Финансовое мошейничество

Основные виды финансового мошенничества и как не попасться на уловки злоумышленников

С развитием технологий в жизни современного человека появились новые финансовые возможности – управление счетами на расстоянии, онлайн-оплата покупок, бесконтактные платежи через телефон и многое другое. К сожалению, и изобретательность кибермошенников не остается на месте – злоумышленники придумывают новые способы обмана. Чтобы не попасться на уловки аферистов, нужно помнить о простых правилах финансовой безопасности. В нашем дайджесте расскажем про основные виды финансового мошенничества и как его избежать. Материал подготовлен на основе проекта Банка России «Финансовая культура» и состоит из основных блоков:

1. Телефонные мошенники.
2. Финансовое мошенничество.
3. Черные кредиторы.

Телефонные мошенники

Будьте бдительны!

Если вам звонят из банка и просят сообщить персональные данные или информацию о карте/счете — будьте бдительны, это могут быть мошенники! Злоумышленники используют специальные технологии и на экране вашего телефона высвечивается официальный номер банка. Они могут обратиться к вам по имени-отчеству и попросить секретные сведения о карте или счете. Например, чтобы остановить подозрительную операцию.

Помните о том, что сотрудники банка не запрашивают персональные данные или информацию о карте и счете. Если звонят с подобными вопросами – это мошенники.

Чтобы этого не случилось, следуйте инструкции:

- Не говорите и не вводите ПИН-код, трехзначный код с обратной стороны карты, или одноразовый пароль из СМС.
- Не набирайте на телефоне никаких комбинаций и не переходите по ссылкам.
- Положите трубку. Позвоните в банк по официальному номеру — он есть на сайте или обратной стороне карты.
- Самостоятельно наберите номер на клавиатуре телефона.

Не перезванивайте обратным звонком, так снова можно попасть к мошенникам.

Теперь не проведешь!

3 простых правила финансовой безопасности, которые помогут сориентироваться в сложный момент:

- Звоните в банк сами

Набирайте номер вручную. Телефон горячей линии указан на обратной стороне карты и на официальном сайте банка. Перезванивая на номер, с которого пришел подозрительный звонок или сообщение, вы рискуете снова попасть к мошенникам.

- Сосредоточьтесь

Если банк выявит подозрительную транзакцию, он приостановит ее на срок до двух суток. У вас есть до 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.

- Не говорите никому секретные коды

Если вас убеждают продиктовать или ввести CVC/CVV-код на обратной стороне карты, пин-код или коды из СМС — это мошенники! Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

Финансовое мошенничество

Как распознать мошенников? Что делать, если вас все-таки обманули? Как защитить себя и свою семью? Скорее всего один из этих вопросов вы когда-нибудь задавали себе.

Мы подготовили памятку «Как работать с банковской картой и не попасться на уловки мошенников»:

- Осмотрите банкомат. На картоприемнике не должно быть посторонних документов, клавиатура не должна шататься.
- Набирая пин-код, прикрывайте клавиатуру рукой.
- Подключите мобильный банк и СМС-уведомления.
- Если совершаете покупки через интернет, никому не сообщайте секретный код из СМС.
- Никогда не теряйте из виду вашу карту.

Обокрали! Что делать?

3 простых шага в случае незаконного списания денег с банковской карты:

1. Позвоните в банк (номер есть на обороте карты или на главной странице сайта банка) и заблокируйте карту.

2. Запросите выписку по счету и напишите заявление о несогласии с операцией.
3. Обратитесь с заявлением в полицию.

Кибермошенничество. Как не попасться?!

Кибермошенники придумывают разные способы обмана. На пример, вам приходит СМС или письмо «от банка» со ссылкой, просьбой перезвонить или уведомление о крупном выигрыше. Или звонят «из банка» и просят отправить личные данные. Или пишут в социальных сетях от имени родственников или друзей, которые попали в беду, и просят перевести деньги на неизвестных счет.

