЫЕ

- СТРАХ ПАНИКА
- ЧУВСТВО СТЫДА

«Вы выиграли крупную сумму денег»

«Вам положены социальные выплаты»

«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере…»

«С вашего счета списали все деньги»

«Ваш родственник попал в аварию и сбил человека»

«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела»

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

1. Не отвечайте
на звонки с незнакомых номеров

2. Прервите разговор
Если он касается финансовых вопросов

3. Не торопитесь
принимать решение

4. Проверьте информацию в Интернете
или обратитесь за помощью к близким родственникам

5. Не перезванивайте
по незнакомым номерам

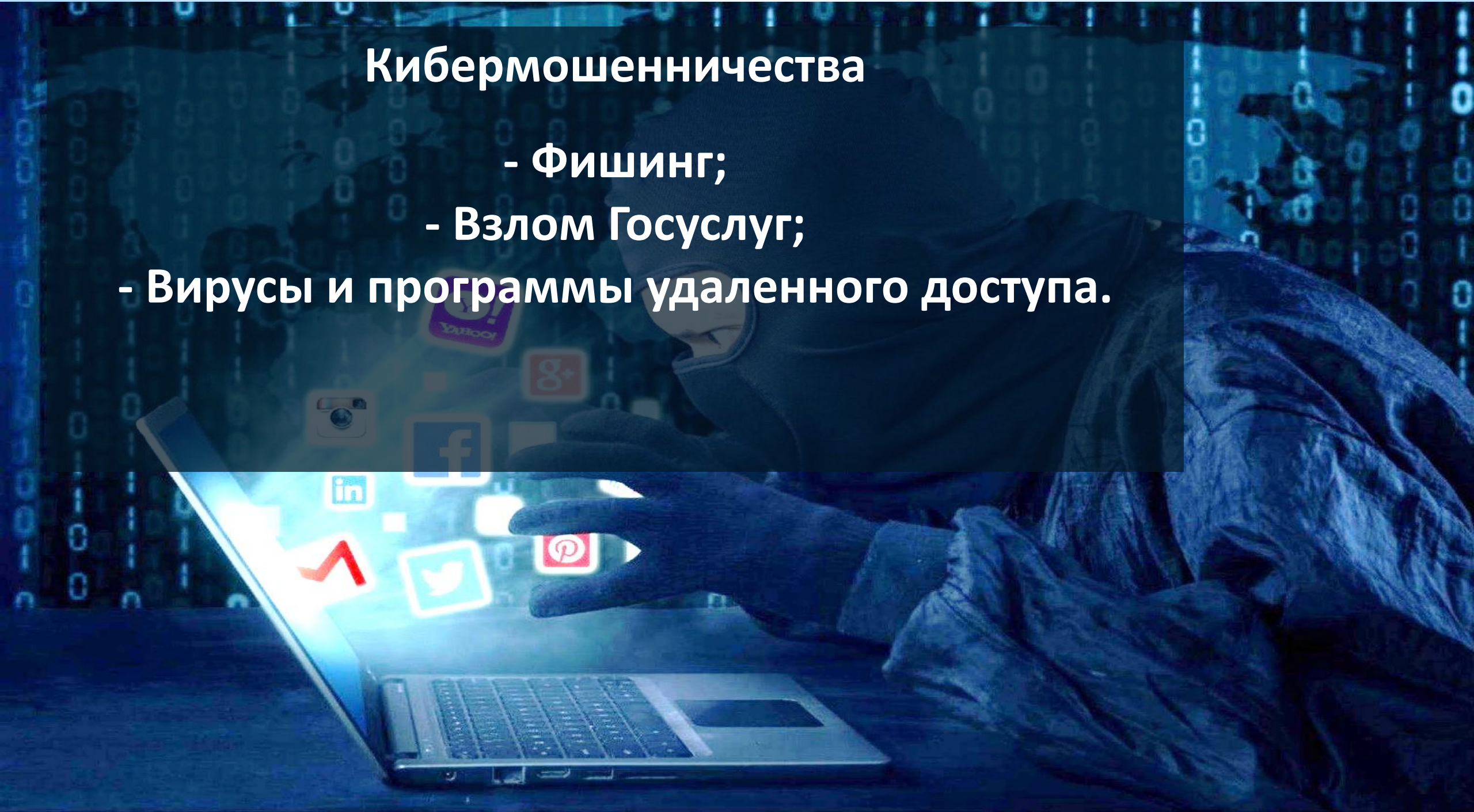
6. Самостоятельно позвоните
близкому человеку /в банк / в организацию

