**Прокуратура Уярского района**

**Красноярского края**

**ПРЕДУПРЕЖДАЕТ:**

|  |  |
| --- | --- |
|  |  |

**Осторожно: мошенники!**

**Не дайте себя обмануть!**

**Мы расскажем Вам о том**

**как не стать жертвой мошенничества**

В последнее время наиболее распространенным видом мошенничества стало мошенничество в сфере информационно-телекоммуникационных технологий или компьютерной информации. По данным Генеральной прокуратуры Российской Федерации на них приходится около 70% всех хищений, совершенных путем обмана или злоупотребления доверием. При этом более 42,7% мошенничеств совершалось с использованием средств мобильной связи. Также Генпрокуратура РФ констатировала значительное увеличение числа краж, совершенных с банковского счета или в отношении электронных денежных средств: за последние 5 лет зарегистрировано увеличение таких преступных посягательств более чем в 11 раз.

На территории Красноярского края в 2022 году жертвами интернет-преступников стали 7206 жителей. Причиненный ущерб составил 1 340 869 494 рублей.

Мы хотим Вам рассказать о преступлениях, связанных с хищением личных данных, с помощью которых преступник может совершить кражу денежных средств, которые находятся на ваших личных счетах в различных банках. Также мы хотим рассказать о различных видах мошенничества с использованием мобильного телефона, которые встречаются очень часто.

На сегодняшний день жизнь большинства из нас сложно представить без сотовых телефонов и сети Интернет: заказать еду, оплатить счета, купить одежду, найти человека и многое другое можно сделать, не выходя из дома, достаточно иметь мобильный телефон или компьютер с доступом в Интернет.   
Но если для одних людей это отличная возможность сэкономить свое время и максимально облегчить себе жизнь, то для других более «предприимчивых» граждан открывается огромное поле для мошеннической деятельности.

Для того чтобы не стать жертвой мошенничества достаточно следовать инструкциям, указанным в данной брошюре!

**Ситуация 1**

**Хищение при помощи VPN!**



С момента введения в отношении России санкций VPN-сервисы стали очень популярны среди российских пользователей. Однако мало кто знает о том, что VPN может быть опасным. Чаще всего пользователи скачивают VPN на мобильные устройства. Подключаясь к VPN, пользователь должен понимать, что он добровольно предоставляет свои данные разработчикам приложения. Главная опасность VPN — высокий риск утечки данных.

Пользователи думают, что VPN лишь дает возможность пользоваться не доступными в регионе сайтами, но вместо этого рискуют потерять свои данные, которые находятся на их устройстве.  Использование VPN-сервисов равносильно тому, что отдать свой паспорт первому встречному незнакомцу.

Важно помнить, что VPN-сервисы нельзя оставлять постоянно включенными, особенно одновременно с приложениями банков или онлайн-магазинов. При оплате покупок или совершении переводов в мобильных банках VPN обязательно нужно выключать. Если пользователь все-таки зашел, например, в онлайн-банк, стоит немедленно принять меры, чтобы избежать утечки важных данных: в этом случае следует обновить учетные данные, поставить ограничение на банковские переводы, запретить онлайн-платежи. В противном случае велик риск использования личных данных, таких как номер банковского счета, пароля к карте, и иных персональных данных, позволяющих злоумышленникам похитить принадлежащие Вам денежные средства.

Прокуратура района не рекомендует пользоваться VPN сервисами!

**Ситуация 2**

**Розыгрыш призов!**

|  |  |
| --- | --- |
|  | Вам пришло сообщение о том, что Вы выиграли дорогостоящий подарок и просят перевести деньги за получение приза! |

НИКОГДА НЕ ОТПРАВЛЯЙТЕ ДЕНЬГИ НЕЗНАКОМЫМ ЛЮДЯМ!

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше, равна нулю! В дальнейшем вернуть отправленные Вами денежные средства будет очень сложно! Любая просьба перевести денежные средства для получения выигрыша должна насторожить Вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, при этом порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета, карты или «электронные кошельки» физических или юридических лиц.

