ПАМЯТКА КЛИЕНТАМ БАНКА ВТБ О СОБЛЮДЕНИИ БЕЗОПАСНОСТИ

при пользовании банковскими картами, интернет-банком и другими услугами банка

1 **Если Вам поступают звонки** от имени «банковских работников» или SMS-сообщения, сообщения в социальных сетях и мессенджерах якобы от Банка ВТБ (ПАО) (далее – Банк) с информацией, касающейся 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 **SMS-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 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**:

8 800 100-24-24
8 800 200-23-26
8 800 500-24-24
8 800 700-00-24
8 800 700-24-24

А также с данных номеров, начинающихся с **+7 495**:

+7 495 777-24-24
+7 495 777-77-24
+7 495 745-80-00
+7 495 925-80-00

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** обращайте внимание на содержание SMS-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 минимизировать риск попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от Банка SMS-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 При использовании мобильного телефона соблюдайте следующие меры безопасности: **не подключайтесь к общедоступным Wi-Fi-сетям, не устанавливайте приложения из недостоверных 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 SMS-коды и SMS-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.