

**Мы заботимся о вашей безопасности, но ваша бдительность – главное препятствие на пути у мошенников.**

**Никогда не сообщайте эти данные третьим лицам даже сотрудникам банка:**

- Полный номер карты
- Трехзначный код на обороте карты
- Пин-код
- Код для входа в онлайн кабинет Банка
- Одноразовый код из смс / push сообщения
- Кодовое слово (можно назвать сотруднику только в том случае, если вы сами обратились в Банк)

**Сотрудник Банка никогда не будет:**

- Просить вас перевести деньги на «безопасный счет»
- Просить вас установить стороннее приложение для проведения операций
- Связываться с вами с личного телефона, электронной почты или мессенджера
- Торопить и требовать принять срочное решение

**Будьте внимательны:**

- Не переходите по незнакомым ссылкам
- Проверяйте адреса наших сервисов на наличие посторонних символов. Например:  
 [Небезопасно | 0z0n.ru](https://0z0n.ru)
- Проверяйте безопасность соединения, если нет значка  <https://> - вероятно вы находитесь на мошенническом сайте
- Устанавливайте на мобильные устройства только проверенные приложения
- Установите пароль для блокировки экрана вашего мобильного телефона и регулярно меняйте его
- Переводите деньги только в том случае, если вы знаете кто получатель
- Подключите и следите за смс / push оповещениями о совершенных операциях
- При проведении незнакомой вам операции с вашего счета/карты или подозрении на взлом вашего аккаунта – немедленно обратитесь по телефону 8 800 555-89-82 или в чате приложения Ozon
- Если при телефонном разговоре у вас возникли подозрения, что с вами разговаривает не сотрудник банка, завершите разговор и свяжитесь с нами по официальному номеру 8 800 555-89-82 или в чате приложения Ozon
- Если вы потеряли телефон обратитесь в Банк для блокировки счета, а также к мобильному оператору для блокировки сим-карты.