**Ситуация 3**

**Мошенничество с кредитными картами.**

|  |  |
| --- | --- |
|  | Звонящий на мобильный телефон злоумышленник представляется сотрудником службы технической поддержки либо службы безопасности Вашего банка и сообщает, что с принадлежащего Вам счета осуществлен перевод денежных средств в пользу незнакомого Вам человека. Злоумышленник предлагает отменить указанную финансовую операцию, но для этого ему необходимо получить данные Вашей пластикой карты. |

НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ РЕКВИЗИТЫ ВАШЕЙ БАНКОВСКОЙ КАРТЫ И ДРУГИЕ ПЕРСОНАЛЬНЫЕ СВЕДЕНИЯ!!!

Помните, что банки никогда не звонят на телефоны своих клиентов и не просят сообщить реквизиты их банковской карты! Позвоните на горячую линию Вашего банка и убедитесь в том, что денежные средства с Вашей карты не переводились. Телефон банка Вы найдете на обратной стороне карты.

**Ситуация 4**

**Ошибочный перевод денежных средств!**

|  |  |
| --- | --- |
|  | Вам пришло сообщение о поступлении денежных средств на Ваш счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок, и человек на другом конце провода сообщает, что ошибочно перевел Вам деньги и просит вернуть их обратно тем же «Мобильным переводом». |

НА САМОМ ДЕЛЕ НИКАКОЙ ОШИБКИ НЕ БЫЛО! ДЕНЕГ ВАМ НЕ ПРИСЫЛАЛИ!

Помните, что отправитель денежных средств может вернуть переведенные Вам денежные средства, просто написав заявление в своем банке.

Самым правильным решением в данном случае будет позвонить на горячую линию Вашего банка и уточнить о поступлении Вам денежных средств. Телефон Вашего банка Вы найдете на обратной стороне карты.

И если Вам действительно переведены денежные средства от незнакомого лица, не спешите возвращать деньги по первому требованию: вернув деньги сразу после звонка злоумышленника, последний получит и Ваши деньги, а через некоторое время и свои.

В этом случае не отправляйте деньги незнакомцу, а предложите ему официально обратиться в свой банк и написать заявление о возврате денежных средств.

**Ситуация 5**

**Несчастный случай с родственниками**

|  |  |
| --- | --- |
|  | На Ваш телефон поступает звонок, причем он может осуществляться как на мобильный телефон, так и стационарный. Звонящий представляется сотрудником полиции и сообщает, что Ваш родственник задержан и находится в отделе полиции за совершение преступления (совершил ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений).  Далее лжесотрудник вымогает у Вас взятку и взамен обещает отпустить Вашего родственника. Злоумышленник просит не прерывать телефонный разговор, это необходимо для того, чтобы Вы не могли связаться по телефону с настоящим родственником. |

ВСЯ ЭТА СИТУАЦИЯ ВЫМЕСЕЛ! ВАШЕМУ РОДСТВЕННИКУ НИЧЕГО НЕ УГРОЖАЕТ!

Достаточно лично позвонить Вашему родственнику, чтобы убедиться, что у него все в порядке. Если родственник сразу не ответит, то перезвоните ему позднее, либо позвоните людям, которые могут находиться с ним рядом.

**Ситуация 6**

**СМС – мошенники!**

|  |  |
| --- | --- |
|  | На Ваш телефон поступает смс-сообщение с текстом «Ваша карта заблокирована, для помощи в разблокировке позвоните по телефону 8800\*\*\*\*\*09».  Если вы позвоните по указанному номеру телефона, то злоумышленник представившейся сотрудником банка, попросит сообщить реквизиты Вашей банковской карты, а также иные персональные данные, получив которые похитит с Вашего счета денежные средства. |

НИКОГДА НЕ ПЕРЕЗВАНИВАЙТЕ НА НОМЕРА ТЕЛЕФОНОВ, УКАЗАННЫЕ В CMC - СООБЩЕНИЯХ! НИКОМУ НЕ СООБЩАЙТЕ РЕКВИЗИТЫ ВАШЕЙ БАНКОВСКОЙ КАРТЫ И ДРУГИЕ ПЕРСОНАЛЬНЫЕ СВЕДЕНИЯ!

Самым правильным решением в данном случае будет позвонить на горячую линию Вашего банка и уточнить о возможной блокировке карты. Телефон Вашего банка Вы найдете на обратной стороне карты.

