

Памятки по кибербезопасности

Обещают сверхприбыль?

Гарантируют доход выше,
чем по депозитам?

И никаких рисков?

Будьте бдительны!

За выгодными
условиями могут
скрываться финансовые
пирамиды!



Проверьте на сайте Банка России,
законно ли работает компания:



◀ Есть ли
у нее
лицензия?

cbr.ru/fmp_check/



◀ Нет ли
организации
в списке
нелегалов?

cbr.ru/inside/warning-list/

Осторожно мошенники:

Как не попасть на удочку мошенника



**Вам позвонили / прислали SMS из «Банка»,
гос. учреждений, МВД, Банка России**

- Прервите разговор и перезвоните на «горячую линию» своего банка по официальному номеру телефона
- Ни в коем случае не сообщайте никакие персональные данные звонящему
- Сотрудники банка не запрашивают ваши данные



**Вам позвонили/прислали SMS
с неизвестного номера с просьбой
о помощи близкому человеку**

- Не торопитесь переводить деньги
- Перезвоните знакомому и уточните обстоятельства



**Вам предлагают оплатить пошлину / налог /
процент от суммы гос. поддержки или просят
реквизиты банковской карты для
перечисления денег**

- Любые выплаты государственной помощи предоставляются на безвозмездной основе
- Проверенная информация о мерах государственной поддержки только в официальных источниках:



портал.Госуслуги



обьясняем.рф



моифинансы.рф



fincult.info

Осторожно мошенники:

Как не попасть на удочку мошенника



**Вам позвонили / прислали SMS из «Банка»,
гос. учреждений, МВД, Банка России**

- Прервите разговор и перезвоните на «горячую линию» своего банка по официальному номеру телефона
- Ни в коем случае не сообщайте никакие персональные данные звонящему
- Сотрудники банка не запрашивают ваши данные



**Вам позвонили/прислали SMS
с неизвестного номера с просьбой
о помощи близкому человеку**

- Не торопитесь переводить деньги
- Перезвоните знакомому и уточните обстоятельства



**Вам предлагают оплатить пошлину / налог /
процент от суммы гос. поддержки или просят
реквизиты банковской карты для
перечисления денег**

- Любые выплаты государственной помощи предоставляются на безвозмездной основе
- Проверенная информация о мерах государственной поддержки только в официальных источниках:



портал.Госуслуги



ob'yasnayem.rf



moifinansi.rf



fincult.info

Осторожно мошенники:

Как не попасть на удочку мошенника



**Вам позвонили / прислали SMS из «Банка»,
гос. учреждений, МВД, Банка России**

- Прервите разговор и перезвоните на «горячую линию» своего банка по официальному номеру телефона
- Ни в коем случае не сообщайте никакие персональные данные звонящему
- Сотрудники банка не запрашивают ваши данные



**Вам позвонили/прислали SMS
с неизвестного номера с просьбой
о помощи близкому человеку**

- Не торопитесь переводить деньги
- Перезвоните знакомому и уточните обстоятельства



**Вам предлагают оплатить пошлину / налог /
процент от суммы гос. поддержки или просят
реквизиты банковской карты для
перечисления денег**

- Любые выплаты государственной помощи предоставляются на безвозмездной основе
- Проверенная информация о мерах государственной поддержки только в официальных источниках:



портал.Госуслуги



обьясняем.рф



моифинансы.рф



fincult.info

Как пользоваться цифровыми финансовыми услугами **безопасно**

Как делать правильно?

Сотрудник банка не имеет права запрашивать номер вашей карты, трехзначный номер с обратной стороны карты (CVV / CVC-код) или код-подтверждения из СМС.

Банки НИКОГДА этого не делают



Для отслеживания движения средств по счету нужно подключить СМС или push-уведомления по используемой банковской карте и электронному кошельку (внимание: эта услуга может быть платной).

Совершать покупки в интернете с помощью отдельной дебетовой банковской карты (не зарплатной или той, где хранятся все доступные средства).

Совершать онлайн-покупки только на проверенных сайтах и только убедившись предварительно, что сайт поддерживает протокол 3D-Secure (адрес начинается с букв https, а не http).

Никому не говорить, не записывать и прикрывать рукой при вводе в банкомате или банковском терминале ПИН-код своей банковской карты.

