Прокуратура г. Усть-Кута напоминает !

Финансовая грамотность населения способствует принятию грамотных решений, минимизирует риски и тем самым способна повысить финансовую безопасность граждан. Низкий уровень финансовой грамотности может привести не только к банкротству, но и к неграмотному планированию выхода на пенсию, уязвимости к финансовым мошенничествам, чрезмерным долгам и социальным проблемам, включая депрессию и прочие проблемы.

Согласно статистическим данным МВД России в настоящее время, именно молодые люди (младше 18 лет) всё чаще становятся жертвами мошенников: пользуясь неопытностью и доверчивостью детей и подростков, злоумышленники крадут деньги с их карт и со счетов их родителей. Для обмана используются игры, призы и даже предложения о подработке. Вместе с развитием онлайн-услуг и цифровых сервисов мошенничество с похищением личных средств физических лиц стало одним из основных рисков во многих странах.

К любой ситуации необходимо относится с критическим восприятием. Рекомендуется воспринимать с сомнением все звонки, когда собеседник вас куда-то отправляет, склоняет вас к каким-то действиям, требует переводить деньги или что-то оформлять.

Необходимо запомнить несколько общих простых правил:

Правила действий при телефонных звонках:

1. Внимательно проверять входящий номер.

2. Не отвечать и не перезванивать по неизвестным и сомнительным номерам. Даже если телефон кажется верным, стоит всегда проверять номера в официальных справочниках и на официальных сайтах.

3. Прервать разговор - если он касается финансовых вопросов.

4. Не совершать операций или действий по инструкциям звонящего.

5. Никому не сообщать коды подтверждения из СМС-сообщений.

6. Не торопиться принимать решение.

7. Установить приложение для фильтрации входящих вызовов. Заблокировать звонки с подозрительных номеров.

Правила действий с банковскими картами и при расчетных операциях:

1. Не передавать банковскую карту посторонним. Требовать проведения операций с ней только в личном присутствии и никогда не терять ее из виду.

2. Не делать покупки и не вводить код CVV/CVC на сомнительных сайтах.

3. Данные карты (номер, пин-код, CVC-код) нельзя сообщать никому, даже сотрудникам банка.

4. Нельзя писать пин-код на карте и хранить его отдельно.

5. Если банковская карта потерялась, необходимо немедленно сообщить в банк и заблокировать ее. То же самое – если пришло СМС-сообщение о покупке или снятии денег в банкомате, а вы этого не делали.

6. Не использовать открытые точки Wi-Fi (интернет в общественных местах: транспорте, кафе, кинотеатрах), когда заходите в интернет-банк или пользуетесь мобильным банковским приложением.

7. Оплата в интернет-магазине не должна происходить как перевод средств на чей-то личный счет.

Правила действий в интернете и в переписке для защиты от фишинга и кибермошенничества:

1. Не следует верить информации о выигрышах, платить деньги за участие в челленджах и обольщаться легким заработком.

2. Не переходить по ссылкам в письмах или сообщениях о выигрыше денег, гаджета или другого приза, не кликайте на подозрительные объекты.

3. Опасно скачивать по просьбе незнакомцев какие-либо приложения, открывать незнакомые и странные ссылки.

4. Никому в переписке не сообщать коды подтверждения из СМС-сообщений.

5. Обращать внимание на почтовый домен, с которого приходят письма. Мошенники обычно используют общедоступные домены gmail.com, mail.ru и т.п., или домены, похожие на официальные имена компаний (напр. sberbankc[.]ru, lc-sberbank[.]com и т.д.)

6. Обращать внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга.

7. Быть осторожными с вложениями в письмах или сообщениях. Открывайте только те вложения, которые ждали.

8. Если в ходе общения в мессенджере бот или робот предлагает ввести личную финансовую информацию (коды из СМС-сообщений от банка, полные данные карты, ФИО, паспортные данные и т. д.), необходимо прервать общение, обратиться в отделение банка либо самостоятельно связаться с организацией по официальным контактам, которые указаны на официальном сайте компании.

9. Нельзя фотографировать и отправлять свои личные данные, копии паспортов и других документов, банковских карточек и деньги незнакомым людям.

10. Предложение общаться в мессенджере, а НЕ ЧЕРЕЗ официальные сайты торговых площадок (например, «Авито» или «Юлу») – первый признак мошенника.

11. Для защиты своих аккаунтов – необходимо подключить двухфакторную аутентификацию.

Если возникает хоть одно сомнение, происходит какое-то пугающее действие, о котором указано ранее, необходимо остановится!

В случае необходимости обратиться в полицию по **номеру 112.**