7. Не сообщайте
CVV/CVC и иные
данные банковских карт

Возьмите паузу и спросите совета у родных и друзей!

Кибермошенничества

- Фишинг;
- Взлом Госуслуг;
- Вирусы и программы удаленного доступа.



ФИШИНГ

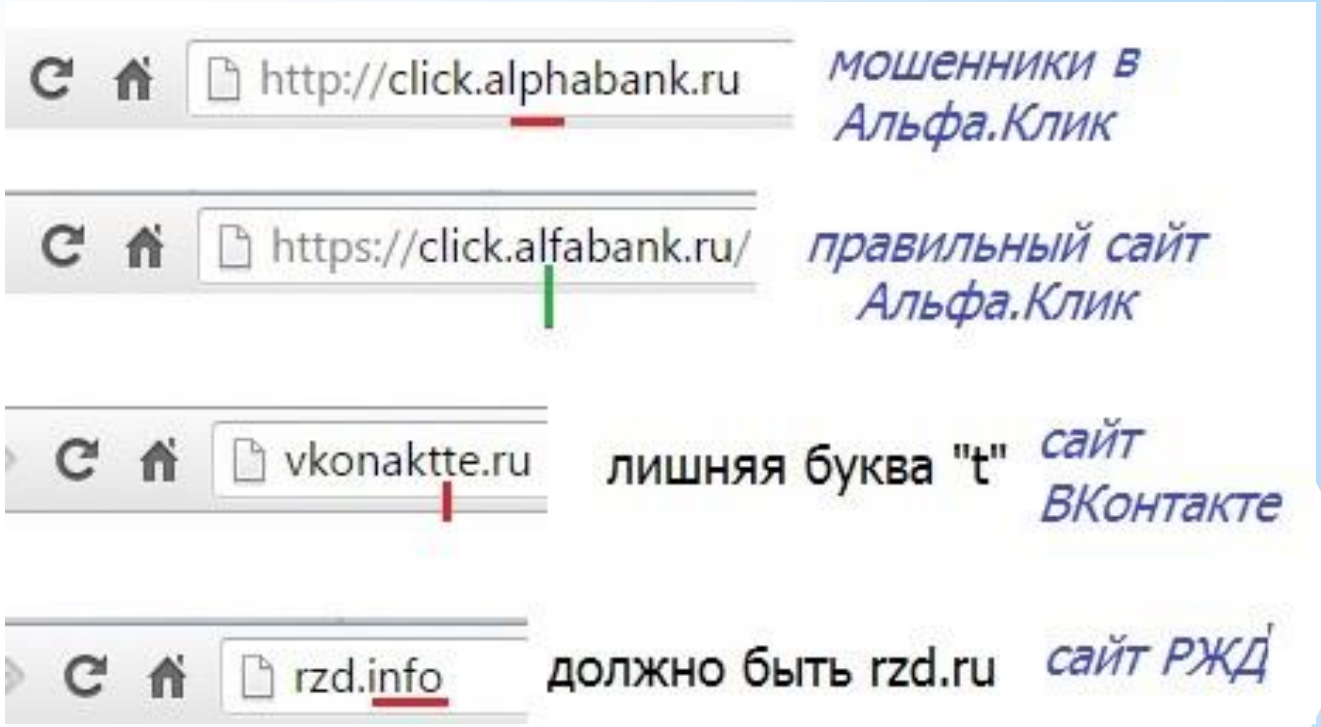
Мошенники создают сайты двойники с целью:

- Списания денег путем выманивания у жертв банковских сведений для совершения ПЛАТЕЖЕЙ/ПЕРЕВОДОВ;
- Взлома аккаунтов социальных сетей, портала Госуслуг и др.;
- Заражения устройств жертвы «Вирусом».

