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»

Интернет-мошенники

Дружи с финансами
НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН

Москва, 2016

ПОНЯТИЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Интернет – кладезь информации, неисчерпаемый источник общения, бездонное море пользовательских приложений и бескрайние просторы для действий различных криминальных и полукриминальных личностей.

С точки зрения закона мошенничеством является хищение имущества, которое выполняется посредством обмана или злоупотребления доверием. То есть похищение чужих денег или иных ценностей при помощи Интернета является точно таким же уголовным преступлением, как и деяние, совершенное в реальной жизни.

Согласно социологическим опросам, каждый пятый житель России либо не осведомлен вовсе, либо имеет весьма смутное представление о том, какие опасности могут подстерегать его на просторах Всемирной паутины. В данной брошюре рассказывается о наиболее типичных способах сетевого мошенничества. Конечно, способов, которые используют аферисты, значительно больше, но ознакомившись с этими примерами, а также соблюдая правила, приведенные на стр. 10, вы наверняка сможете распознать расставленную ловушку и не угодить в нее. Предупрежден – значит вооружен!

СОДЕРЖАНИЕ

ПОПРОШАЙКИ В СЕТИ

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать, передавать деньги или нет.

СОСТАВЛЯЕМ ГОРОСКОП

Интернет переполнен объявлениями, предлагающими составить персональный гороскоп – быстро, качественно и бесплатно. Требуется лишь заполнить анкету (имя, фамилия, дата рождения) и оставить адрес электронной почты для обратной связи.

Любители астрологии указывают требуемые данные, но вместо гороскопа на почту приходит письмо с еще одним условием: для получения звездных предсказаний нужно выслать СМС-сообщение с набором из определенных цифр. После чего гороскоп может быть пришлют, а может быть, и нет. Как повезет.

Предложения об отправке СМС-сообщений нужно игнорировать. За каждую эсэмэску со счета вашего телефона будет списано несколько сотен рублей!

«ВАШ АККАУНТ ЗАБЛОКИРОВАН»

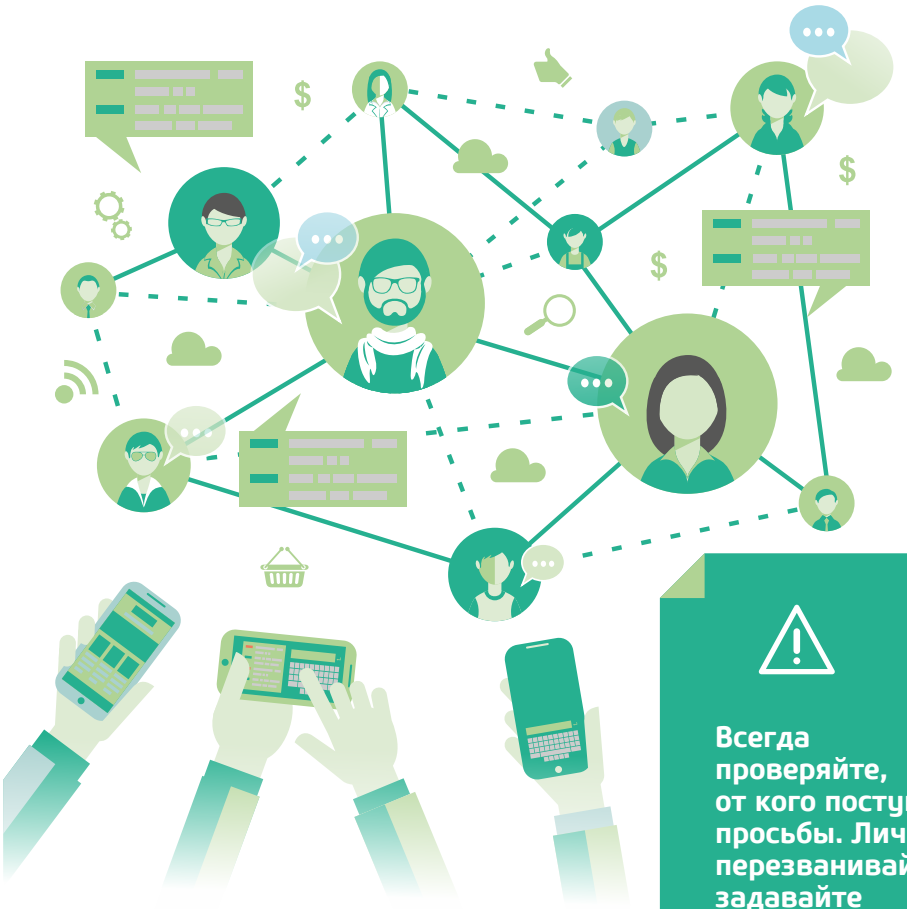
К вашему аккаунту в социальных сетях привязан определенный адрес электронной почты. Если вам вдруг придет сообщение типа:

«В системе (далее будет указано название используемой вами социальной сети, например «Одноклассники» или «ВКонтакте») зарегистрирована заявка на восстановление доступа страницы, к которой привязан данный почтовый адрес. Если вы этого не делали и это ваша страница, вам необходимо срочно отменить запрос на эту операцию по ссылке...»

Ни в коем случае не переходите по ссылке! Удаляйте письмо, не раздумывая. Вы столкнулись с попыткой так называемого фишинга. С английского это слово можно перевести как «выуживание». Злоумышленники создали сайт-фальшивку, копирующий реальную страницу социальной сети. После того как вы введете пароль от своего аккаунта, контроль над вашей учетной записью перейдет в руки мошенников.

Самостоятельно (а не по ссылке из письма!) наберите адрес сайта в интернет-браузере. Введите логин и пароль. В случае возникновения проблем с доступом обратитесь в службу поддержки социальной сети.

МОШЕННИЧЕСТВА В МЕССЕНДЖЕРАХ (ПРОГРАММЫ ДЛЯ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ – SKYPE, VIBER, WHATSAPP И ДР.)



Переписка при помощи мессенджеров содержит такие же опасности, как и общение по электронной почте: рассылка спама, ссылок на сайты-фальшивки (фишинг) и так далее. Иногда мошенники могут обратиться к вам от имени вашего знакомого, взломав его учетную запись. Как правило, речь пойдет о просьбе типа «Срочно положи деньги на вот этот номер телефона. Я потом перезвоню и все объясню».

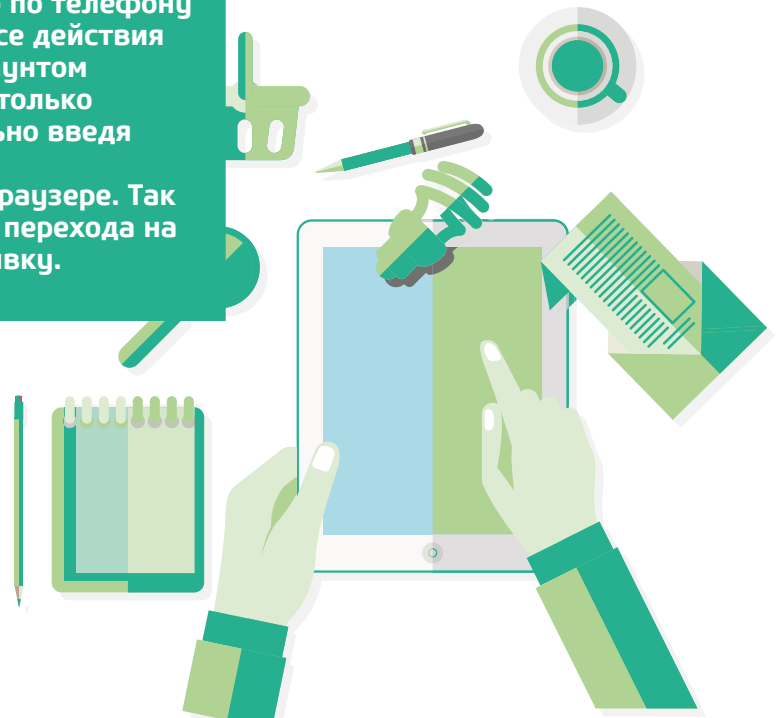
Всегда проверяйте, от кого поступают просьбы. Лично перезванивайте, задавайте вопросы, ответы на которые никто, кроме вашего знакомого, знать не может.

ПИСЬМА ЯКОБЫ ОТ АДМИНИСТРАЦИИ ПЛАТЕЖНОЙ СИСТЕМЫ

Платежи через Интернет имеют массу преимуществ – это удобно и быстро. Но при этом следует проявлять такую же осмотрительность, как и при обращении с наличными или деньгами на банковских картах. Желающих присвоить ваши средства в Интернете не меньше, чем в реальном мире.

