- При получении звонков или смс о блокировке карты позвоните в банк по официальному номеру, указанному на обратной стороне карты, не перезванивайте обратным звонком, а наберите номер самостоятельно.
- Не переводите деньги неизвестным лицам на неизвестные расчетные счета и телефонные номера через анонимные платежные системы.
- Не соглашайтесь на предоплату при покупке (продаже) имущества через бесплатные интернет-порталы, такие как avito.ru, auto.ru и прочие.
- Не отправляйте о себе слишком много информации при совершении интернет-покупок (данные счетов, пароли, домашние адреса и телефоны и так далее).
- Не подтверждайте операции, которые не проводили.
- Не заходите на подозрительные сайты.
- Не переходите по сомнительным ссылкам и не открывайте подозрительные вложения к письмам.
- Не отправляйте СМС-сообщения, не вводите свой номер телефона на сомнительных сайтах при регистрации.
- Не размещайте персональную и контактную информацию о себе в открытом доступе, а также слишком подробную информацию о себе в социальных сетях.
- Никогда не совершайте покупки в непроверенных интернет-магазинах, особенно если требуется внесение предоплаты.
- Установите комплексную систему защиты (антивирус, антиспам-фильтр). Используйте брандмауэр, он поможет предотвратить кражу конфиденциальных данных или другие подобные действия. Используйте только лицензионное антивирусное программное обеспечение с обязательным и систематическим обновлением баз вирусных сигнатур.
- Перед использованием скачиваемых файлов обязательно проверяйте их антивирусными приложениями на наличие вредоносных и потенциально вредоносных программ.
- Периодически обновляйте логины и пароли, используемые в интернет-пространстве при регистрации, не используйте один пароль для всех Интернет-ресурсов.

Уполномоченный по правам человека в Пермском крае призывает граждан к бдительности во избежание совершения фактов мошенничества. Предупредите своих родственников и знакомых, не поддавайтесь на уловки мошенников!

В случае возникновения подобных ситуаций и особенно если Вы или Ваши близкие стали жертвой мошенников необходимо незамедлительно обращаться в ближайший отдел полиции или позвонить 102/112 (для любых операторов мобильной связи).

Уполномоченный по правам человека в Пермском крае
Миков Павел Владимирович
Адрес: 614990, г. Пермь, ул. Ленина, 51; каб. 229
Тел.: 8 (342) 217-76-70
E-mail: ombudsman@uppc.permkrai.ru
Сайт: ombudsman.perm.ru

Прием граждан осуществляется по адресу:
Адрес: г. Пермь, ул. Куйбышева, 8
Дни приёма:
вторник с 10.00 до 13.00
четверг с 17.00 до 20.00

Прокуратура Пермского края:
Адрес: 61499, г. Пермь, ул. Луначарского, 60
Тел.: 8 (342) 217-53-10
Справочная по обращениям: 8 (342) 217-53-08
Сайт: www.prokuror.perm.ru
Интернет-прием: http://prokuror.perm.ru/faq1/form/

Главное управление МВД России по Пермскому краю
Адрес: 614990, г. Пермь, Комсомольский пр. 74
Дежурная часть: (342) 246-77-00
«Телефон горячей линии»: (342) 246-88-99
E-mail: gumvd59@mvd.ru
Сайт: 59.мвд.рф

Следственное управление Следственного комитета Российской Федерации по Пермскому краю
Адрес: 614064, г. Пермь, ул. Героев Хасана, д. 53в
Тел.: (342), 249-54-55
Телефон доверия: (342) 249-54-64
Сайт: perm.sledcom.ru

Отпечатано в типографии «Форвард-С» (ИП Худяков С. А.). 614064, г. Пермь, ул. Героев Хасана, 55б. Тел.: (342) 205-54-41. E-mail: forward-s2011@yandex.ru. Тираж 500 экз. Заказ №1382.

Уполномоченный по правам человека в Пермском крае

Как не стать жертвой телефонных и интернет-мошенников

2020

Увеличение количества пользователей сети Интернет и сотовой связью неизбежно приводит и к росту преступлений в этой сфере с использованием информационно – телекоммуникационной сети. Жертвой телефонных и интернет-мошенников может стать любой человек.