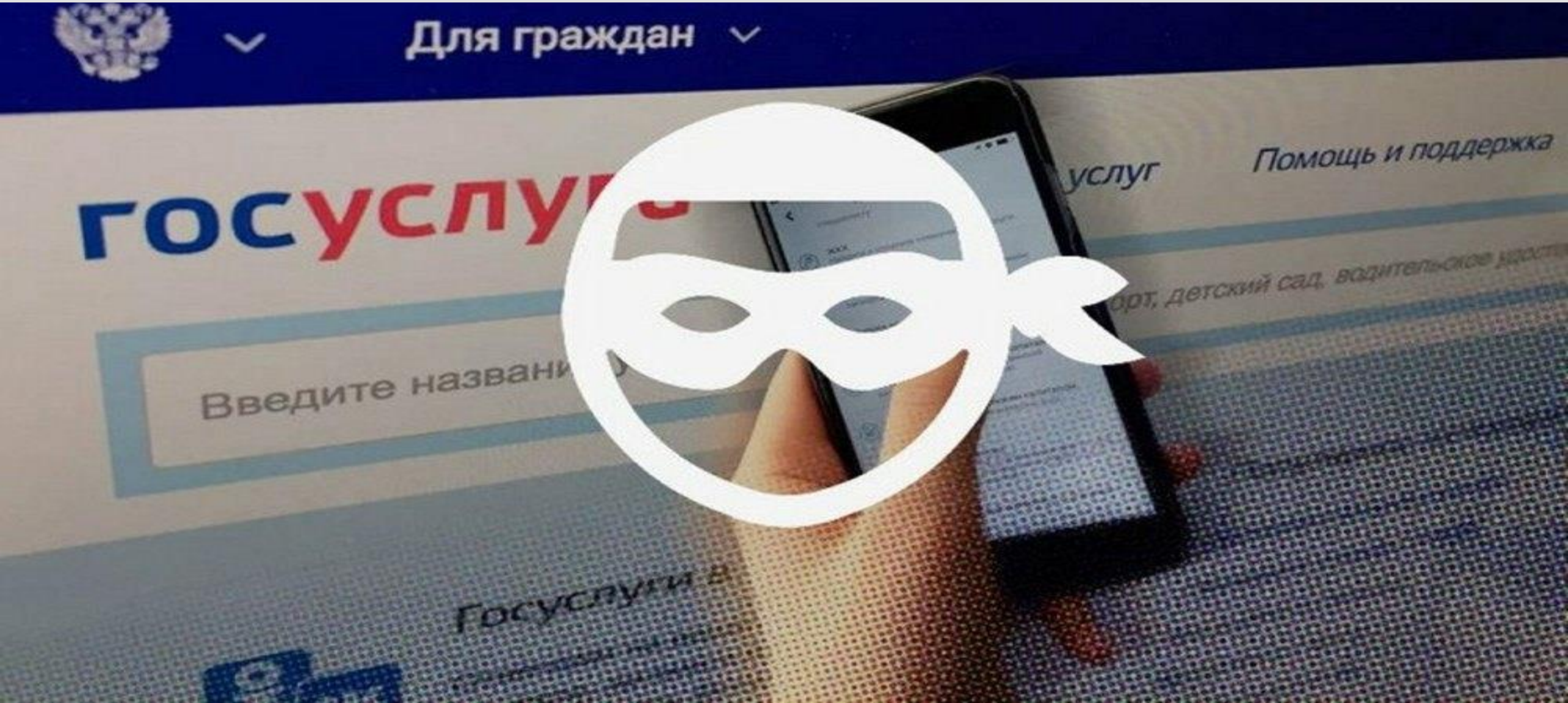
КАК РАСПОЗНАТЬ САЙТ ДВОЙНИК

- **ПРИ ПРОВЕРКЕ ОБРАТИТЕ ВНИМАНИЕ НА ДОМЕН (ИМЯ) САЙТА:**

- **Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I» (onL1ne вместо onLIne);**
- **Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);**
- **В некоторых случаях для написания домена используются буквы похожие на латинские из алфавита другого языка;**
- **Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU**



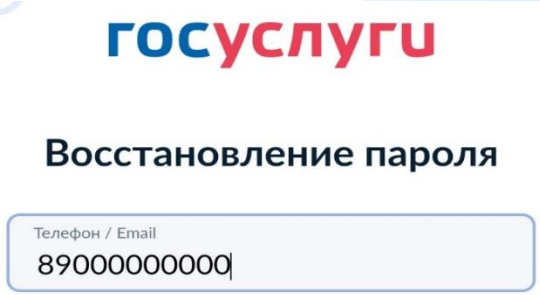
Взлом личного кабинета Госуслуг



Как мошенники получают доступ к Госуслугам

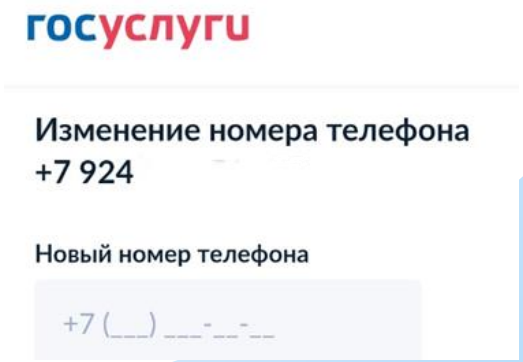
- **Телефонный звонок от «оператора сотовой связи». -Сообщают что необходимо продлить срок действия сим-карты или обновить паспортные данные.**
