Памятка
Клиентам Банка ВТБ (ПАО) для обеспечения безопасности при пользовании банковскими картами и интернет-банком.

1. При поступлении звонков от имени «банковских работников», а так же СМС сообщений, сообщений 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 перезванивать на указанные в сообщениях номера,
   -не сообщать звонящим поступающие на телефон СМС-коды подтверждения, данные банковских карт: номер карты, срок действия, контрольный код с обратной стороны карты, а так же **персональные сведения**: серия и номер паспорта, адрес регистрации,
   - **прекратить контактировать и немедленно самостоятельно обратиться в Банк** по телефонам, содержащихся на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах, объяснив оператору причину обращения.
   Необходимо запомнить, что от Банка не могут поступать звонки с номера **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 принадлежит Банку, но предназначены только для приема входящих звонков.
2. При использовании карты в сети Интернет (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 сети Интернет обращайте 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.
3. Необходимо понимать, что необходимо самостоятельно обеспечить сохранность / конфиденциальность реквизитов своей карты и ПИН-кода (например, не писать ПИН-код на самой карте и не передавать карту третьим лицам), операции по снятию наличных, совершенные с использованием ПИН-кода, считаются выполненными самим держателем карты и опротестованию не подлежат.
4. Владельцам смартфонов и планшетов, используемых для выхода в сеть Интернет, настоятельно рекомендуем **использовать антивирусное ПО**, которое поможет уменьшить вероятность попадания вредоносных программ в устройство, предназначенных для перехвата приходящих от Банка СМС – сообщений, компрометации персональных данных и карточных авторизационных данных.
5. Не храните на своём устройстве средства доступа к системам дистанционного банковского обслуживания (логины и пароли), номера карт, паспортные данные и прочую конфиденциальную информацию, чтобы она не стала доступна третьим лицам в случае утраты устройства.
6. Рекомендуем соблюдать следующие меры, повышающие безопасность при использовании мобильного телефона: не подключаться к общедоступным Wi-Fi-сетям, **не устанавливать приложения из недоверенных источников**, не открывать подозрительные письма и ссылки и т. д.
7. Рекомендуем **отключить функцию «удаленного восстановления пароля»** в настройках личного профиля ВТБ-Онлайн в разделе смены пароля.
8. **Необходимо не реже раза в сутки** проверять работоспособность телефона и СИМ – карты, на который приходят СМС – коды и СМС – информирование. При неработоспособности или утере смартфона немедленно обращаться в банк и блокировать доступ в ВТБ-Онлайн. Проверить все действия и операции в ДБО в период неработоспособности телефона. Рекомендуется написать заявление сотовому оператору о запрете принимать обращения на блокировку/ разблокировку/замену СИМ – карты от третьих лиц по доверенности.