При пользовании банкоматом проявлять осторожность, обращать внимание на посторонних вокруг, на подозрительные устройства и наклейки в местах ввода ПИН-кода и карты.

Не допускать посторонних к банковской карте, электронному кошельку, мобильному телефону, личному компьютеру и не оставлять открытым банковское / платежное приложение после совершения операций.

Использовать сложные и разные пароли, регулярно их менять, никому не сообщать и никогда не пересылать по электронной почте, в СМС и мессенджерах. Идеальный пароль – ассоциативный, который можно не записывать. Если есть опасения забыть пароль – записывать в бумажный блокнот, но в зашифрованном виде.

Незамедлительно сообщать в банк или платежную организацию о потере карты или взломе кошелька.

При скачивании программы проверять, настоящая ли она. Мошенникам удастся размещать даже в надежных магазинах приложений программы, маскирующиеся под государственные сервисы или инвестиционные инструменты госкомпаний. Если разработчик приложения сомнителен – не стоит загружать его.

Регулярно удалять информацию о платежах с помощью очистки буфера файлов (cache) и файлов сохранения данных (cookies).

Устанавливать лицензионные антивирусные программы на все гаджеты (телефоны, компьютеры, планшеты).

Как пользоваться цифровыми финансовыми услугами **безопасно**

Как делать правильно?

Сотрудник банка не имеет права запрашивать номер вашей карты, трехзначный номер с обратной стороны карты (CVV / CVC-код) или код-подтверждения из СМС.

Банки НИКОГДА этого не делают



Для отслеживания движения средств по счету нужно подключить СМС или push-уведомления по используемой банковской карте и электронному кошельку (внимание: эта услуга может быть платной).

Совершать покупки в интернете с помощью отдельной дебетовой банковской карты (не зарплатной или той, где хранятся все доступные средства).

Совершать онлайн-покупки только на проверенных сайтах и только убедившись предварительно, что сайт поддерживает протокол 3D-Secure (адрес начинается с букв https, а не http).

Никому не говорить, не записывать и прикрывать рукой при вводе в банкомате или банковском терминале ПИН-код своей банковской карты.

При пользовании банкоматом проявлять осторожность, обращать внимание на посторонних вокруг, на подозрительные устройства и наклейки в местах ввода ПИН-кода и карты.

Не допускать посторонних к банковской карте, электронному кошельку, мобильному телефону, личному компьютеру и не оставлять открытым банковское / платежное приложение после совершения операций.

Использовать сложные и разные пароли, регулярно их менять, никому не сообщать и никогда не пересылать по электронной почте, в СМС и мессенджерах. Идеальный пароль – ассоциативный, который можно не записывать. Если есть опасения забыть пароль – записывать в бумажный блокнот, но в зашифрованном виде.

Незамедлительно сообщать в банк или платежную организацию о потере карты или взломе кошелька.

При скачивании программы проверять, настоящая ли она. Мошенникам удастся размещать даже в надежных магазинах приложений программы, маскирующиеся под государственные сервисы или инвестиционные инструменты госкомпаний. Если разработчик приложения сомнителен – не стоит загружать его.

Регулярно удалять информацию о платежах с помощью очистки буфера файлов (cache) и файлов сохранения данных (cookies).

Устанавливать лицензионные антивирусные программы на все гаджеты (телефоны, компьютеры, планшеты).

Как пользоваться цифровыми финансовыми услугами **безопасно**

Категорически нельзя:



для оплаты
перейдите по ссылке

отправьте
ваш CVV код

?!



Совершать СМС-платежи на короткие номера для оплаты интернет-услуг и переводов непроверенным получателям (а детям и пожилым родственникам стоит вовсе заблокировать на девайсах возможность переводов на такие номера либо подключить опцию одобрения платежей).

Сохранять пароли, личные данные, номера и другие реквизиты или фотографии банковских карт в онлайн-сервисах или в мобильном устройстве.

Реагировать на сообщения от банка или платежной организации, предлагающие срочно снять наличные или перевести деньги на «безопасный счет».

Совершать онлайн-платежи, подключившись к открытым точкам доступа Wi-Fi (введенная при таком выходе в онлайн платежная информация может стать общедоступной).

Передавать банковскую карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/CVC-код) могут быть использованы мошенниками для интернет-платежа или оплаты покупок.