- **Телефонный звонок от «сотрудника портала Госуслуг». -Сообщают о подозрительной активности.**
- **В целях подтверждения личности, а так же под другим предлогом требуют сообщить/продиктовать СМС-код который поступит на телефон с портала Госуслуг.**

- **В ЭТО ВРЕМЯ мошенники зная абонентский номер жертвы. На сайте Госуслуг открывают вкладку: «Восстановление пароля».**



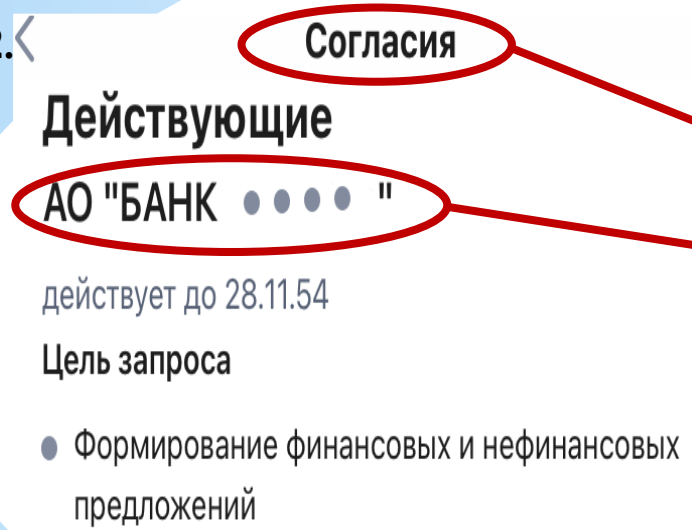
- **Указывают номер жертвы и ждут когда, им сообщать код из СМС.**

- **Для аккаунтов где установлен вход на портал по смс-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. На самом деле повторно приходит КОД для изменения номера телефона.**



Способ защиты:

1. НИКОМУ НЕ СООБЩАЙТЕ КОД ИЗ СМС-СООБЩЕНИЯ ПОСТУПИВШИЙ С ПОРТАЛА ГОСУСЛУГ.

