мои финансы

Минфин России

НИФИ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ФИНАНСОВЫЙ ИНСТИТУТ

Как пользоваться цифровыми финансовыми услугами безопасно

Категорически нельзя:

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/CVC-код, код из СМС или push-уведомлений.

мои финансы

Минфин России

НИФИ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ФИНАНСОВЫЙ ИНСТИТУТ

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 накладки 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 удается 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).