КОНТАКТНАЯ ИНФОРМАЦИЯ

Пресс-центр Проекта
117105, Россия, Москва,
Варшавское шоссе, дом 9, стр. 28
+7 (495) 640 80 91
press@vashifinancy.ru
www.вашифинансы.рф

Подготовлено АНО «ЭПШ ФБК» по заданию Министерства финансов Российской Федерации в рамках выполнения контракта № FEFLP/FGI-2-1-9 «Разработка брошюр и проведение семинаров по теме «Финансовая безопасность на финансовом рынке» для взрослого населения» по проекту «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации».

Москва, 2016. – 12 с.
Тираж 500 экземпляров

ПО ЗАКАЗУ МИНИСТЕРСТВА ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации»

Мобильные мошенники

Дружи с финансами
НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН

Москва, 2016

МОБИЛЬНЫЕ МОШЕННИЧЕСТВА: ПСИХОЛОГИЯ И ТЕХНОЛОГИЯ

Представить себе современного человека без сотового телефона весьма сложно. За короткий срок мобильники проделали путь от громоздких чемоданчиков до миниатюрных «трубок» весом меньше ста граммов. А затем снова стали увеличиваться в размерах – появились смартфоны (от английского smart – умный и phone – телефон), потом – планшетные компьютеры.

Современный «мобильник» может рассказать о своем владельце практически все: о его семье и друзьях, кем работает, с кем чаще общается, где любит проводить свободное время. И даже о таком непубличном моменте, как состояние банковских счетов своего владельца, сотовый телефон прекрасно осведомлен.

Разумеется, взрывное развитие сотовой связи не прошло мимо преступного мира. На первых порах в ходу были банальные кражи аппаратов, но сегодня криминальные схемы существенно модифицировались, ведь информация, содержащаяся в телефоне, подчас стоит в десятки и сотни раз дороже, чем собственно «трубка».

Мобильные мошенничества можно разделить на две группы. Первая – она сравнительно невелика – новейшие технические разработки разработками в области перехвата и копирования данных. Вторая «работает» по классическим мошенническим схемам: знатоки человеческой психологии подбирают такие «ключики», которые заставляют нас самих выдавать все секреты.

В данной брошюре мы расскажем вам об основных приемах, которые используют мобильные мошенники. Надеемся, что соблюдение мер безопасности убережет вас от неприятностей.

СОДЕРЖАНИЕ

МОШЕННИЧЕСТВА «НА ДОВЕРИИ»

Сколь бы стремительно ни развивался технический прогресс, люди всегда остаются людьми. И методы, которыми пользуются мобильные мошенники, по сути своей ничем не отличаются от тех, что были в ходу и 100, и 200 лет назад. Тяга к легким деньгам, любопытство, беспечность, страх, сострадание – на этом стараются «сыграть» злоумышленники XXI века.

СООБЩЕНИЕ О ВЫИГРЫШЕ ПРИЗА

СМС-сообщение гласит: «Вы выиграли приз! Для получения справки звоните по номеру 111-22-33». Если вы перезвоните на указанный номер (чего делать, между прочим, не следует. Помните, что бесплатный сыр бывает только в мышеловке), то вежливая девушка представится как сотрудница крупного банка (варианты – оператора сотовой сети, интернет-провайдера) и расскажет, что их компания проводит розыгрыш призов среди клиентов. Если вы честно сообщите, что клиентом компании «X» не являетесь, условия лотереи тут же изменятся, и окажется, что в число победителей вы попали, поскольку являетесь «потенциальным потребителем услуг». Далее выяснится, что для оформления приза (вариантов опять много: начиная с уплаты налоговой пошлины и заканчивая платежом в пользу курьерской компании) необходимо приобрести карты оплаты одной из платежных систем и продиктовать коды оператору. После чего разговор неожиданно для вас прервется. Мошенники уже перевели на свой счет весь номинал карты оплаты.

Получив подозрительный звонок, сообщите об этом вашему оператору связи или обратитесь в организацию, от имени которой вам предлагают получить ценный приз.

Все действия с вашим номером мобильного телефона следует совершать только в салонах связи сотового оператора. И уж тем более нельзя заключать никакие договоры с незнакомцами на улицах.

