

Памятка
клиентам Банка ВТБ (ПАО) о соблюдении финансовой безопасности при использовании
банковскими картами, интернет-банком и другими услугами банка

1. Если Вам поступают звонки от имени «банковских работников», а так же СМС-сообщения, сообщения в социальных сетях и мессенджерах от якобы «Банк ВТБ» (ПАО) (далее - Банк), в которых содержится информация, касающаяся финансовых операций (*подозрительный платеж (операция), сумма оплаты или Ваша карта заблокирована, проблемы с проведением операции, заблокирован доступ в ВТБ-Онлайн и т.п.*):
 - **ни в коем случае не перезванивайте на указанные в сообщениях номера,**
 - **не сообщайте звонящим поступающие на телефон СМС-коды подтверждения и данные банковских карт:** номер карты, срок действия, контрольный код с обратной стороны карты, а также **персональные сведения:** серия и номер паспорта, адрес регистрации,
 - **прекратите контактировать и немедленно самостоятельно обратитесь в Банк по телефонам, которые указаны на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах.** Объясните оператору причину Вашего обращения.
2. Запомните, что от Банка не могут поступать звонки с номеров **8-800: (800) 100-24-24, (800) 200-23-26, (800) 500-24-24, (800) 700-00-24, (800) 700-24-24** и **(495) 777-24-24, (495) 777-77-24, (495) 745-80-00, (495) 925-80-00** – эти номера принадлежат Банку, но предназначены только для приема входящих звонков.
3. При использовании карты в Интернете (особенно при привязке к регулярным платежам или аккаунтам) **пользуйтесь только проверенными сайтами**, т.к. велика вероятность перейти на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные.

Официальный сайт Банка - <https://www.vtb.ru/>, ВТБ-Онлайн <https://online.vtb.ru/>

При проведении операции в Интернете обращайтесь внимание на **содержание СМС-сообщения с кодом подтверждения операции**, а именно: на место проведения операции (*например, чтобы вместо наименования ТСП не было card2card и т.п.*), сумму и вид платежа.

Не вводите код, если есть расхождения в месте проведения операции.

4. **Крайне важно** самостоятельно обеспечить сохранность / конфиденциальность реквизитов своей карты и ПИН-кода (*например, не пишите ПИН-код на самой карте и не передавайте карту третьим лицам*). Напоминаем, что операции по снятию наличных, совершенные с использованием ПИН-кода, считаются выполненными самим держателем карты и опротестованию не подлежат.
5. Если Вы выходите в Интернет через смартфон или планшет, настоятельно рекомендуем **использовать антивирусное ПО**. Это поможет уменьшить вероятность попадания вредоносных программ в устройство, предназначенных для перехвата проходящих от Банка СМС-сообщений, компрометации персональных данных и карточных авторизационных данных.
6. Не храните на своём устройстве средства доступа к системам дистанционного банковского обслуживания (логины и пароли), номера карт, паспортные данные и другую конфиденциальную информацию, чтобы она не стала доступна третьим лицам в случае утраты устройства.
7. Рекомендуем соблюдать следующие меры, повышающие безопасность при использовании мобильного телефона: не подключайтесь к общедоступным Wi-Fi-сетям, **не устанавливайте приложения из недоверенных источников**, не открывайте подозрительные письма и ссылки и т. д.
8. Рекомендуем **отключить функцию «удаленного восстановления пароля»** в настройках личного профиля ВТБ-Онлайн в разделе смены пароля.
9. **Не реже раза в сутки** проверяйте работоспособность телефона и сим-карты, на который приходят СМС-коды и СМС-информирование. При неработоспособности или утере смартфона немедленно обращайтесь в Банк и блокируйте доступ в ВТБ-Онлайн. Проверяйте все действия и операции в системах дистанционного обслуживания в период неработоспособности телефона. Рекомендуем написать заявление сотовому оператору о запрете принимать обращения на блокировку/разблокировку/замену сим-карты от третьих лиц по доверенности.