2. 

ИЧНОМ КАБИНЕТЕ, ЗАЙТИ В «ПРОФИЛЬ»;

ЫРАТЬ РАЗДЕЛ «СОГЛАСИЯ И ДОВЕРЕННОСТИ»;

ОЗВАТЬ СОГЛАСИЯ НА ОБРАБОТКУ

СОНАЛЬНЫХ ДАННЫХ У БАНКОВСКИХ

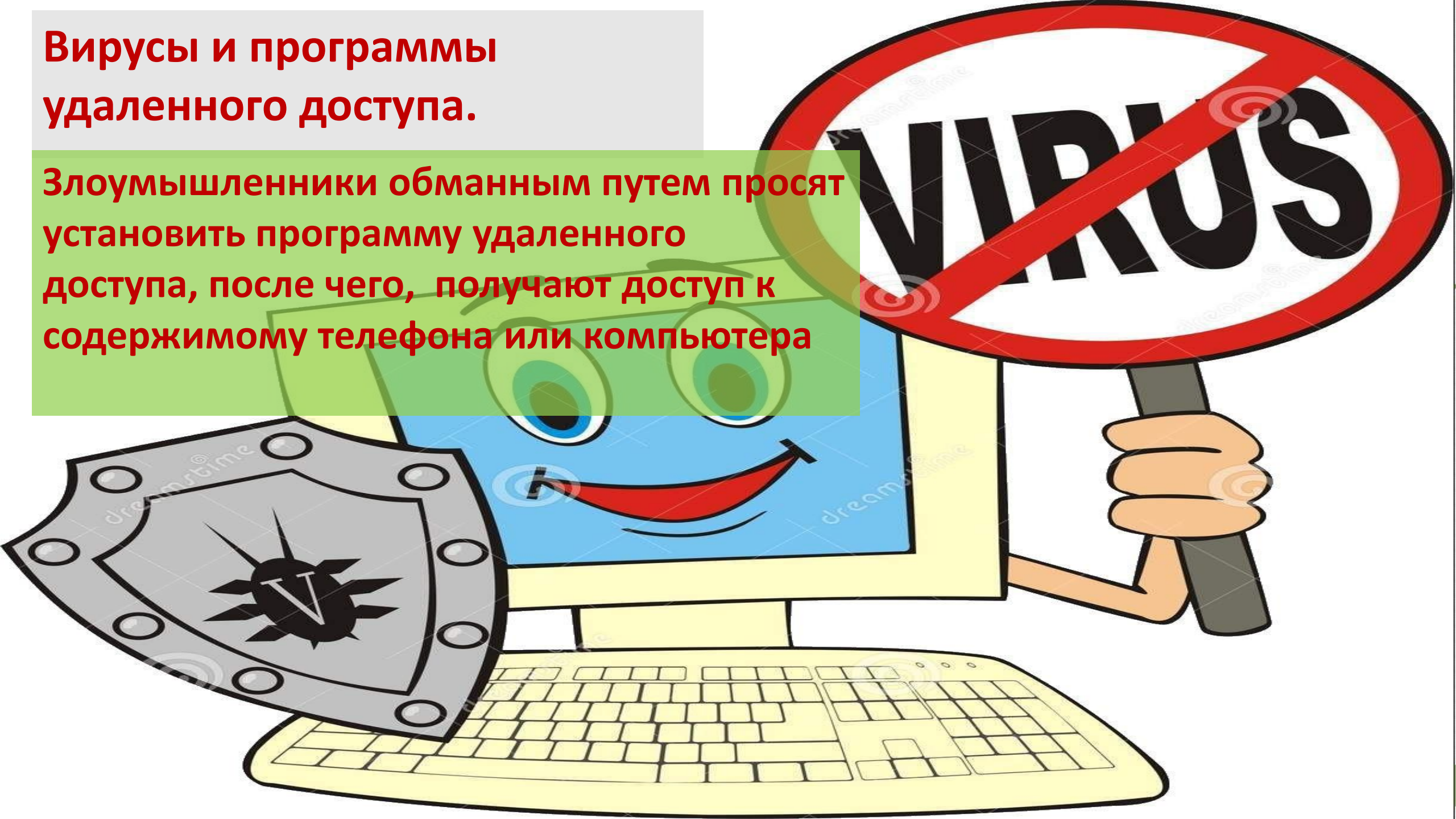
АНИЗАЦИЙ.