ДЕНЕЖНЫЙ БОНУС ЗА ПОДКЛЮЧЕНИЕ

Вам предлагают (как правило, на улице) подписать некий «Договор на подключение услуг мобильной связи». В качестве бонуса вам на счет обещают зачислить круглую сумму. При этом никаких затрат нести не придется, все расходы будут погашены «оператором сотовой компании в рамках рекламной акции».

Разумеется, никаких денег никто вам на счет не положит. Наоборот, подписанный вами договор (с указанием паспортных данных, номером мобильного телефона и личной подписью) откроет мошенникам путь для расходования ваших средств. Это может быть платная подписка на информационные услуги, звонки за границу и так далее.

БЛОКИРОВЩИКИ РЕКЛАМЫ

Реклама может быть очень назойливой. К сожалению, заполонила она и наши телефоны, просочившись в виде много численных СМС-оповещений, информационных рассылок и тому подобного. Соблазн согласиться отправить сообщение на короткий номер, после которого реклама перестанет вам поступать, велик. Вот только результат такого действия окажется прямо противоположным. Мало того, что само сообщение скорее всего будет платным, так еще и его отправка может спровоцировать новую волну рекламных подписок, которую вы сами и вызвали, отправив злосчастное сообщение.

Прежде чем отправлять сообщения на любые короткие номера, выясняйте у вашего мобильного оператора стоимость такой услуги.

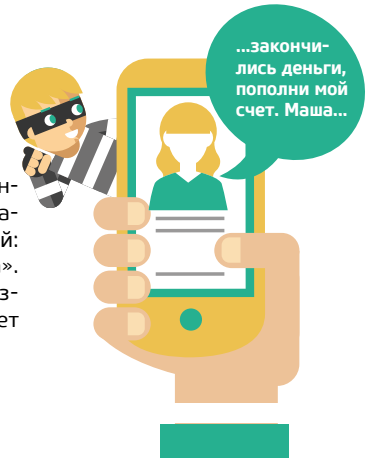
Откликаясь на просьбу о помощи, соблюдайте меры предосторожности: лично набирайте продиктованный номер телефона, уточняйте, кто должен ответить на другом конце линии. Если понимаете, что не сможете воспрепятствовать побегу с вашей собственностью, можно отговориться тем, что села батарейка.

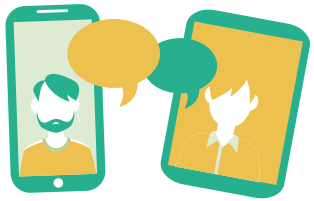
ПРОСЬБА ОДОЛЖИТЬ ТЕЛЕФОН НА УЛИЦЕ ДЛЯ ЗВОНКА

Ситуации бывают разные, может, человеку действительно крайне важно осуществить звонок. Но мошенники звонят на короткие номера либо успевают за короткое время набрать комбинацию для перевода денег. Также они могут банально убежать с вашим телефоном.

«ПОЛОЖИ НА СЧЕТ 200 РУБ., ПОТОМ ОБЪЯСНЮ. ЛЕНА»

Самый массовый и трудно доказуемый вариант мошенничества, с которым сталкивался почти каждый владелец мобильного телефона. СМС-сообщение с просьбой: «У меня закончились деньги, пополни мой счет. Маша». Некоторые абоненты, особенно люди пенсионного возраста, пополняют счет мошенников, думая, что пишет кто-то из знакомых или близких людей.





ЕСЛИ ДРУГ ПОПАЛ В БЕДУ...

Злоумышленники сообщают вам по телефону, что ваш родственник или друг попал в аварию/отделение милиции и так далее и, пользуясь вашими смешанными чувствами, просят либо продиктовать им номер карты пополнения счета, чтобы он мог выйти на связь с вами, либо отдать им энную сумму денег за его вызволение. В последнем случае сумма выкупа может исчисляться десятками тысяч рублей, и многие мошенники их получают!

Не предпринимайте никаких действий, лично не убедившись, что ваш родственник или знакомый точно попал в затруднительную ситуацию. Самое простое – просто позвоните ему.

