

ПАМЯТКА ДЛЯ РЕАГИРОВАНИЯ НА НЕПОНЯТНОЕ ОБРАЩЕНИЕ
(по телефону, в СМС-сообщении, на электронной почте, в мессенджере, в социальной сети)

1. Чего не делать.

- ✓ Не снимайте трубку (если номер вам незнаком и вы не ждете важного звонка).
- ✓ Не следуйте никаким советам, просьбам и командам того, кого вы не видите (не сообщайте никакой личной информации, не переходите по неизвестным ссылкам, не перезванивайте по незнакомым номерам, не устанавливайте приложений и прочее).

2. Что делать.

- ✓ Сбрасывайте, выходите из общения (при любом возникшем сомнении, непонятности, отсутствии возможности проверить).
- ✓ Проверяйте (подлинность источника, личности звонящего, сообщенных данных).
- ✓ Уточняйте (задавайте столько вопросов, сколько решите).
- ✓ Просите повторить любую пропущенную, непонятую, дополнительную информацию.
- ✓ Перезванивайте сами (по официальным номерам, найденным самостоятельно).
- ✓ Просите о помощи окружающих людей (не принимайте финансовых решений не посоветовавшись с близкими).
- ✓ Тестируйте звонящего (реагируйте нестандартно):
 - отрицайте названную о вас информацию,
 - признавайте совершенные от вашего имени платежи,
 - тяните время,
 - просите назвать какие-либо сведения о личном счете,
 - высказывайте желание явиться лично (в банк, отделение полиции),
 - предлагайте пригласить вашего помощника,
 - просите убедить вас, что это не мошенник и т.п.

3. Как относиться.

- ✓ Не спешить.
- ✓ Контролировать эмоции (осознавать их и отдавать себе отчет – кто вызвал эти чувства).
- ✓ Не бояться не успеть, потерять выгоду, не выиграть, потерять покупателя.
- ✓ Воспринимать ситуацию отстраненно.
- ✓ Сохранять свой ритм (берите паузу тогда, когда сочтете нужным, не следуйте логике звонящего, не вникайте в его сложные объяснения).
- ✓ Быть независимым в действиях (сознавать – исполняете ли вы чью-то волю).

- ✓ Быть подозрительным, не верить переданному вам в дистанционном формате (даже услышанному и увиденному посредством мобильного устройства; помнить - должность звонящего подтверждает только документ, а не слово).
- ✓ Не терять внимательности при чтении сообщений, ссылок, адресов.
- ✓ Будьте взрослыми (не реагируйте на похвалу или осуждение).
- ✓ Вы имеете право быть бестактными (высказывайте свои подозрения и замеченные неуместности).
- ✓ Не старайтесь выглядеть значительным в глазах звонящего (вы имеете право быть непонятливым, медлительным, недальновидным и прочее).
- ✓ Если к вам обращаются, владея вашими личными данными, значит полной информации звонящим все же не хватает.

Развивайтесь

- ✓ Обращайте внимание на рекомендации в общественных местах.
- ✓ Читайте и слушайте рассказы потерпевших.
- ✓ Не полагайтесь на свою уверенность и опыт (для всех есть свой ключ).
- ✓ Делайте выводы и перестраивайтесь, вырабатывайте полезные привычки и правила.

ПОЛИЦИЯ

ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает, в регионе увеличивается количество случаев телефонного и интернет мошенничества.



1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.



2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!



3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с вашими деньгами.



4. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.



5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.



6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!



7. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.



8. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку – преступление!



9. В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас!



**Если Вы стали жертвой мошенников,
незамедлительно обращайтесь в полицию
по телефонам: 02 или 112**

НЕ ДАЙ СЕБЯ
ОБМАНЫТЬ!!!

Осторожно, мошенники!



НЕ ДАЙ СЕБЯ
ОБМАНУТЬ!!!