Оставлять незавершенными платежные онлайн-операции. Если вы передумали оплачивать, нужно удалить данные платежной карты.

Переходить в мессенджеры из агрегаторов частных объявлений для дальнейшего обсуждения деталей купли-продажи в частном порядке. Переводить предоплату за товар незнакомым людям и передавать данные своей платежной карты: CVV/CV C-код, код из СМС или push-уведомлений.

Как пользоваться цифровыми финансовыми услугами **безопасно**

Категорически нельзя:



для оплаты
перейдите по ссылке

отправьте
ваш CVV код

?!



Совершать СМС-платежи на короткие номера для оплаты интернет-услуг и переводов непроверенным получателям (а детям и пожилым родственникам стоит вовсе заблокировать на девайсах возможность переводов на такие номера либо подключить опцию одобрения платежей).

Сохранять пароли, личные данные, номера и другие реквизиты или фотографии банковских карт в онлайн-сервисах или в мобильном устройстве.

Реагировать на сообщения от банка или платежной организации, предлагающие срочно снять наличные или перевести деньги на «безопасный счет».

Совершать онлайн-платежи, подключившись к открытым точкам доступа Wi-Fi (введенная при таком выходе в онлайн платежная информация может стать общедоступной).

Передавать банковскую карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/CVC-код) могут быть использованы мошенниками для интернет-платежа или оплаты покупок.

Оставлять незавершенными платежные онлайн-операции. Если вы передумали оплачивать, нужно удалить данные платежной карты.

Переходить в мессенджеры из агрегаторов частных объявлений для дальнейшего обсуждения деталей купли-продажи в частном порядке. Переводить предоплату за товар незнакомым людям и передавать данные своей платежной карты: CVV/CV C-код, код из СМС или push-уведомлений.

КАК РАСПОЗНАТЬ ФИНАНСОВУЮ ПИРАМИДУ



Финансовая пирамида — это мошеннический проект, который имитирует выгодные инвестиции.

Вас призывают вложить деньги в фиктивный бизнес и агитируют приводить друзей и родственников.

В результате можно потерять не только деньги, но и доверие своих близких.

КАКИМИ БЫВАЮТ ФИНАНСОВЫЕ ПИРАМИДЫ?

Пирамиды могут маскироваться под любые компании: кредитные потребительские кооперативы (КПК), микрофинансовые организации (МФО) и просто интернет-проекты.



*Фантазия обманщиков безгранична.
Они предлагают вложиться в сельское
хозяйство или криптовалюты, открыть
бизнес по франшизе.*

Ключевое отличие от реального бизнеса —
организаторы ничего производят и ни во что
не инвестируют деньги вкладчиков. Мошенники
просто собирают их в свой карман.

ПРИЗНАКИ ФИНАНСОВОЙ ПИРАМИДЫ



Обещают высокий доход

Если вам «гарантируют» десятки или даже сотни процентов в год без всякого риска, это точно аферисты.



Вас просят приводить новых клиентов

И обещают начислить процент от их взноса. Так преступники пытаются побыстрее вовлечь как можно больше людей в свою аферу, собрать с них деньги и скрыться.