3. НАСТРОИТЬ ВХОД НА ГОСУСЛУГИ ПО ПАРОЛЮ И КОДУ ИЗ СМС-СООБЩЕНИЯ.

4. РЕГУЛЯРНО, РАЗ В ПОЛГОДА, МЕНЯТЬ ПАРОЛИ ДОСТУПА.

Вирусы и программы удаленного доступа.

Злоумышленники обманным путем просят установить программу удаленного доступа, после чего, получают доступ к содержимому телефона или компьютера



В целях безопасности рекомендуется использовать программы по блокировке спам-звонков» и «Антивирусы»

«ПРОГРАММЫ ПО БЛОКИРОВКЕ СПАМ-ЗВОНКОВ»:

- Наиболее популярные приложения «Who Calls», «Truecaller», «Не звони мне», «Call Blocker», «Яндекс антиспам».
- Так же у всех операторов сотовой связи имеется услуга «Антиспам»;

«Антивирусы»:

- Популярные «Касперский», «Avast», «ESET», «NORTON».
- У антивирусов имеется функция защиты от фишинговых сайтов, подозрительных ссылок;
- Защита от утечки данных.
- Функция «Антивор» для удаленной блокировки, очистки и поиска телефона.

Мошенничества в сети интернет:

- Мошенничества в сфере купли и продажи;
- Мошенничества, совершаемые под предлогом оказания услуг;
- Финансовые пирамиды, фиктивные инвестиции.

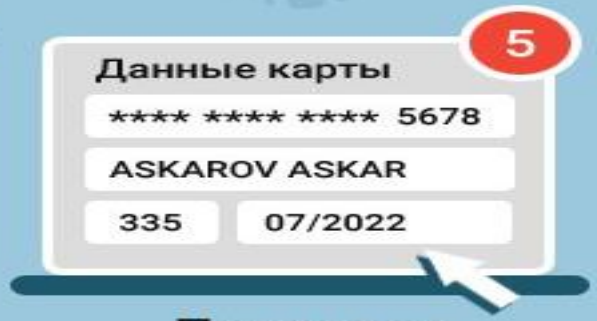
Мошенничества в сфере купли и продажи

Мошенник откликается на объявление

Предлагает оплату безналом, просит доставку

Для расчета с продавцом скидывает ссылку на сайт-двойник

При переходе по ссылке сайт запрашивает данные банковской карты



Продавец вводит данные

Мошенник крадёт деньги

Сделайте репост, поделитесь с друзьями!

Мошенник покупатель

СХЕМА ОБМАНА:

