Как обезопасить себя от телефонных мошенников

В любые времена, в любой стране мира, где бы ни появлялись деньги, там появятся люди, желающие их забрать, причем, "не всегда" законным путем. По этому же принципу, как только сотовая связь проникла в нашу с вами жизнь, следом появились и, так называемые, телефонные мошенники. Их основная цель - любым способом получить средства с Вашего счета и при этом остаться не пойманными. Причем, это у них неплохо получается, благо и вариантов обмана абонентов также накопилось предостаточно. Все они основаны на моменте внезапности, когда у человека теряется внимание и он готов к необдуманным поступкам. Такого момента мошенники добиваются, либо сообщая очень хорошую новость (выигрыш крупного приза), либо очень плохую новость (родственник попал в беду). После того как "клиент" введен в состояние рассеянности, мошенник может выставлять свои условия и если в последний момент у "жертвы" не проясняется сознание, то мошеннику удается задуманное. Причем ни в коем случае не стоит быть слишком самоуверенным, так как на крючок мошенников часто попадают очень бдительные люди. Итак, попробуем выделить основные способы мобильного мошенничества, а также найти способы и общие правила поведения в подобных ситуациях.

ОСНОВНЫЕ ВИДЫ МОБИЛЬНОГО МОШЕННИЧЕСТВА

1. Выигрыши. Бесплатный сыр бывает только в мышеловке. Если Вам пришло SMS с уведомлением о выигрыше машины или миллиона, не спешите отправлять SMS, это обман.

2. Ошибочные платежи. На практике бывает так, что Вам действительно кладут деньги по ошибке, поэтому проверьте баланс, даже если Вам внезапно пришло уведомление о пополнении баланса.

3. Просьба о помощи. Если Вам звонят или присылают SMS Ваши родные или друзья с незнакомых номеров, лучше проверьте информацию, перезвонив и удостоверившись действительно ли им необходима Ваша помощь.

4. Выманивание пароля. Ваш пароль - это Ваша персональная информация, не делитесь им ни с кем, даже с родными, если только этот пароль не передается при личной встрече и с Вашего согласия.

5. SMS из банка. Бывает несколько случаев, когда банк обращается к Вам по вопросам просроченных платежей, блокировки карты, блокировки счета, предложений и др. Если даже Вы получили подобное SMS от банка

или Вам, Вашим близким позвонили по этим вопросам, позвоните по официальному номеру телефона в банк и уточните информацию. Ни в коем случае не звоните по указанным номерам в SMS.

6. Wangiri – схема, при которой Вы перезваниваете на незнакомый номер при внезапном обрыве связи и Вас пытаются удерживать на линии как можно дольше. В этом случае с Вашего лицевого счета могут списываться крупные суммы денег.

7. Предложение познакомиться. Помните, внезапное знакомство по SMS практически невозможно. Не отправляйте обратных SMS с кодовыми словами, на короткие номера, ведь так с Вами желают познакомиться только мошенники. Отправка обратного SMS с кодом может привести к списанию крупной суммы с Вашего лицевого счета.

8. Требование выкупа. Если Вы что-либо потеряли и Вам пришло уведомление, поступил звонок о найденной пропаже, не спешите переводить деньги или встречаться с нашедшими пропажу. Сразу обратитесь в полицию, полицейские лучше всего разбираются в делах о пропавших вещах.

СПИСОК ОБЩИХ РЕКОМЕНДАЦИЙ, КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОБИЛЬНОГО МОШЕННИЧЕСТВА

- Никогда не разглашать конфиденциальную информацию о себе, кодовое слово, логины и пароли доступа в личный кабинет посторонним лицам. Не предоставлять любую информацию при входящих звонках на номер, даже если звонящий представляется сотрудником оператора связи и просит какие-нибудь уточняющие конфиденциальные данные.
- Не доверять просьбам о помощи, приходящим с неизвестных номеров, особенно якобы от имени ваших родственников, друзей и знакомых или же от «полиции», «МВД», «банка» и «налоговой службы». В любых подобных случаях обязательно постарайтесь сначала связаться с ними лично и уточнить, действительно ли у них возникли проблемы.
- Не передавать телефон в незнакомые руки, не оставлять его в незнакомом месте. При ремонте обязательно извлечь СИМ-карту, чтобы избежать возможного ее клонирования. После ремонта проверить смартфон с помощью антивирусных программ.
- Никогда не открывать ссылки, полученные в СМС с неизвестных номеров. По возможности не принимать участие в акциях, лотереях и викторинах, даже если они проводятся мобильным оператором.

- Завести отдельный номер для размещения объявлений в интернете, поиска работы, размещения объявлений на сайтах купли-продажи, покупок и заказов на порталах, не заслуживающих доверия. Стараться как можно меньше личной информации публиковать в открытом доступе в соц. сетях.
- Установить антивирус или другое защитное программное обеспечение на смартфон.
- При нахождении в роуминге необходимо понимать, что и за рубежом можно стать жертвой тех же схем мошенничества, которые действуют и в зоне обслуживания домашней сети. Но неприятности, от которых вы сможете более или менее легко отделаться дома, могут принести гораздо больший вред во время пребывания за границей.

В заключении хотелось бы напомнить в очередной раз известную поговорку "Доверяй, но проверяй!". Именно повышенной бдительностью можно себя обезопасить в подобных случаях от действий мошенников и сохранить свои нервы и деньги.

Обо всех фактах телефонного мошенничества Вы можете сообщить в дежурную часть ОМВД России по Октябрьскому району по тел. 102 (с сотового телефона) или 02 (со стационарного телефона).