

**хочу**  
управлять  
своими  
финансами

**могу**  
делать это  
из дома

**знаю**

- возможности и риски использования мобильного и интернет-банка
- какие услуги доступны в платежных терминалах и банкоматах
- оплатить покупку в интернете можно электронными деньгами
- как безопасно хранить логины и пароли

# цифровые финансовые услуги и каналы взаимодействия



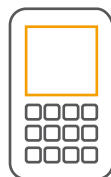
## Банкоматы и платежные терминалы банков

Стационарные устройства самообслуживания (электронные «кассиры» банков).



## Небанковские платежные терминалы

Стационарные устройства самообслуживания организаций – платежных посредников, которые принимают платежи от граждан в адрес банков, МФО и других организаций.



## Мобильный банк

Доступная держателю банковской карты услуга по получению уведомлений от банка и управлению банковской картой с помощью СМС.



## Интернет-банк

Инструмент управления банковским счетом через интернет при помощи личного кабинета. Доступ в личный кабинет – с официального сайта банка или из мобильного приложения (устанавливается на компьютер, планшет или смартфон).

### Возможности

<b>Снять / внести наличные</b>	✓ ✗*
<b>Осуществить платежи (налоги, ЖКХ и др.)</b>	✓
<b>Оплатить интернет-покупку</b>	✗

Только внести (по номеру карты)	✓
наличными	✓
наличными	✓

<b>Заблокировать карту</b>	✓
<b>Получить выписку по счету</b>	✓
<b>Совершить перевод</b>	✓

✓	✓
✓	✓
✓	✓

\* Возможно только с помощью банкомата.

<b>Открыть или закрыть вклад, оформить кредит</b>	✗
---	---

✓
---

### Особенности и риски

Номер карты и ПИН-код могут быть украдены с помощью специально установленного злоумышленниками устройства.

Ощутимые комиссии, размер которых можно узнать только по завершении операции.

Стоимость СМС-команд зависит от банка.

Комиссии за совершение операций отсутствуют или минимальны, в сравнении с такими же операциями в офисе банка.

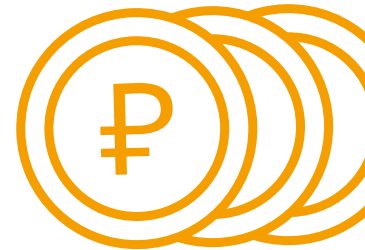
Могут «зажевать» карту, отказаться принять поврежденную или грязную купюру.

Полная потеря денег, дополнительные комиссии, задержки платежей – в «фальшивых» терминалах.

Злоумышленник, завладевший мобильным телефоном, логином и паролями, может получить доступ к банковским счетам.

## Электронные деньги

Это цифровое средство платежа. Для их использования нужен электронный кошелек – своеобразный аналог банковского счета. Пополнить электронный кошелек можно переводом с банковской карты, со счета мобильного телефона или наличными.



**Открывать электронные кошельки и переводить между ними электронные деньги в России имеют право только кредитные организации**



получившие лицензию на осуществление переводов денежных средств без открытия банковских счетов

включенные в Перечень операторов электронных денежных средств (публикуется на официальном сайте Банка России [cbr.ru](http://cbr.ru))



### Особенности и риски использования



Электронные деньги не могут размещаться во вклады.

Чем меньше информации предоставляет владелец кошелька, тем больше ограничений по максимальному остатку и сумме переводов и платежей.



### Основные возможности



Оплачивать покупки в интернете и переводить денежные средства другим людям, не имея банковской карты / счета.

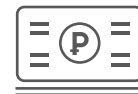


В отличие от средств на банковских счетах граждан электронные деньги не застрахованы государством.

Совершать платежи, предоставляя получателю средств минимальную информацию о себе.



Обналичить электронные деньги непросто (иногда удерживается комиссия).



## Основные риски и советы для потребителей

1

**Быстрый доступ к финансовой услуге не всегда сопровождается полной и необходимой информацией**

- Убедитесь, что поняли все основные условия предоставления услуги до заключения сделки (нажатия на виртуальную кнопку).
- Изучите отзывы и информацию о поставщике услуги.

2

**В случае технического сбоя найти виновника и вернуть деньги может быть непросто.**

- Тщательно выбирайте организацию, с которой будете взаимодействовать напрямую.
- Расплачиваясь в интернете банковской картой, убедитесь, что используете технологию 3D-Secure (подтверждение операции через СМС).

3

**Незащищенная персональная информация может попасть в руки мошенников.**

- Используйте сложные пароли, обновляйте их. Никогда и никому их не сообщайте.
- Если вы подозреваете, что пароль стал кому-то известен – немедленно смените его, заблокируйте банковские карты и доступ к интернет-банку.

### Контакты для обращений

Роспотребнадзор [www.rosпотребнадзор.ru](http://www.rosпотребнадзор.ru)  
 Банк России [www.cbr.ru](http://www.cbr.ru)  
 Финансовый уполномоченный (омбудсмен) [finombudsman.ru](http://finombudsman.ru)  
 Федеральная служба судебных приставов [fssprus.ru](http://fssprus.ru)  
 Бесплатная горячая линия Роспотребнадзора для потребителей финансовых услуг 8-800-100-29-26