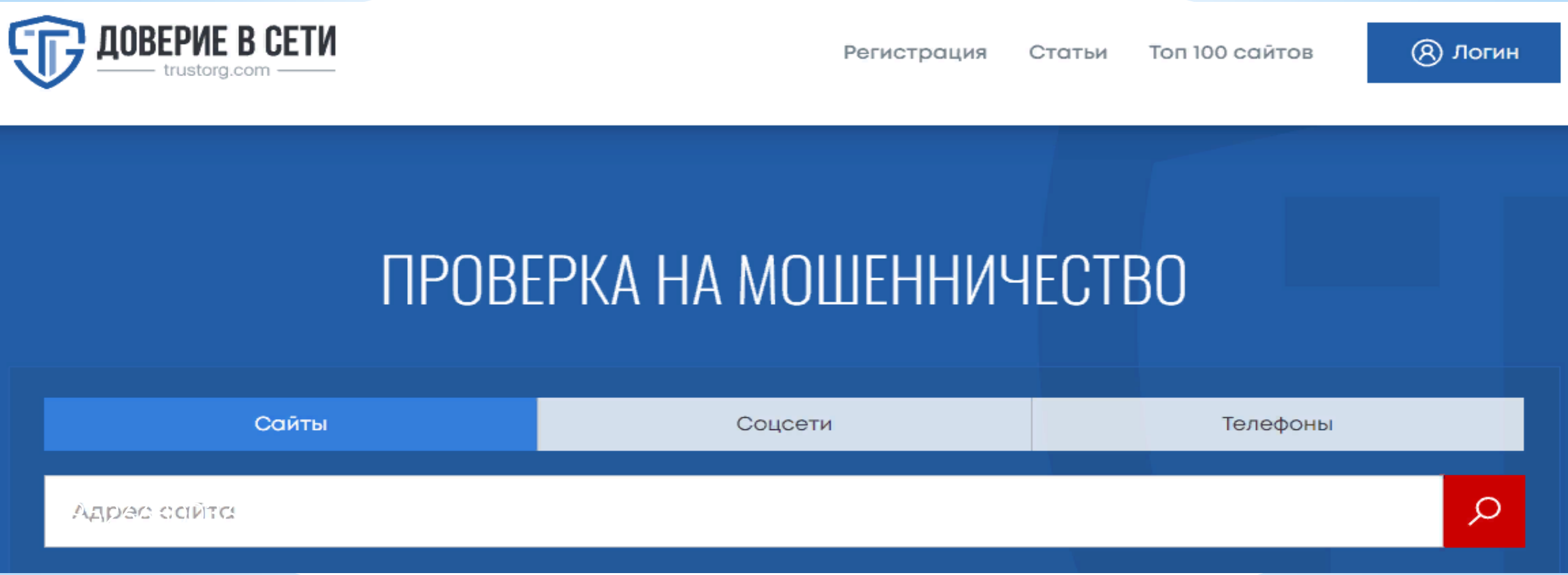
- **1. Мошенник откликается на объявление.**
- **2. Предлагает оплату безналичным способом, просит осуществить доставку;**
- **3. Под предлогом осуществления безопасной сделки скидывает продавцу ссылку на сайт двойник;**
- **4. При переходе по ссылке сайт запрашивает данные банковской карты (номер карты, защитный CVV-код карты, код из СМС);**
- **5. Продавец (жертва) вводит требуемые данные карты.**
- **6. Мошенник КРАДЕТ ДЕНЬГИ.**

Мошенник - продавец

СХЕМА ОБМАНА:

- **1. Продавец-мошенник размещает в сети интернет заманчивое объявление о продаже товара.**
- **2. Жертва откликается на объявление, оговаривают условия купли-продажи.**
- **3. Продавец-мошенник просит внести предоплату или оплатить полную стоимость товара;**
- **4. Жертва совершает оплату/предоплату.**
- **5. Продавец -мошенник перестает выходить на связь.**

Проверьте продавца/покупателя при помощи различных сервисов. Например на сайте «Доверие в сети»



Мошенник продавец

Признаки мошенничества

Отказ от личной встречи

Отказ от наложенного платежа

Заниженная стоимость товара

Требование предоплаты

Необходимо перейти по ссылке на сайт (двойник) для безопасной сделки

Настойчивые просьбы быстрее оплатить товар

- *Насторожитесь если номерная емкость телефона продавца не соответствует региону его местонахождения

Советы по безопасности

Покупайте и продавайте в вашем городе, из рук в руки

Называйте только номер карты - этого достаточно для перевода денег

Оформите отдельную карту для оплаты в интернете

Не отправляйте деньги наперед

Настаивайте на наложенном платеже без предоплаты

Проверяйте данные продавца/покупателя в интернете

- ***Не переходите по неизвестным ссылкам, для совершения безопасной сделки сформируйте ссылку самостоятельно.**

МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ ОКАЗАНИЯ УСЛУГ

- Поиск работы через интернет;
- Поиск услуг по доставке товаров.