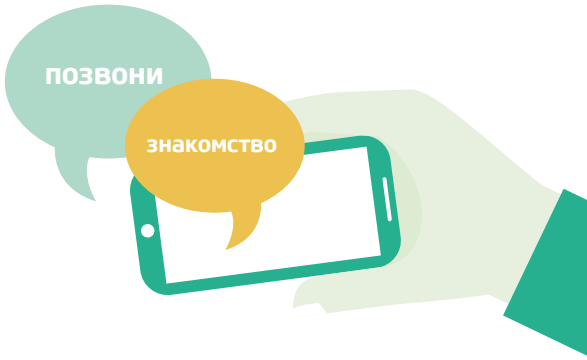
«ВЕРНИТЕ, ПОЖАЛУЙСТА, МОИ ДЕНЬГИ»

Пользователь мобильного телефона получает СМС-сообщение о том, что кто-то перевел на его счет определенную сумму. Чаще всего она невелика – 100–200 рублей. Через несколько минут приходит и другая эсэмэска с просьбой вернуть ошибочно переведенные деньги.

«ПЕРЕЗВОНИ МНЕ»

С неизвестного номера поступает звонок или сообщение с просьбой «перезвонить» или более интригующего содержания – «перезвонить и познакомиться с симпатичной девушкой / молодым человеком».

Звонки на такие номера чаще всего тарифицируются по завышенным расценкам, а на другом конце провода никакого обещанного знакомого или нового знакомства не обнаруживается.



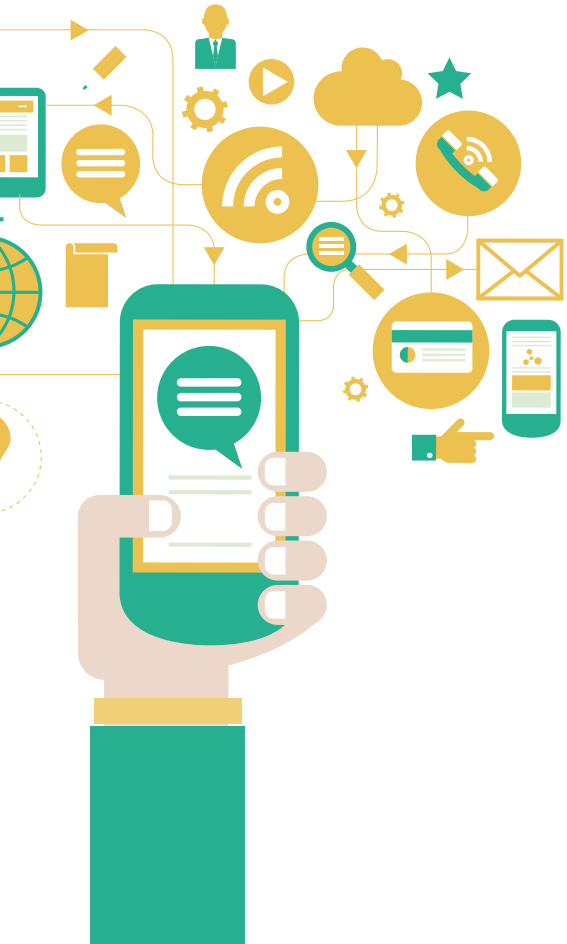
Часто такие сообщения отправляются из Интернета – в этом случае номер отправителя не сообщается, вместо него на дисплее адресата появляется короткий номер, максимально похожий на служебное сообщение.

Если доверчивый абонент решит вернуть деньги, он может недосчитаться на своем счете гораздо большей суммы.

«ГОВОРИТ СЛУЖБА ПОДДЕРЖКИ»

Вам поступает звонок с неизвестного номера либо номер звонящего вовсе скрыт: «Уважаемый абонент, с вами говорит дежурный инженер Иван Иванов. Нашей службой проводится перевод телефонов на другую частоту связи (это лишь пример, вариантов может быть множество). Номер телефона, баланс, все остальное не изменится, не волнуйтесь! Наберите на клавиатуре телефона «звездочку», а потом цифры...»

Стоп! Как только вы наберете продиктованную комбинацию и вышлете ее по СМС, с вашего мобильного счета будут переведены средства. И вернуть их вам не сможет ни сотовый оператор, ни милиция. Вы самостоятельно воспользовались услугой «Мобильный перевод», которая есть у любого федерального оператора сотовой связи.



