При использовании дистанционных сервисов всегда существует риск того, что злоумышленники попытаются получить несанкционированный доступ к вашей конфиденциальной информации. Такие риски могут быть связаны с:

- использованием вредоносных программ (вирусов, троянов, фишинговых страниц), которые перехватывают логины, пароли, коды подтверждения;
- получением доступа к вашему устройству (компьютеру, смартфону, планшету) посторонними лицами, в том числе членами семьи, коллегами или злоумышленниками;
- использованием простых или одинаковых паролей для разных сервисов, хранением реквизитов доступа «на виду» или передачей их третьим лицам;
- подключением к публичным/незащищенным Wi-Fi сетям при проведении финансовых операций;
- утратой, хищением или продажей устройства без предварительного удаления данных и выхода из учетных записей.

При реализации этих рисков злоумышленники могут получить доступ к вашим учетным записям и совершать платежи, переводы, заключать сделки и выполнять другие операции без вашего согласия.

Как снизить риски несанкционированного доступа

Чтобы защитить свою конфиденциальную информацию и финансы, рекомендуем соблюдать следующие меры безопасности.

1. Безопасность устройства

- Используйте актуальные версии операционной системы и приложений, своевременно устанавливайте обновления.
- Установите надежное антивирусное программное обеспечение и регулярно обновляйте его базы.
- Установите блокировку экрана (PIN-код, пароль, биометрия) и не передавайте устройство посторонним.
- Не устанавливайте программное обеспечение из неизвестных источников и не предоставляйте приложениям избыточные разрешения.

2. Конфигурация и учетные записи

- Используйте сложные, уникальные пароли для финансовых сервисов и личного кабинета, не храните их в открытом виде и не передавайте третьим лицам.
- Включите двухфакторную аутентификацию (подтверждение операций одноразовыми кодами, биометрией и т.п., где это предусмотрено).
- Регулярно просматривайте список устройств и сессий, имеющих доступ к вашему аккаунту, и при необходимости удаляйте неизвестные.

3. Поведение в сети

- Не переходите по ссылкам из подозрительных писем, SMS и сообщений в мессенджерах, даже если они выглядят как сообщения от банка или финансовой организации.
- Не вводите реквизиты доступа (логины, пароли, коды) на сайтах и в приложениях, если у вас есть сомнения в их подлинности.
- Не сообщайте коды подтверждения операций, пароли, реквизиты карт и другую конфиденциальную информацию по телефону, в мессенджерах или по электронной почте, даже если собеседник представляется сотрудником организации.

Что делать при утрате, хищении или компрометации устройства

Если вы потеряли устройство, с которого совершаете финансовые операции, либо подозреваете, что к нему получили доступ третьи лица, необходимо как можно быстрее предпринять следующие шаги.

- Немедленно свяжитесь с АО «НПФ «Ростех» по указанным на сайте каналам и сообщите о возможном несанкционированном доступе.
- Заблокируйте доступ к интернет-банку и другим финансовым сервисам, а при необходимости — ограничьте проведение операций.
- Обратитесь к оператору связи для блокировки SIM-карты, если к вашим сервисам привязан номер телефона.
- Используйте функции удаленной блокировки и/или стирания данных на устройстве (если они включены).
- Измените пароли ко всем важным учетным записям (почта, интернет-банк, госуслуги и др.).

Как мы защищаем ваши данные

АО «НПФ «Ростех» применяет организационные и технические меры защиты информации на высоком уровне, включая многофакторную аутентификацию, шифрование каналов связи, мониторинг операций и механизмы противодействия мошеннической активности в соответствии с требованиями Банка России. Вместе с соблюдением рекомендаций, описанных выше, это позволяет существенно снизить риск несанкционированного доступа к вашей конфиденциальной информации и финансовым операциям.