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (ч. 1 ст. 159 УК РФ);

Мошенничество в сфере компьютерной информации – хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ч. 1 ст. 159.6 УК РФ)

Основными видами мошенничества по телефону являются:

- звонки о том, что кто-то из родственников попал в беду и необходима сумма для решения вопроса о прекращении уголовного дела, освобождении и т.д.;
- звонки о желании приобрести товар, размещенный на различных Интернет-сайтах гражданами в объявлениях о продаже. В таких случаях мошенник звонит по объявлению и просит продиктовать номер банковской карты для перечисления аванса за товар, а потом просит сообщить различные коды доступа, с целью получения доступа к банковскому счету жертвы;
- звонки от имени сотрудников банков о блокировке банковской карты, задолженности по кредиту и т.п. В ходе общения мошенники просят сообщить различные коды доступа, либо совершить какие-либо операции, в результате злоумышленники получают доступ к банковскому счету жертвы;
- СМС-сообщения либо звонки о каком-либо выигрыше, для получения которого необходимо перечислить некую сумму.

Компьютерное (или «кибер-») мошенничество представляет собой новую, динамично развивающуюся категорию преступлений. Беспечность в использовании Интернет-ресурсов и выборе скачиваемого интернет-контента зачастую приводят к утрате персональных данных, в том числе и сведений о банковских реквизитах пользователя.

Основными способами мошенничества в Интернет-пространстве являются:

- размещение мошенниками на сайтах бесплатных объявлений предложений о намерении покупки или продажи какого-либо имущество, в последующем, в ходе общения злоумышленник предлагает осуществить предоплату или аванс. В результате, перечислив денежные средства, жертва не получает ни услугу, ни товар;
- неправомерный доступ к конфиденциальным данным пользователей («фишинг») – при данном способе злоумышленники создают точную копию официального сайта банка или интернет-магазина. Перейдя на подложный сайт, ничего не подозревающий пользователь осуществляет привычные операции – вводит свои логин и пароль, оплачивает товары путем ввода реквизитов банковской карты, при этом указанные им данные попадают в руки мошенников. Переход на подобный подложный сайт может быть осуществлен как через поисковую систему интернет-браузера, так и по ссылке, приведенной в электронном письме. Полученные данные могут использоваться для изготовления поддельных банковских карт с целью обналичивания денег, либо их траты в виртуальной среде;
- мошеннические интернет-магазины, чаще всего такие интернет-магазины работают по 100% предоплате. Цена на товар, как правило, ниже среднерыночной;
- объявления в социальных сетях о помощи деньгами, на лечение ребенка, родственника и прочее. Такие объявления могут быть вовсе фиктивными, либо мошенники могут использовать реальные объявления, в том числе с сайтов известных благотворительных организаций, с изменёнными банковскими реквизитами;
- разнообразные схемы мошенничества с удаленной работой, когда злоумышленники представляются в виде работодателей и предлагают быстрый заработок. При этом для начала работы необходимо зарегистрироваться на платном интернет-ресурсе либо произвести иные платежи.

Перечисленные способы телефонного и кибермошенничества не являются исчерпывающими, существует множество иных вариаций подобных схем, а также мошенниками разрабатываются все новые механизмы хищения денежных средств.

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

- Необходимо проявлять осторожность в общении по телефону с незнакомыми людьми и при совершении финансовых операций в сети Интернет, помнить о необходимости проверки сведений.
- Ни под каким предлогом не сообщайте никому информацию, размещенную на вашей банковской карте (номер, дату, ПИН-код карты, трехзначный CVV/CVC-код с обратной стороны карты или одноразовый пароль из СМС), цифровые или буквенные коды, логины и пароли доступа, свои персональные данные.
- Не передавайте карту посторонним лицам.
- При утрате банковской карты незамедлительно обратитесь в банк с целью блокировки карты.
- В случае потери мобильного телефона с подключенной услугой «Мобильный банк», следует срочно обратиться в контактный центр банка для блокировки услуги.