Как обезопасить себя от кибермошенников:

1. Не переходите по неизвестным ссылкам, не перезванивайте на сомнительные номера.
2. Никому не сообщайте персональные данные, тем более пароли и коды.
3. Не храните данные карт на компьютере или в смартфоне.
4. Проверяйте информацию. Если вам звонят и сообщают что-то о вашем счете (по ошибке списали или зачисли деньги), не следуйте никаким инструкциям и срочно сами звоните в банк.
5. Установите на компьютере антивирус.

Черные кредиторы

Знаете ли вы, у кого есть право выдавать кредиты? А как отличить нелегальных кредиторов от легальных? И что делать, если кредитор оказался черным? Сейчас мы все расскажем!

Кто может выдавать кредиты?

Выдавать кредиты и займы на постоянной основе могут только:

- банки
- микрофинансовые организации (МФО)
- кредитные потребительские кооперативы (КПК и СКПК)
- ломбарды

Для этого у них должно быть специальное разрешение Банка России.

Кто такие черные кредиторы?

Если у компании нет разрешения Банка России на выдачу кредитов (или лицензии у банка), а она все равно привлекает клиентов, выдает себя за лицензированную

организацию и кредитует потребителей, то перед вами нелегальный (или черный) кредитор. Нелегальные кредиторы могут действовать по-разному. Например, выдавать кредиты под очень высокие проценты, но при этом не прибегать к откровенному криминалу. А могут использовать преступные схемы, чтобы обманом завладеть деньгами и имуществом клиентов.

Как распознать черного кредитора?

- Проверьте, есть ли компания в реестре на сайте Банка России.

Если компании нет в Справочнике по кредитным организациям или в Справочнике участников финансового рынка на сайте Банка России — это не легальный кредитор. Но даже если вы нашли название компании в списке, будьте внимательны. Мошенники могут подделать сайт, используя название легальной компании. Поэтому пользоваться финансовыми услугами онлайн следует особенно внимательно!

Как черные кредиторы обманывают клиентов?

Часто заемщики не подозревают, что перед ними нелегальная организация. Вот три самые популярные схемы, по которым мошенники привлекают невнимательных клиентов.

1. Предоплата за кредит

Кредитор просит оплатить проверку кредитной истории или страховку, берет комиссию за выдачу кредита, предлагает оплатить услуги нотариуса или членский взнос для вступления в кооператив. Клиент отдает деньги — и «помощник» исчезает.

2. Использование Данных

Клиент приносит в организацию полный пакет документов. Мошенники могут взять кредит от его имени или обнулить его счета.

3. Сомнительные бумаги

Мошенники могут подменить договор и дать клиенту на подпись другие условия, где, например, не указан срок возврата. Это позволит им запросить всю сумму с процентами уже на следующий день.

Если вы столкнулись с черным кредитором

Если кредитор не указан в реестре на сайте Банка России или указан, но нарушает правила — обратитесь в интернет – приемную Банка России и подайте заявление в правоохранительные органы. Если черные кредиторы пытаются взыскать с вас просроченную задолженность, выдавая себя за коллекторов, или поручив это им на самом деле, вы можете обратиться в Федеральную службу судебных приставов. Черным кредиторам только на руку, если пострадавшие от их незаконных действий будут по тем

или иным причинам умалчивать о случившемся. Не верьте, когда вас убеждают, что обращаться за защитой ваших прав бесполезно!

Как не попасть к черным кредиторам? 3 простых правила.

1. Не соблазняйтесь заманчивым предложением

Если вам предлагают подозрительно выгодные условия, убедитесь, что в договоре действительно прописаны все обещания, которые сулит реклама. Не берите кредит, если формулировки двусмысленны или противоречат тому, что написано в рекламе. При необходимости проконсультируйтесь с юристом.

2. Внимательно читайте договор

В документах легального кредитора должны быть четко прописаны порядок заключения договора, выдачи кредита или займа, условия его возврата или использования. Кредитор обязан выдать вам документы или хотя бы ознакомить вас с ними. По закону можно взять документы домой и подумать в течение пяти дней. Условия договора за это время не поменяются.

3. Берите кредит или заем только у легального кредитора

Деятельность легальных кредиторов регулируется законом, в отличие от черных кредиторов.

