**Номера горячих линий основных системно - значимых кредитных учреждений в России**

* АО Сбербанк

8 800 555 55 50

* ПАО ВТБ

8 800 100 24 24

* ПАО Газпромбанк

8 800 100 07 01

* АО Почта Банк

8 800 550 07 70

* ПАО Росбанк

8 800 234 44 34

* АО Россельхозбанк

8 800 100 01 00

* АО Альфа Банк

8 800 200 00 00

* ПАО Промсвязьбанк

8 800 999 03 03

На официальном сайте МВД России до населения доводится информация о зарегистрированных случаях мошенничества.

В 2023 году УМВД России по Хабаровскому краю \*

зарегистрировано

более **3,5 тыс.**

мошеннических действий,

ущерб составил

более **1,6 млрд. рублей.**

**В случае совершения мошеннических действий пострадавшим необходимо обращаться:**

* в Дежурную часть УМВД России по Хабаровскому краю\*
по тел.: +7(4212)38 7777
* по телефону горячей линии МВД России:

8 (800) 222-74-47

**Как защититься**

**от мошенников?**

**Наиболее распространенные виды финансового мошенничества**

1. **Звонки от представителей "банков", "правоохранительных органов", "операторов сотовой связи", "сервиса Госуслуги"** с целью получения данных банковских карт и счетов, в том числе через кодовые сообщения, предоставляющие мошенникам доступ к телефону и установленным на нем приложениям.
2. **Предложения заработать в интернете на так называемых "инвестициях"**, например, через вложение денег в криптовалюту, биржевые операции.
3. **Сообщения в мессенджерах, социальных сетях или электронные письма с подозрительными ссылками**, переход по которым связан с финансовыми угрозами.
4. **Предложения получить выплату или компенсацию от государства**, для оформления которой нужно сообщить данные карты или другую личную информацию.
5. **Звонки с просьбами помочь родственникам, знакомым**, которые якобы попали в трудную жизненную ситуацию, а также вымогательства денег под предлогом получения выигрыша в лотерею.
6. **Продажа или покупка товаров в интернете**.
7. **Фишинг –** кража персональных данных и денежных средств с помощью поддельных сайтов, аккаунтов.

**Наиболее опасные виды фишинга**

* Сообщения с просьбой денежного займа, голосования в конкурсе, ссылкой на «смешное видео» от кого-то из ваших друзей. При переходе на страницу голосования или для просмотра «смешного видео» вам предлагается ввести логин и пароль на странице, похожей на главную страницу социальной сети, после чего аккаунт оказывается взломанным.
* Интернет-магазины, кинотеатры, службы доставки и прочее. Здесь целью становятся данные, позволяющие получить доступ к привязанным банковским картам. В зоне риска находятся и те, кто вводит платежные данные в онлайн-магазинах: ошибившись с окном ввода, не проверив адрес в строке браузера. Существуют сервисы, имитирующие ошибку транзакции с целью ее повторения, например, чтобы провести транзакцию два раза подряд.
* Игра на чувствах и эмоциях через публикацию на страницах социальных сетей эмоциональных историй о детях или животных, нуждающихся в помощи, с подкреплением поста фотографиями, документами и сообщением «максимальный репост». Главная угроза – создание конверсии поста и его распространение от одного человека по цепочке его друзей и контактов.
* Игра на любопытстве. Заманчивые предложения в личных сообщениях, либо в ленте. В любом случае попросят перейти по какой-либо ссылке и ввести данные: личные или банковской карты.

**Правила поведения**

* Работники силовых ведомств, банков, компаний сотовой связи, сервиса Госуслуги никогда не звонят гражданам и не пугают потерей денежных средств, не предлагают обновление персональных данных по ссылкам сторонних приложений. При поступлении таких звонков необходимо незамедлительно прервать телефонный разговор.
* Никому не сообщайте полные данные банковский карты, коды и одноразовые пароли, которые приходят посредством СМС-сообщений. Это делать категорически нельзя. Тем самым вы открываете злоумышленнику доступ к вашему счету.  **Если вам позвонили, представились и запросили код, положите трубку — это мошенники.**
* **Не совершайте никакие финансовые операции по указанию незнакомых лиц**, кем бы они ни представлялись: сотрудниками правоохранительных органов, банков, операторов сотовой связи, МФЦ, сервиса Госуслуги или иных организаций.

Злоумышленник может получить доступ к аккаунту только в том случае, если пользователь сам передаст всю необходимую для входа информацию. Берегите свои персональные данные, будьте внимательны. **Пользуйтесь только официальными сайтами и приложениями.**

Если вас просят обновить какие-либо сведения, не переходите по предложенным ссылкам. Для получения ваших данных мошенники могут использовать фишинговые страницы.

**Устанавливайте приложения только из официальных магазинов** — RuStore, Google Play, App Store и AppGallery.

**Защитите свой аккаунт:**

⚫ Придумайте **сложный парол**ь, используйте его только **для одного аккаунта и меняйте его не реже одного раза в три месяца.**

⚫ Подключите двухфакторную аутентификацию, если её у вас ещё нет. Это повышает безопасность данных. Три варианта второго фактора защиты:

1. код из СМС,

2. одноразовый код из приложения,

3. вход по биометрии. Используйте один из них.

❗ **Никому и никогда не сообщайте пароль для входа в аккаунт и сведения о втором факторе защиты.**