**Ситуация 7**

**Мошенники под видом покупателей!**

|  |  |
| --- | --- |
|  | На Ваш телефон звонит злоумышленник и сообщает, что готов приобрести товар, который Вы разместили для продажи в сети Интернет. Злоумышленник сообщает, что готов приобрести Ваш товар прямо сейчас, но в связи с тем, что он находится в другом городе ему необходимо помочь перевести Вам деньги. Для того чтобы это сделать злоумышленник предлагает пройти к ближайшему банкомату и следовать его инструкциям. |

НИКОГДА НЕ СЛЕДУЙТЕ УКАЗАНИЯМ И ИНСТРУКЦИЯМ ДРУГИХ ЛЮДЕЙ ПРИ РАБОТЕ С ВАШЕЙ БАНКОВСКОЙ КАРТОЙ!

Помните, что для того чтобы осуществить Вам перевод денежных средств в счет покупки товара, Вашего личного участия не требуется.

Самым правильным решением в данном случае будет сообщить лжепокупателю о том, что продажа товара может быть осуществлена только в обычном порядке, он может перевести денежные средства на Ваш счет в любом доступном отделении банка, поэтому идти к банкомату и производить манипуляции со своей банковской картой Вы не станете.

**Ситуация 8**

**Мошенничество в социальных сетях!**

|  |  |
| --- | --- |
|  |  |
| На Ваш страницу в социальной сети приходит сообщение от Вашего знакомого с просьбой срочно перевести ему денежные средства на указанный номер счета или карту. | |

НЕ СПЕШИТЕ ПЕРЕВОДИТЬ ДЕНЕЖНЫЕ СРЕДСТВА ПО ПЕРВОЙ ПРОСЬБЕ! УБЕДИТЕСЬ, ЧТО ЭТО ДЕЙСТВИТЕЛЬНО ВАШ ЗНАКОМЫЙ!

Для того чтобы убедиться в том, что Вашему знакомому действительно нужны денежные средства, позвоните на его мобильный телефон у убедитесь в том, что именно он написал Вам сообщение. Можно также задать злоумышленнику личный вопрос, ответ на который может знать только Ваш знакомый. Злоумышленник не станет на него отвечать!

Для того чтобы не стать жертвой мошенничества достаточно следовать вышеуказанным рекомендациям!

Если в отношении Вас и Ваших близких совершено преступление незамедлительно обратитесь в правоохранительные органы. Постарайтесь сохранить сведения о поступивших от злоумышленников Вам телефонных звонках, смс - сообщениях, переписках в социальных сетях, а также других данных которые смогут помочь правоохранительным органам в установлении и поимки преступников.

**Ситуация 9**

**Мошенничество с ценными бумагами**

Как действуют мошенники: мошенники предлагают популярную сейчас услугу — открытие брокерского счёта.

Мошенники звонят по телефону представляются представителями банка или брокерского агентства и просят установить поддельное приложение, которое очень похоже на банковское. В скаченной программе всё так устроено, что любые проведенные операции приводят в итоге только к одному - переводу денежных средств на счёт злоумышленника. В этом случае человек рискует своими сбережениями на всех имеющихся у него счетах.

Категорически возбраняется устанавливать неизвестные приложения! Никогда не скачивайте программу, даже если об этом просит человек, который позвонил по телефону и представился сотрудником банка.

Не стоит верить обещаниям сверхприбыли и скорого обогащения. Фондовый рынок всегда несёт риски, и если Вам об этом не говорят, то это или преступники, или не очень честные сотрудники брокерских компаний.

Как отличить брокера от мошенника?

Если вам звонят и предлагают открыть брокерский счёт, главное в этом вопросе не торопиться. После звонка нужно зайти на сайт брокера, изучить его. Найти компанию в реестре Центробанка. Список опубликован на сайте. Если вы не увидели там фирму, с представителем которой говорили по телефону, значит, она не может предоставлять брокерские услуги на бирже. Значит Вам звонил мошенник!

Также не стоит открывать брокерский счёт по ссылкам, которые присылают по почте или в мессенджерах. Любые подозрительные предложения надо просто игнорировать.

Если Вы хотите участвовать в торгах на бирже, то лучше найти время и сходить в офис брокера или банка.