

Памятка

Клиентам ВТБ при пользовании банковскими картами и интернет-банком

1. При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных -сообщений от якобы «ВТБ» (далее Банка), например, «*Ваша карта заблокирована*», «*Заблокирована сумма оплаты*», «*Есть проблемы с проведением операции*» и т.п.):
 - **ни в коем случае не перезванивайте на указанные в сообщениях номера,**
 - **не сообщайте данные банковских карт:** срок действия, контрольный код с обратной стороны карты, **СМС-коды подтверждения,** а также **персональные сведения:** серия и номер паспорта, адрес регистрации и пр.
2. От Банка не могут поступать звонки с номера **8(800)100-24-24, 8(800)500-24-24 , 8(800)700-24-24** – эти номера принадлежат Банку, но предназначены только для приема входящих звонков.
3. В описанных выше ситуациях следует считать, что звонки или сообщения приходят от **мошенников, прекратить контакт и самостоятельно обратиться в Банк** по телефонам, содержащимся на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах.
4. При использовании карты в интернете (особенно в случае привязки к регулярным платежам или аккаунтам) **пользуйтесь только проверенными сайтами,** т.к. велика вероятность перейти на поддельный сайт, созданный мошенниками для получения клиентских данных, включая данные карты.
5. При проведении операции в интернете обращайте внимание на **содержание СМС-сообщения с кодом подтверждения операции,** а именно на сумму и вид платежа, а также место проведения операции (так, вместо наименования продавца не может быть указано *card2card* и т.п.). Не вводите код, если есть расхождения в месте проведения операции.
6. Владельцам смартфонов, используемых для выхода в интернет, настоятельно рекомендуем **использовать антивирусное ПО,** которое поможет уменьшить вероятность попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от Банка СМС-сообщений, кражи персональных данных и карточных авторизационных данных.
7. Рекомендуем соблюдать меры предосторожности, повышающие безопасность самого мобильного телефона. Например, не подключаться к общедоступным Wi-Fi-сетям, **не устанавливать приложения из недостоверных источников,** не открывать подозрительные письма и ссылки и т.д.
8. Обращайте внимание на диалоговые окна авторизации и совершения операций. **Никогда не вводите номер телефона «для получения СМС-кодов», карточные данные «для подключения 3DS защиты», а также СМС-коды для «отмены операции».** При этом необходимо учитывать, что работник **Банка никогда не звонит клиенту в процессе его авторизации или использования ВТБ-Онлайн.**
9. Рекомендуем **отключить функцию «удаленного восстановления пароля»** в настройках личного профиля ВТБ-Онлайн в разделе смены пароля. Также рекомендуем использовать и регулярно менять псевдонимы в качестве логина (УНК) для входа в ВТБ-Онлайн.
10. Написать заявление сотовому оператору о запрете принимать обращения на блокировку/разблокировку/замену СИМ-карты от третьих лиц по доверенности.