Запомните: ни одна платежная система не предложит своим клиентам выслать пароль по электронной почте или сообщить его по телефону оператору. Все действия с вашим аккаунтом совершайте, только самостоятельно введя адрес сайта в интернет-браузере. Так вы избежите перехода на сайт-фальшивку.

Один из самых распространенных способов – рассылка писем якобы от администрации платежной системы. Например, с предложением установить программное обеспечение на свой компьютер, чтобы обезопасить проведение платежей. К таким письмам приложен и файл с программой-«защитником». Другой вариант – уведомление о блокировке вашего счета. Чтобы этого избежать, нужно нажать на указанную ссылку (открывается сайт, один в один напоминающий интернет-страницу платежной системы) и ввести свои персональные данные. Иногда мошенники действуют и вовсе незатейливо – просят прислать логин и пароль, ссылаясь, скажем, на проведение технических работ. Итог будет один – выполнив все инструкции, вы лишитесь своих денег.



АФЕРЫ, СВЯЗАННЫЕ С ИНТЕРНЕТ-МАГАЗИНАМИ

Через Интернет вам могут предложить приобрести все что угодно, а распознать подделку при покупке через Сеть бывает сложно. Во-первых, обращайте внимание на цены. Вас должна насторожить стоимость, которая намного ниже, чем в других местах. Поверьте, никто не продаст вам, к примеру, флагманскую модель телефона в два-три раза дешевле, чем она стоит в среднем по рынку. Отсутствие полных контактных данных продавца, таких как телефон и фактический адрес, – повод поискать другой интернет-магазин. Всегда перезванивайте и подробно выясняйте все характеристики интересующего вас товара. Неуверенные, а тем более неправильные ответы свидетельствуют о том, что вы говорите с жуликами.

Не платите за интернет-покупки банковскими переводами или через платежные системы. Настаивайте на расчетах с курьером после доставки и внимательного осмотра товара.

ОСТОРОЖНО: ВИРУС!

Компьютеры, как и люди, могут заболеть, подхватив вирусы. На сегодняшний день вариантов «цифровых инфекций» существует неисчислимое множество. Самые зловредные из них имеют общие черты. Их задачей может быть скачивание персональных данных с вашего компьютера, воровство паролей от сайтов или платежных систем и так далее. Причем болезнь может переноситься «на ногах». Пользуясь компьютером, вы можете и не подозревать, что он давно заражен вирусом и все это время пересылает информацию мошенникам.

Не экономьте на антивирусных программах. Всегда устанавливайте самые актуальные версии и регулярно обновляйте их. Не открывайте файлы, приложенные к письмам с неизвестных вам адресов.

МОШЕННИКИ В ИНТЕРНЕТЕ – КУДА НА НИХ ЖАЛОВАТЬСЯ?

Если вы столкнулись с мошенничеством в Интернете, то жаловаться следует туда же, куда обращаются в случае обычного хищения, – в правоохранительные органы. Не стоит думать, что раз вы не знаете мошенника в лицо, то дело безнадежно. Не отказывайтесь от подачи жалобы и по причине небольшой суммы похищенного. Вполне возможно, что ваша жалоба окажется далеко не первой, и сведения, сообщенные именно вами, помогут вывести злоумышленников на чистую воду.

Интернет-преступлениями в структуре Министерства внутренних дел РФ занимается Управление «К». Подать официальное заявление можно, например, через Интернет на официальном интернет-ресурсе МВД России. Старайтесь припомнить как можно больше деталей (названия сайтов, ник злоумышленника на форуме, номера счетов и транзакций, адреса электронной почты и пр.). Второй вариант – принести заявление в ближайшее отделение полиции, после первичной проверки документы все равно попадут специалистам Управления «К».

КТО ПОМОЖЕТ, КРОМЕ ПОЛИЦИИ

В случае, если деньги были перечислены мошеннику через электронную платежную систему (например, WebMoney), стоит обратиться в службу поддержки клиентов. Есть шанс, что электронный счет аферист будет заблокирован. Это облегчит дальнейший возврат ваших денег.