ВЫМАНИВАНИЕ ПАРОЛЕЙ

Ваши пароли должны знать только вы. Это аксиома. Однако мошенники используют множество уловок, чтобы их выманить. Например, вам звонит ребенок с просьбой сообщить код, который придет вам в СМС-сообщении, объясняя это тем, что он ошибся, указывая номер телефона. Последствия такого шага могут быть разными, самый безобидный вариант – с вашего счета будет списано 100–200 рублей.

Другой распространенный прием – эсэмэска с номера телефона вашего знакомого с примерным текстом: «Хочу сделать тебе подарок! Сообщи мне код, который получишь на телефон». Или просят помочь – мол, телефона под рукой нет, нужно где-то ввести код подтверждения. Не спешите слать в ответ код. Велика вероятность, что телефон взломан и аферисты рассылают сообщения без ведома настоящего владельца номера.

Еще раз напомним: никому не сообщайте ваши пароли и коды подтверждения.

ОБЪЯВЛЕНИЯ КУПЛИ-ПРОДАЖИ НА САЙТАХ

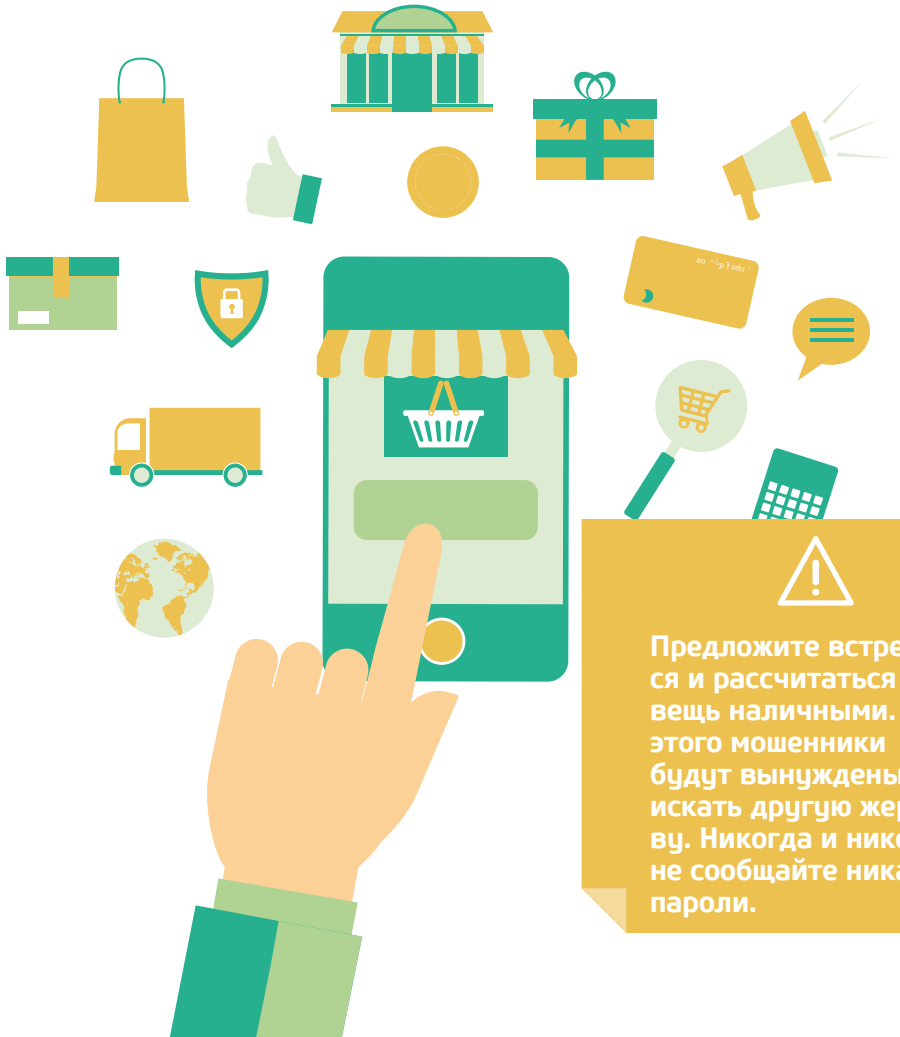
Разместив объявление о продаже или покупке вещей в Интернете, будьте осторожны и не попадитесь на такое мошенничество:

– Алло, здравствуйте, вы еще не продали велосипед? Нет? Ой, как здорово! У меня жене такой как раз нужен. Только я из другого города, но это ничего – я вам доверяю и сейчас переведу деньги. А жена завтра приедет и заберет, она у вас там по делам будет. Какой у вас номер карты?