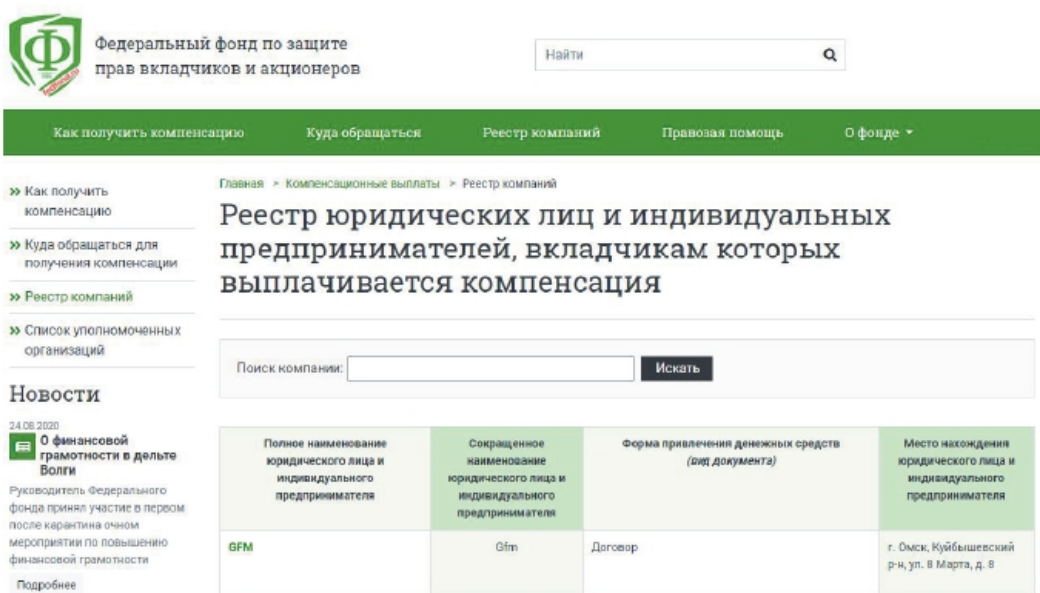


Нет подтверждения инвестиций

Вам показывают только красивые презентации и не дают взглянуть на финансовые документы, бухгалтерскую отчетность. Деньги просят перевести на чей-то персональный счет либо электронный кошелек или же внести наличными, при этом не выдают никаких чеков

МОЖНО ЛИ ВЕРНУТЬ ДЕНЬГИ, ЕСЛИ ПИРАМИДА РУХНУЛА?

Можно, но при условии, что пирамида попала в реестр **Федерального фонда по защите прав вкладчиков и акционеров**. Только он выплачивает компенсации обманутым клиентам некоторых компаний. На сайте Фонда **fedfond.ru** можно посмотреть список пирамид, по которым идут выплаты.



Федеральный фонд по защите прав вкладчиков и акционеров

Найти

Как получить компенсацию Куда обращаться Реестр компаний Правовая помощь О фонде

Главная > Компенсационные выплаты > Реестр компаний

Реестр юридических лиц и индивидуальных предпринимателей, вкладчикам которых выплачивается компенсация

Поиск компании: Искать

Полное наименование юридического лица и индивидуального предпринимателя	Сокращенное наименование юридического лица и индивидуального предпринимателя	Форма привлечения денежных средств (вид документа)	Место нахождения юридического лица и индивидуального предпринимателя
GFM	Gfm	Договор	г. Омск, Куйбышевский р-н, ул. 8 Марта, д. 8

Новости

24.08.2020

О финансовой грамотности в дельте Волги

Руководитель Федерального фонда принял участие в первом после карантина очном мероприятии по повышению финансовой грамотности

[Подробнее](#)

МАКСИМАЛЬНЫЙ РАЗМЕР КОМПЕНСАЦИИ:

- для ветеранов и инвалидов Великой Отечественной войны — **250 000 рублей**
- для всех остальных граждан — максимум **35 000 рублей**



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

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



СМС, МЕССЕНДЖЕРЫ, СОЦСЕТИ



Вам пришло СМС от банка с информацией:

- о заблокированном платеже или карте;
- о выигрыше;
- об ошибочном переводе на ваш банковский счет или мобильный телефон с просьбой вернуть деньги.

— Что делать?



**НЕ ПЕРЕХОДИТЕ
ПО ССЫЛКЕ И
НЕ ПЕРЕЗВНИВАЙТЕ!**

Проверьте информацию, позвонив в банк по номеру, который указан на вашей банковской карте.



Знакомый в соцсетях просит дать в долг или перевести деньги на лечение.

— Что делать?



**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ СРАЗУ!**

Перезвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страницу взломали.



Контактный центр Банка России

8 800 300-30-00
(бесплатно для звонков из регионов России)

+7 499 300-30-00
(в соответствии с тарифами вашего оператора)

300
(бесплатно для звонков с мобильных телефонов)

Все представленные номера доступны для звонков круглосуточно



fincult.info
ПОРА УЗНАТЬ ПРО ДЕНЬГИ ВСЕ



Банк России



**ОСТОРОЖНО:
МОШЕННИКИ!**

НИКОГДА
НЕ СООБЩАЙТЕ
НЕЗНАКОМЫМ ЛЮДЯМ
ТРЕХЗНАЧНЫЙ КОД
НА ОБОРОТЕ КАРТЫ, PIN-КОД
И ПАРОЛИ ИЗ СМС



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО



Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Спрашивают данные карты.