На мошеннический сайт можно пожаловаться и на специальных сервисах, предназначенных для блокирования вредоносных сайтов. В частности, такие жалобы рассматриваются Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (http://rkn.gov.ru/).

Пожаловаться на вредоносные сайты можно и в службу поддержки крупных поисковых систем, таких как

Яндекс **«Яндекс» (https://webmaster.yandex.ru/delspam.xml?ncrnd=1383)**

@mail.ru **или Mail.ru (https://help.mail.ru/mail-help/security/fraud).**

Аналогичные сервисы есть и на сайтах социальных сетей.

ПРАВИЛА ИНТЕРНЕТ-БЕЗОПАСНОСТИ

1. Главное правило – **не воспринимайте Интернет как нечто виртуальное** и оторванное от настоящей жизни. Грань между цифровым миром и вашей повседневностью чрезвычайно тонка. Вы же не будете рассказывать первому встреченному на улице человеку ваши секреты или, скажем, комбинацию цифр от сейфа? Вот и в Интернете делать этого не следует ни в коем случае.

2. Старайтесь **не открывать сайты платежных систем по ссылке** (например, в письмах). Обязательно проверяйте, какой адрес (https://www....) указан в браузере. Помните, что в Интернете много мошеннических сайтов, копирующих до мелочей легальные ресурсы. Сравните два адреса: www.primer.ru (настоящий сайт) – www.prymer.ru (сайт-фальшивка).

3. Никогда и **никому не сообщайте ваши пароли**. Вводить пароли можно и нужно только на самих сайтах платежных систем, страницах социальных сетей и т. д. **Не ленитесь придумывать сложные комбинации** для доступа к различным сервисам и храните их в надежных местах. Самый частый способ взлома личных данных – это элементарный подбор пароля типа «12345» или parol. Возьмите за правило использовать разные пароли для захода на разные интернет-ресурсы.

4. **Не размещайте в общем доступе публикации о дорогостоящих покупках или сделках.** Оставляя сообщения в социальных сетях, избегайте указания своего точного адреса, равно как и сведений о датах планируемой поездки в отпуск. Велик риск, что в ваше отсутствие в квартиру наведаются не виртуальные, а вполне реальные воры.

5. **Не давайте деньги в долг неизвестным вам лицам** – в Интернете не существует гарантий возврата кредитов.

6. **Не принимайте предложений об участии** в различных проектах, **если это требует уплаты** взноса. Например, устройство на удаленную работу, знакомства.

7. Выходя в Интернет с **общественного компьютера** или подключая свое оборудование к публичным сетям (например, в кафе), **не совершайте онлайн-покупки**, не заходите на сайты под своим логином.

8. **Не соглашайтесь на просьбы о перечислении денег на лечение** и иные благотворительные цели, тщательно не перепроверив всю информацию.

ПОЛЕЗНЫЕ ССЫЛКИ

1. Управление «К» МВД России (специализируется на расследовании преступлений в сфере компьютерных технологий).
https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

2. Образовательно-выставочный проект «Дети в Интернете» информирует детей, родителей и учителей о потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз и полезных возможностях глобальной сети для образования, развития, общения и досуга.
http://detionline.com/

3. Брошюра «Безопасность детей в Интернете» от компании Microsoft.
http://www.ifap.ru/library/book099.pdf

4. Фонд развития Интернета – проекты, направленные на развитие и безопасное использование глобальной сети.
http://www.fid.su/

5. Служба по предотвращению интернет-мошенничества компании «МегаФон»
http://stopfraud.megafon.ru

6. Служба по предотвращению интернет-мошенничества компании «МТС».
http://www.mts.ru/help/useful_data/safety/

7. Служба по предотвращению интернет-мошенничества компании «Билайн».
http://safe.beeline.ru/index.wbp

8. Центр безопасности от компании Microsoft.
https://www.microsoft.com/ru-ru/security/default.aspx

9. «Безопасность детей в Интернете – что могут взрослые?». Материалы сетевого сообщества «Начальная школа».
http://www.nachalka.com/bezopasnost

ЭТО ЗАКОН!

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

4. «Правила оказания услуг связи по передаче данных» (утверждены Постановлением Правительства Российской Федерации от 23.01.2006 № 32).

5. «Правила продажи товаров дистанционным способом» (утверждены Постановлением Правительства Российской Федерации от 27.09.2007 № 612).