Дальше – самый тонкий момент. Чтобы украсть ваши средства, преступникам мало знать номер банковской карточки, необходим еще и код подтверждения операции. Как вариант продолжение беседы может быть таким:

– ...Чтобы оплатить, мне нужно присоединить вашу карту к нашим корпоративным счетам, с них я оплачу за велосипед. Сейчас вам придет пароль на телефон, продиктуйте мне его.

Речь мошенников быстрая, настойчивая, фразы они повторяют одну за другой, чтобы не дать вам опомниться и сорваться с крючка.



Предложите встретиться и рассчитаться за вещь наличными. После этого мошенники будут вынуждены искать другую жертву. Никогда и никому не сообщайте никакие пароли.

ТЕХНИЧЕСКИЕ СПОСОБЫ КРАЖИ ИНФОРМАЦИИ

Технически кража информации возможна практически с любого цифрового носителя данных, будь то телефон, планшет или компьютер. Причем многие реально действующие способы ассоциируются больше с фантастическими фильмами о технологиях далекого будущего, нежели с реальностью. Это плохая новость. Хорошая заключается в том, что большая часть таких методов весьма дорогостояща и применяется только по специальному заказу. А значит риск стать жертвой столь технологически продвинутых преступников у рядовых граждан невелик.

Однако ряд методов уже получил довольно широкое распространение, поэтому соблюдать ряд мер безопасности необходимо.

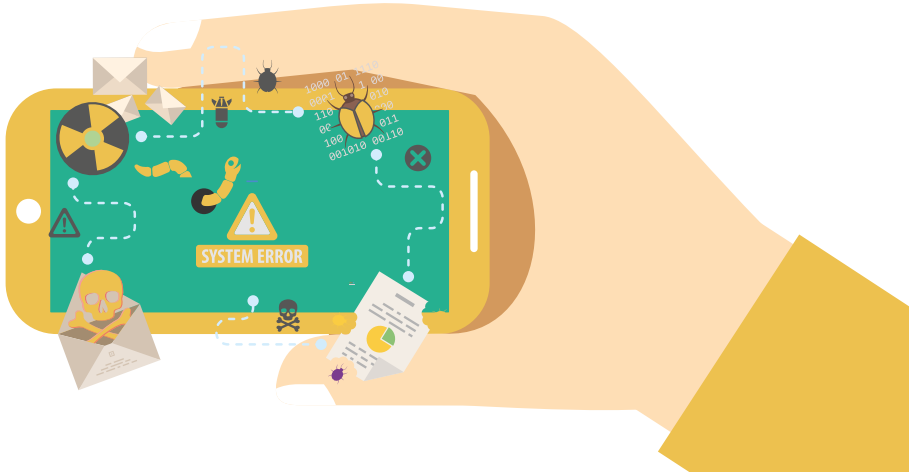
АТАКА «КЛОНОВ»

Технически есть способ сделать полную копию вашего сотового телефона, включая банковскую информацию, пароли доступа, адресную книгу. При наличии современного оборудования для этого необходимо поместить телефон рядом со специальным устройством на несколько минут. Но такая техника – это, скорее, из арсенала спецслужб. На бытовом уровне технически продвинутым мошенникам для «клонирования» требуется примерно час времени и наличие компьютера. Если вы потеряли свой телефон, а потом его вам возвращают, есть риск того, что аппарат побывал в руках специалистов и теперь у него есть двойник. На всякий случай рекомендуем поменять все пароли и коды доступа, а также заглянуть в салон сотовой связи и попросить заменить сим-карту (номер телефона после этой процедуры не изменится).