— Что делать?



СРАЗУ ПОЛОЖИТЕ ТРУБКУ — ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.



Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

— Что делать?



НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят совершить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.



Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

— Что делать?



ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.



ИНТЕРНЕТ



Предлагают вложить деньги на очень выгодных условиях.

— Что делать?



ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.



На сайтах с объявлениями («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

— Что делать?



НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.



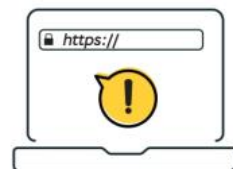
Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

— Что делать?



ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись **https://** и «замочек» в адресной строке браузера.



Выгодные ставки
всем заемщикам?

Гарантируют
одобрение даже
с плохой кредитной
историей?

Обещают
кредит
без справок
и проверок?

Будьте бдительны!

За выгодными
условиями часто
скрываются мошенники!



Проверьте на сайте Банка России,
законно ли работает компания:



◀ Есть ли
у нее
лицензия?

cbr.ru/fmp_check/



◀ Нет ли
организации
в списке
нелегалов?

cbr.ru/inside/warning-list/



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

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?

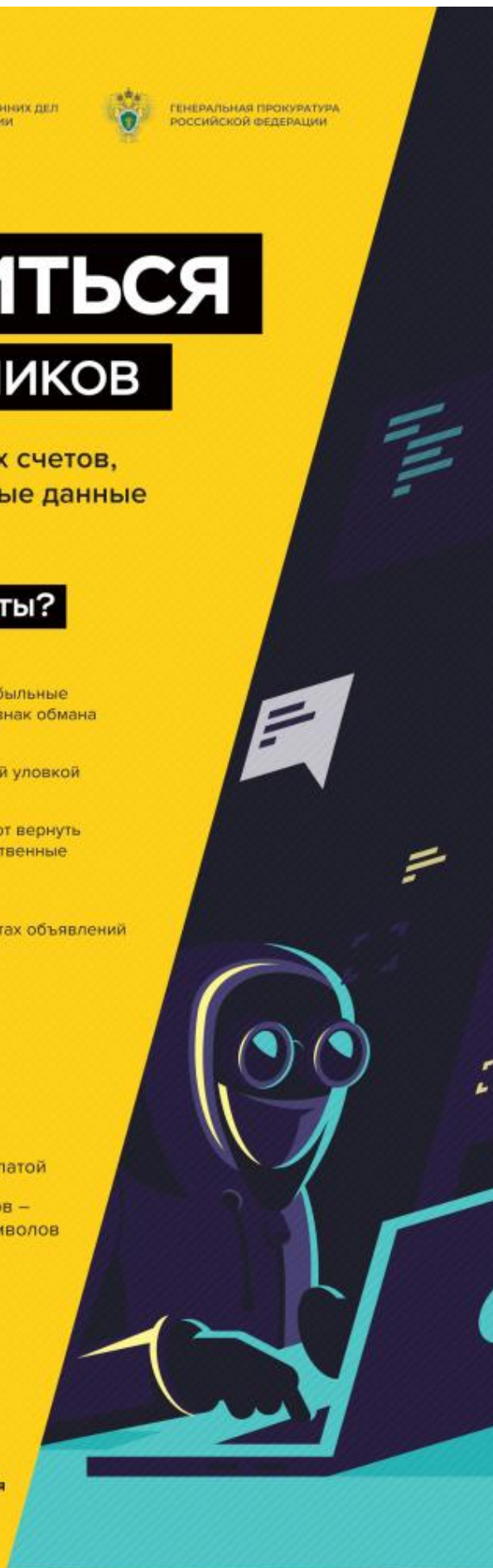
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам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



Подробнее о правилах
кибергигиены
читайте на fincult.info



Финансовая
культура





ОСТОРОЖНО: МОШЕННИКИ!



Вам звонят из банка и просят сообщить персональные данные или информацию о карте/счете – БУДЬТЕ БДИТЕЛЬНЫ, ЭТО МОГУТ БЫТЬ МОШЕННИКИ!

Злоумышленники с помощью специальных технологий могут сделать так, что на экране вашего телефона высветится официальный номер банка.