ПОСЛЕ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЯ О ПОИСКЕ РАБОТЫ:

- поступает звонок менеджера;
- проводит опрос, оговаривает условия работы.

ДАЛЕЕ МОШЕННИКИ ПРЕДЛАГАЮТ:

- пройти платные курсы;
- зарегистрироваться на сайте, с подтверждением личности посредством ввода СМС-кода;
- зарегистрировать банковскую карту для получения заработной платы, подтверждая кодом из СМС.

НА САМОМ ДЕЛЕ СМС-КОД НЕОБХОДИМ ДЛЯ ВХОДА В БАНКОВСКОЕ ПРИЛОЖЕНИЕ, ЛИБО ЛИЧНЫЙ КАБИНЕТ ПОРТАЛА ГОСУСЛУГ

Так же имеются случаи мошенничества под предлогом заработка от продаж на популярных марке «Вайлдбериз» и «Озон», либо под предлогом накрутки рейтинга положительных отзывов.

Мошенники предлагают:

- Зарабатывать на оценке товара (ставить «лайки»);	**-Перейти по ссылке на сайт маркетплейса, при этом вы попадаете на сайт двойник, где при регистрации требуется внесение персональных данных, в том числе коды из СМС-сообщений**
- «закупать» товар для реализации, при этом денежные средства на «закуп» впоследствии поступают мошенникам.	

Как себя обезопасить:

- Поиск информации о компании в открытых источниках. Если не имеется никаких сведений — это повод насторожиться.
- Не совершайте платежи/переводы в адрес потенциального работодателя (даже если вам объясняют их необходимость для будущей работы — например, плата за вводное обучение, рабочую форму или рабочие инструменты).
- Не сообщайте/не указывайте коды из поступивших смс-сообщений;
- Не выполняйте действия в «Банковских приложениях» по чьей либо просьбе/указанию (Например для открытия «Рабочего счета» и др.)

СОВРЕМЕННЫЕ ВИДЫ ФИНАНСОВЫХ ПИРАМИД

КРИПТО-ПИРАМИДА

НЕЛЕГАЛЬНЫЙ ФОРЕКС

Финансовые организации, которые работают по видом легальных и завлекают высоким процентом

ФИНАНСОВЫЕ ПИРАМИДЫ

Признаки финансовой пирамиды

1. Обещание слишком высоких доходов
2. Прибыль за счет привлечения новых вкладчиков
3. Ограниченный доступ к учредительным документам и финансовой отчетности компании
4. Сомнительные договоры
5. Агрессивная реклама

Как себя обезопасить:

- **Проверять брокерскую компанию на сайте Банка России на наличие лицензии;**
- **Не доверять рекламе о биржах в социальных сетях;**
- **Не верить заманчивым и убедительным обещаниям о высокой доходности и отсутствии риска;**

Внимание! Как не стать жертвой мошенничества

- *Не отвечайте на подозрительные звонки, не перезванивайте на незнакомые номера;*
- *Прервите разговор если он касается финансовых вопросов;*
- *Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам, самостоятельно позвоните в банк или организацию;*
- *Не сообщайте сведения о банковских картах, CVV/CVC-коды;*
- *Не кому не перечисляйте денежные средства;*
- *Не переходите по ссылкам, не устанавливайте приложения поступившие по ссылке в СМС-сообщениях;*
- *В случае утери или кражи телефона с подключенной услугой «Мобильный банк» необходимо обратиться в контактный центр Банка для блокировки услуги, также необходимо заблокировать SIM-карту;*

«Основные способы мошенничеств, совершенных с применением информационно-коммуникационных технологий»

МВД по Республике Бурятия