ТЕЛЕФОННЫЕ ИНФЕКЦИИ

Наибольшее распространение получил такой вид «технического» мошенничества, как «вирусы». В сотовых аппаратах (в первую очередь речь о смартфонах) они действуют ровно по тому же принципу, что и на компьютерах. После установки вся ваша информация может быть переслана преступникам. Под угрозой также ваши банковские счета и собственно сам счет мобильного телефона.

Антивирусные программы сегодня есть и для смартфонов. Установка такого приложения (многие из них распространяются бесплатно) сможет уберечь от неприятностей. Также не стоит открывать ссылки, загружать фотографии, полученные от незнакомых людей. За вполне безобидной картинкой может скрываться вредоносная программа.



ПРАВИЛА БЕЗОПАСНОСТИ:
как не стать жертвой мобильных мошенников

1. Не оставляйте ваш телефон без присмотра в общественных местах.
2. Обязательно установите пароль для разблокировки и доступа к данным. Такая функция есть во всех современных аппаратах.
3. Ценную информацию никогда не храните только в телефоне, дублируйте ее в блокноте, на компьютере.
4. Не покупайте телефоны, бывшие в употреблении, на рынках и в ларьках – большая часть из них украдена, и в случае опознания аппарата прежним хозяином его могут у вас изъять. Если же будет доказано, что вы покупали заведомо краденый телефон, то вам может грозить наказание вплоть до лишения свободы на срок до двух лет.
5. Игнорируйте просьбы положить деньги кому-то на мобильный телефон, если не уверены на 100%, что к вам обращается знакомый человек.
6. **Пользуясь банковскими услугами, в которых задействован номер мобильного телефона, будьте предельно бдительными:**

- **Никогда и никому не сообщайте присылаемые вам пароли и коды подтверждения.**
- **Зная номер вашей банковской карты и телефон, злоумышленники могут попытаться украсть деньги. Храните эту информацию от посторонних.**
- **Представители банка никогда не позвонят вам с просьбой сообщить код подтверждения или код проверки подлинности карты (три цифры, напечатанные на обороте банковской карты возле места для подписи). Если вам поступил такой звонок, немедленно вешайте трубку!**
- **Не открывайте ссылки, не скачивайте прикрепленные файлы, пришедшие от неизвестных вам абонентов.**
- **Сообщения типа «Перезвони мне», «Положи на этот номер сто рублей», пришедшие с незнакомых номеров, игнорируйте. А если абонент есть в вашей адресной книге, все равно перезвоните и уточните. Вдруг его телефон оказался взломан.**

Если вы поняли, что разговариваете с мошенниками и к тому же передали им пароль от банковской карты:

- **Прервите разговор, положите трубку.**
- **Немедленно позвоните в контактный центр своего банка. Такие клиентские службы работают круглосуточно, звонки на них с мобильных телефонов, как правило, бесплатны. С помощью оператора совершите блокировку карты и входа в личный кабинет.**
- **Оставьте заявку на перевыпуск карты банком (иногда это можно сделать по телефону).**
- **Ознакомьтесь с правилами защиты от мошенничества на сайте банка. Если вы среагируете молниеносно, то преступники не успеют перевести деньги, даже если получили от вас пароль. Что касается вкладов, то сначала они переводят средства с депозитов на текущий карточный счет и лишь потом снимают. Поэтому если даже успели «уйти» деньги с карточного счета, то, вполне возможно, со вклада – еще нет.**

7. Отправка СМС-сообщений на сервисные (так называемые короткие) номера чаще всего приведет к списанию средств. Если

Продолжение на стр. 10

же это действительно необходимо, то попробуйте получить уточняющую информацию у вашего оператора сотовой связи, как будет тарифицирована отправка сообщения на данный номер телефона.

8. Никогда не сообщайте никаких персональных сведений (дату рождения, Ф. И. О., данные о родственниках и т. д.), кем бы не представлялся звонящий: сотрудником банка, полиции, менеджером мобильного оператора. Если вам кажется, что это «правильный» звонок, попросите представиться, назвать Ф. И. О., звание и должность, поинтересуйтесь, какой адрес у отделения, офиса. Затем следует узнать телефон этой организации в справочнике и самому перезвонить. Помните: мошенники могут использовать ваши персональные данные в разнообразных преступных схемах.

9. Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу и за него нужно внести залог, штраф, взятку. Не верьте! В 99 случаях из 100 это звонят мошенники. Не предпринимайте никаких действий, не проверив информацию. Имейте в виду, что аферисты – отличные актеры и психологи, они умеют искусно моделировать тембр, интонацию, вдобавок ссылаясь на плохое качество связи. Так что разговаривая якобы со знакомым, попавшим в беду, обязательно задавайте контрольные вопросы. Например, как называется фильм, который вы недавно смотрели.

Будьте внимательны, мошенники с каждым годом становятся все изощреннее в своих способах отъема денег. Наивно полагать, что они способны обхитрить только пожилых людей. В их арсенале полно уловок! «Ключики» можно подобрать и к молодой маме, и к студенту, и к зрелому мужчине.

КУДА ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ

Борьбой с преступлениями в сфере высоких технологий занимается специально созданное для этих целей Управление «К», входящее в структуру Министерства внутренних дел РФ. В отношении лиц, совершающих преступные действия в отношении пользователей мобильной связи, по всей видимости, может быть применено наказание, предусмотренное статьями 159 «Мошенничество» и 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием» Уголовного кодекса РФ. Помощь в противодействии мобильным мошенникам оказывают и операторы сотовой связи. Они стараются поддерживать высокий уровень безопасности предоставляемых услуг, а также заинтересованы сохранять лояльность своих клиентов, поэтому стараются оперативно принять меры для защиты ваших денег и персональных данных.

ПОЛИЦИЯ
112, 911, 102

БИЛАЙН
8 800 700 0611 или 0611
«Уроки мобильной грамотности» от оператора сотовой связи «Билайн». http://moskva.beeline.ru/customers/help/safe-beeline/ugrozy-mobilnykh-moshennikov/uroki-mobilnoi-gramotnosti/

МТС
8 800 250 0890 или 0890
Тематическая страница «Безопасность – это просто» от оператора сотовой связи МТС. http://www.safety.mts.ru/ru/

МЕГАФОН
8 800 550 05 00 или 0505
Тематическая страница «Безопасное общение» от оператора сотовой связи «МегаФон». http://moscow.megafon.ru/bezopasnoe_obschenie/

ТЕЛЕ2
8 800 555 0611 или 611
Тематическая страница «Безопасность» от оператора сотовой связи «Теле2». http://msk.tele2.ru/help/mobilnoe-moshennichestvo/

СПРАВОЧНАЯ ИНФОРМАЦИЯ

Ресурсы в Интернете

- Совместный проект Министерства финансов РФ и Всемирного банка «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации».
  Вашифинансы.рф
- Сайт «Всероссийской недели сбережений».
  http://sberden.ru/
- Региональный центр финансовой грамотности Волгоградской области.
  http://fingram34.ru/
- Региональный центр финансовой грамотности Калининградской области.
  http://fingram39.ru/
- Комитет администрации Алтайского края по финансам, налоговой и кредитной политике.
  https://fin22.ru/fingramm/
- Региональная программа Архангельской области «Повышение уровня финансовой грамотности населения и развитие финансового образования в Архангельской области в 2014–2019 гг.».
  http://dvinaland.ru/-j9vjdp5w
- Региональная программа «Повышение финансовой грамотности населения Республики Татарстан».
  http://tatarstan.ru/fingramota
- Региональная программа «Повышение уровня финансовой грамотности населения Ставропольского края и развитие финансового образования в Ставропольском крае на 2014–2016 гг.».
  http://www.mfsk.ru/training/fin_gram
- Проект «Ваши личные финансы» (Томская область).
  http://vlfin.ru
- Управление «К» МВД России, специализирующееся на расследовании преступлений в сфере компьютерных технологий.
  https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

Полезные книги

- Пятенко С., Сапрыкина Т. **«Личные деньги. Антикризисная книга»**. – М., 2010.
- Пятенко С., Сапрыкина Т. **«Экономический кризис и личные финансы»**. – М., 2009.
- Смирнова Н. **«Про кредиты. Серия: Антикризисный штаб Павла Астахова»**. – М.: «Эксмо», 2009.