Они могут обратиться к вам по имени-отчеству и попросить секретные сведения о карте или счете. Например, чтобы остановить подозрительную операцию.

В ЧЕМ ОПАСНОСТЬ И ЧТО ДЕЛАТЬ?

Узнав нужную информацию, преступник может украсть ваши деньги.

- 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, вы можете снова попасть к мошенникам.





ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ

1 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 звонок или сообщение, вы рискуете снова попасть к мошенникам.

2 Сосредоточьтесь

Если банк выявит подозрительную транзакцию, он приостановит ее на срок до двух суток.

У вас есть 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.

3 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.

Подробнее о том, как защититься от киберкраж и финансовых мошенников, читайте на сайте **fincult.info**

ТЕПЕРЬ
НЕ
ПРОВЕДЕШЬ!



Банк России

Контактный центр Банка России:

8 800 300-30-00

(для бесплатных звонков
из регионов России)

Интернет-приемная
Банка России:

**[www.cbr.ru/
reception](http://www.cbr.ru/reception)**



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

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



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут
представиться службой
безопасности банка,
налоговой,
прокуратурой

Любой неожиданный
звонок, СМС или письмо —
повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции
притупляют
бдительность



3 НА ВАС ДАВЯТ

Аферисты всегда
торопят, чтобы
у вас не было
времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти
сбережения, получить
компенсацию или вложиться
в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников
интересуют реквизиты
карты, пароли и коды
из банковских уведомлений



ВАЖНО!

Сотрудники банков и полиции
НИКОГДА не спрашивают
реквизиты карты, пароли
из СМС, персональные данные
и не просят совершать
переводы с вашей карты



НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной
стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому
приложению и онлайн-банку
- кодовое слово
- персональные данные



Как защитить свои финансы,
читайте на fincult.info




Финансовая
культура

И никаких рисков?

Будьте бдительны!

За выгодными условиями могут скрываться финансовые



- Присылает сообщения и фотографии на «горячую линию» жертв кибербуллинга
- Не в курсе случаев недовольства школьниками «Горячей линией»
- Содержит форму для заполнения ваших данных

Ваше сообщение/фотографии SMS с неизвестного номера с просьбой в помощи близкому человеку

- Не присылает, не отвечает, не реагирует
- Присылает в основном в 1-м классе

Ваша подписка/взнос на получение / какой-то продукт из списка книг, компьютерные игры, продукты бытовой техники и т.д.

[illegible]

- Прогнати злодія і повернутися на «своєму місці» (завдяки базі даних і розробці спеціального програмного забезпечення)
- Не вимагати від користувачів ніяких додаткових дій
- Скориставшись функцією «Забудувати» вийти з мережі

Важко відслідковувати SMS з використанням програм з прошивки в пам'яті блоку чи телефону

- Не потрібно переміщуватися
- Програмують тільки раз в житті

Важко відслідковувати отримання повідомлень / адрес / номерів / ідентифікаторів GSM, відслідковує лише номер телефону

Сотрудник Банка не имеет права выдавать кредит, предоставлять льготные условия кредитования, предоставлять кредит на основании поручительства из СМС.

Банк №190724 (его не делал)

Сотрудник Банка по номеру 1909024 записывает в номер телефона клиента код изобразительного кода с обратной стороны карты (СМС-код) для подтверждения из СМС.

Банк 1909024 (его не должен)

Вопросы и ответы

1. Легко зарегистрироваться и войти в систему.

2. Удобно переводить деньги в другие банки.

3. Можно платить за услуги и делать покупки.

4. Можно подать заявку на кредит и кредитную карту.

5. Можно управлять инвестициями и депозитами.

6. Можно управлять страховками.

7. Можно управлять счетом и видеть историю операций.



Бонитилью обменялось беларусамі.
Она прадставіла сапраўды асаблівае

Большинство «гарантируют» десятки или даже сотни процентов в год, без всякого риска, это точно аферисты.



Вас просят приводить новых клиентов

И обещают намелиться процент от их вноса. Так преступники пытаются побыстрее овалить как можно больше людей в свою аферу, собрать с них деньги и скрыться.

посмотреть список пирамид, по которым идут выплаты.



КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По сообщению из интернета или электронной почты, СМС, сообщений в соцсетях или телеконференциях, репосты, официальной в интернете, распространение, использование от государства

Хранить часто рекомендуется в чистом вакуумном,
и физиологически полезном масле грибов даже от закисания.



