В век высоких технологий и электронных (цифровых) денег высок риск потерять свои заработанные тяжелым трудом денежные средства, если не знать простых вещей. Рассмотрим, как себя вести и что нельзя делать не в коем случае.

Чтобы защитить себя от мошенников, не нужно быть специалистом по безопасности.

Достаточно знать, что и в какой момент может пойти не так — и что делать, чтобы сохранить деньги.

Будьте внимательны, если вдруг в интернете вы встретите одно из таких предложений.

Получите деньги за опрос

Как работает схема.

Мошенники создают сайт, на котором предлагают деньги за простые действия: например, просят пройти короткий опрос или отправить ссылку друзьям. Обещают много: до 200 000 рублей за ответы на несколько вопросов.

Прокуратура Сакмарского района Оренбургской области, с. Сакмара, ул. Советская, д. 15

Телефоны:

(35331)21-8-92

(35331)21-0-16

Электронная почта:

Sakmara@56.mailop.ru

Подключитесь к бесплатному вайфаю.

Как работает схема. Мошенники создают

Прокуратура Оренбургской области

Прокуратура Сакмарского района

ПАМЯТКА

КАК УБЕРЕЧЬ СЕБЯ ОТ ИНТЕРНЕТ-МОШЕННИКОВ

с. Сакмара, 2022 год

Звонок из банка

Как работает схема. Мошенники звонят и представляются сотрудниками банка: говорят, что с вашего счета списаны деньги. Чтобы их вернуть, нужно срочно продиктовать данные карты и сообщить одноразовый код, который придет в смс.

В чем опасность. Мошенники получат доступ к вашему интернет-банку и смогут распоряжаться деньгами. Код из смс нужен, чтобы подтвердить перевод на чужую карту

Вы отвечаете на вопросы, делитесь ссылкой с друзьями. На последнем шаге выясняется, что нужно «активировать аккаунт», «оплатить комиссию», сделать «закрепительный платеж» или ввести номер карты.

В чем опасность. Мошенники возьмут деньги за «комиссию», но никаких выплат не дадут. Реквизиты банковской карты они смогут использовать для будущих списаний. А друзья посчитают вас спамером.

Как защититься:

1. Не верьте, даже если на сайте есть отзывы людей, логотипы известных банков и других авторитетных организаций: все это — уловки мошенников.
2. Если вы ввели данные карты на подозрительном сайте, срочно позвоните в свой банк и расскажите об этом — там подскажут, что делать.

вайфай-точку, которая не требует пароля — подключиться к интернету может любой желающий. Такое соединение обычно настраивают в людных местах: на улице, в кафе или отеле.

Владелец вайфая видит, на какие сайты заходят все подключившиеся, но это не самое страшное. Он может добраться до паролей, которые вы вводите на этих самых сайтах.

В чем опасность. Мошенники могут украсть пароли от социальных сетей и почты, а еще реквизиты карты — если вы расплатитесь ею в интернет-магазине. Зная данные карты, мошенники легко выведут деньги на свои счета. А в социальных сетях они увидят сообщения, которые вы никому не хотели показывать, — вот и повод для шантажа.

Как защититься:

1. Не вводить логины и пароли на сайтах с незащищенным соединением или ошибками безопасности.
2. Отключиться от вайфая и работать через мобильную сеть в случаях, когда нужно вводить логин, пароль или данные карты.

или покупку в магазине.

Как защититься:

1. Скажите, что не можете говорить, и повесьте трубку.
2. Перезвоните в банк самостоятельно или проверьте счет через мобильное приложение.
3. Если назвали мошенникам код или любые другие данные — срочно звоните в банк. Возможно, вы успеете остановить операцию.
4. Запомните: сотрудник банка никогда не попросит назвать код из смс и номер карты при телефонном разговоре