Следуя простым правилам и проявляя внимательность и бдительность при совершении банковских операций, вы минимизируете риск попадания на уловки мошенников. А это значит, что теперь ваши финансы и благосостояние под надежной защитой полученных знаний!

Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ

- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ

Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ
ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

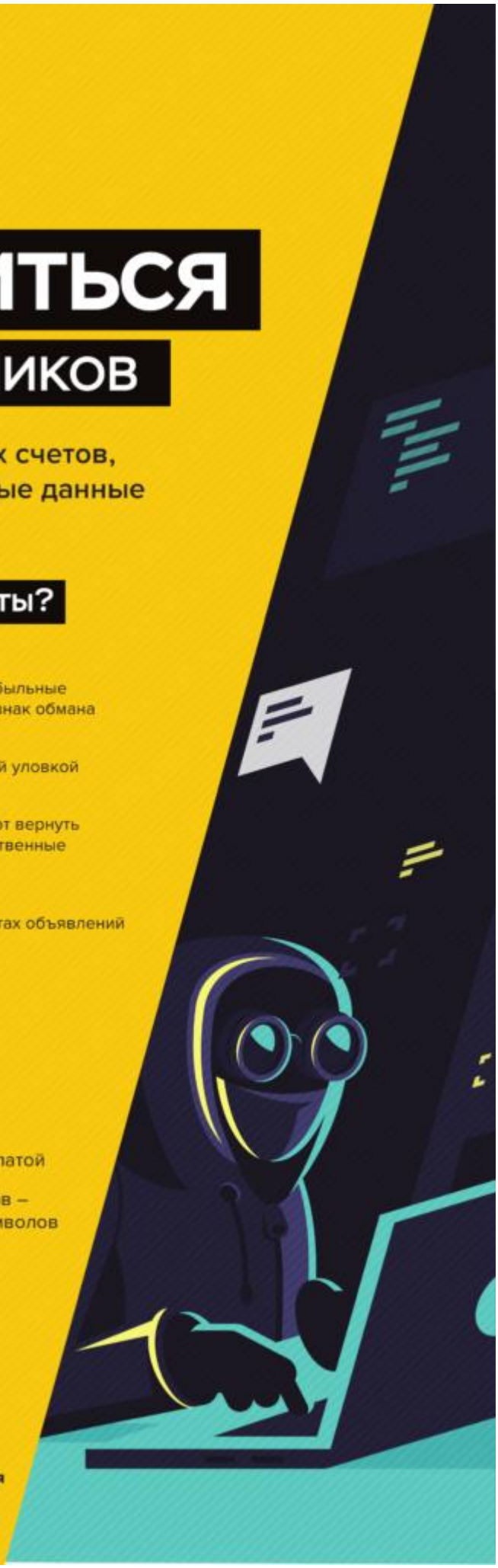
ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на **fincult.info**

Финансовая культура

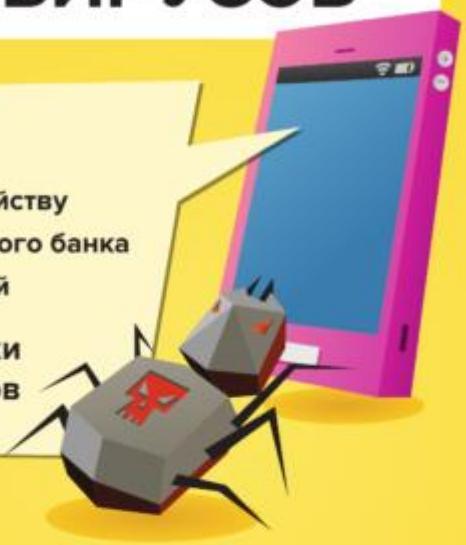
Банк России

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- **Обратитесь в сервисный центр**, чтобы вылечить гаджет
- **Перевыпустите карты, смените логин и пароль** от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- **Используйте антивирус** и регулярно его обновляйте
- **Не переходите по ссылкам** от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- **Обновляйте** операционную систему устройства
- **Избегайте** общедоступных Wi-Fi-сетей

Подробнее о защите гаджетов читайте на fincult.info

Финансовая культура