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес: исполняется от названного лица, перед которым
- В адресной строке: netgear и значок закрытого окна
- Данные: скопирован, не изменено, в тексте есть ошибки

1 Вы можете использовать свой телефон для звонков и сообщений, но не для загрузки приложений.

2 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

3 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

4 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

5 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

6 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

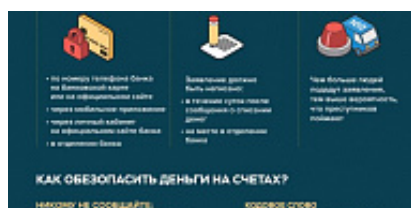
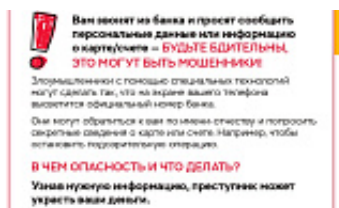
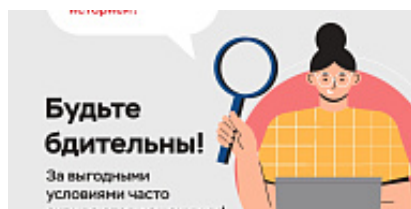
7 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

8 Если вы хотите использовать свой телефон для загрузки приложений, вы должны сначала установить приложение для загрузки приложений.

ОСТОРОЖНО: МОШЕННИКИ!

НИКОГДА

The diagram illustrates the relationship between various IT and business concepts. At the center is a large circle labeled **IT-Infrastruktur**. Surrounding it are several other concepts, each in a yellow circle: **Internet**, **E-Business**, **E-Government**, **E-Marketing**, **E-Procurement**, **E-Logistics**, **E-Healthcare**, **E-Education**, **E-Entertainment**, **E-Travel**, **E-Real Estate**, **E-Insurance**, and **E-Finance**. To the left of the central circle is a large yellow circle labeled **Business Process Management**. To the right is a large yellow circle labeled **Supply Chain Management**. Below the central circle is a large yellow circle labeled **Customer Relationship Management**. Above the central circle is a large yellow circle labeled **Human Resource Management**. To the far left is a large yellow circle labeled **Financial Management**. To the far right is a large yellow circle labeled **Marketing Management**. Below the central circle is a large yellow circle labeled **Operations Management**. Above the central circle is a large yellow circle labeled **Information Management**. To the far left is a large yellow circle labeled **Knowledge Management**. To the far right is a large yellow circle labeled **Innovation Management**. Below the central circle is a large yellow circle labeled **Sustainability Management**. Above the central circle is a large yellow circle labeled **Risk Management**. To the far left is a large yellow circle labeled **Compliance Management**. To the far right is a large yellow circle labeled **Governance Management**. Below the central circle is a large yellow circle labeled **Ethics Management**. Above the central circle is a large yellow circle labeled **Social Responsibility Management**. To the far left is a large yellow circle labeled **Environmental Management**. To the far right is a large yellow circle labeled **Labor Relations Management**. Below the central circle is a large yellow circle labeled **Diversity Management**. Above the central circle is a large yellow circle labeled **Inclusion Management**. To the far left is a large yellow circle labeled **Employee Engagement Management**. To the far right is a large yellow circle labeled **Organizational Culture Management**. Below the central circle is a large yellow circle labeled **Leadership Management**. Above the central circle is a large yellow circle labeled **Team Management**. To the far left is a large yellow circle labeled **Project Management**. To the far right is a large yellow circle labeled **Change Management**.



НА ВАС ВЫХОДЯТ САМИ
Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой. Любой неожиданный звонок, СМС или письмо - повод насторожиться

РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ
Сильные эмоции притупляют бдительность

НА ВАС ДАВЯТ
Аферисты всегда торопят, чтобы у вас не было времени все обдумать

ГОВОРЯТ О ДЕНЬГАХ
Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

ПРОСЯТ СООБЩИТЬ ДАННЫЕ
Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!
Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС, трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Дата публикации: 14.03.2024

Теги: [Финансовая грамотность](#), [МВД](#)

[Копировать ссылку](#)

[Предыдущая новость](#) [К списку новостей](#) [Следующая новость](#)