STOP
МОШЕННИК



Звонки и СМС из банка

Вам звонит сотрудник банка или приходит сообщение о том, что ваша карта заблокирована. Чтобы исправить ситуацию, необходимо позвонить по указанному номеру. Затем под предлогом уточнения информации злоумышленники выясняют данные карты или вынуждают жертву подойти к банкомату, набрать комбинацию клавиш и совершить тем самым операцию по переводу средств.



Взятка

На телефон поступает звонок. Звонивший сообщает, что ваш родственник стал виновником серьезного ДТП, сейчас находится в отделе полиции, задержан за совершение тяжкого преступления и т.п. Затем мошенник предлагает решить проблему с правоохранительными органами за определенное денежное вознаграждение. Как правило, разговор подкрепляется звуковым сопровождением: вы слышите вой сирены, шум проезжающих машин, голоса. Под разными предложениями поговорить с родственником вам не дают. Вся эта ситуация не более чем хорошо отрепетированный спектакль, цель которого – получить ваши деньги.



Просьба дать позвонить

Всегда с осторожностью относитесь к просьбам «дать позвонить». Мошенник, под предлогом срочного звонка родственникам, может взять ваш телефон, поговорить несколько минут, а затем честно вернуть. За это время с вашего счета исчезает кругленькая сумма, потому что звонок был сделан на платную телефонную линию. Предложите самостоятельно набрать номер телефона и дождитесь соединения с абонентом.



Объявление

Вы подаете объявление об утрате личных вещей или документов с просьбой вернуть их за вознаграждение. На ваш телефон поступает звонок. Собеседник заявляет, что нашел пропавшую вещь и готов её вернуть. В подтверждение вашей заинтересованности просит перевести определенную сумму на электронный кошелек. Это мошенничество! Вы не только не вернете пропажу, но и лишитесь денег.



Выигрыш

Вам приходит СМС или звонят с радио, поздравляют с выигрышем автомобиля или ноутбука и просят отправить подтверждающую СМС, либо внести регистрационный «взнос» через систему электронных платежей, купить карту оплаты и назвать её код. Ни в коем случае не делайте этого.



Просьбы о помощи

Люди поддаются панике, чем и пользуются мошенники. «Мама, положи мне 1000 рублей на этот номер, я потом всё объясню» — распространённое мошенническое сообщение с просьбой о помощи. Злоумышленники надеются на то, что женщина не попытается дозвониться до своего ребенка и, поддавшись панике, полонит деньги. Не волнуйтесь. Постарайтесь дозвониться до человека или кого-то из его ближайшего окружения. Лучше чаще звоните близким людям, а не только в день рождения, на Новый год, 8 Марта и 23 Февраля.



Звонок от лица оператора

Вам звонит «техническая служба» оператора связи и предлагает подключить новую услугу, запугивая отключением номера или просят заплатить за услуги роуминга, набрав комбинацию знаков на вашем телефоне.



Поддельный перевод

Абоненту приходит СМС о поступлении на его счет мобильного перевода. Сразу после этого перезванивают жулики, которые излагают легенду, что они по ошибке перевели деньги, и просят их вернуть.



Вредоносные программы

Злоумышленники, маскируя свои программы для смартфонов под полезные, например, счетчики калорий, шагомеры или органайзеры, снабжают их скрытыми вирусами, которые сами отправляют сообщения на платные сервисы. Поэтому не устанавливайте на свой телефон неизвестные программы.



Праздничные открытки

Главным образом в праздники мошенники рассылают сообщения, в которых предлагают перейти по ссылке или отправить СМС с кодом на короткий номер, чтобы получить MMS или праздничную открытку. Просто удалите такое сообщение.



Фальшивый заказ

Мошенники обращаются в службы доставки и делают заказ, как правило, на адрес известной организации. Позже звонят вновь и просят курьера попутно положить деньги на телефон, которые затем собираются вернуть вместе с оплатой заказа. Прибыв на место, доставщик узнаёт, что по указанному адресу никто ничего не заказывал, а положенные на телефон деньги оказались в руках мошенников.

