Памятка по финансовой безопасности для клиентов Банка «РОССИЯ»

Чтобы работа в интернет-банке ABR Direct была безопасной, соблюдайте правила финансовой безопасности.

1) **Интернет-банк и мобильное приложение**

Держите смартфон при себе, чтобы он не попал в руки мошенников. Читайте внимательно СМС-уведомления. Не сообщайте никому коды из СМС. Сообщите в Банк, если сменили номер телефона, потеряли смартфон или сим-карту.

2) **Wi-Fi**

Используйте защищённые точки доступа Wi-Fi. Если Вы подключились к публичной Wi-Fi-сети, не пользуйтесь интернет-банком, не совершайте оплату на сайтах, ничего не скачивайте и не устанавливайте обновления.

3) **Банковская карта**

Никому не сообщайте и не пересылайте ПИН-код, CVC/CVV-код, персональные данные владельца и срок действия карты. Не передавайте карту другим людям, следите, чтобы все операции проводились у вас на глазах.

4) **Онлайн-покупки**

Откажитесь от покупок на сайтах, где не указаны полные реквизиты компании и правила возврата товара.

5) **Пароли**

Ограничьте доступ посторонних лиц к смартфону и компьютеру. Используйте сложные пароли для доступа в интернет-банк. Запоминайте их, нигде не записывайте и никому не пересылайте.

6) **Электронные письма**

Не переходите по ссылкам в письмах от неизвестных отправителей и не отвечайте на такие письма.

7) **Телефоны**

Звоните в Банк только по официальным номерам. Они указаны на сайте Банка, в ABR Direct, в реквизитах вашего договора с Банком и на обороте карты. Если вам позвонили от имени Банка с незнакомого номера, прервите разговор и перезвоните в Банк самостоятельно.

Как понять, что вам звонят мошенники?

Мошенники под видом сотрудников Банка, силовых ведомств или госструктур пытаются завладеть данными ваших карт, паролями и секретными кодами из СМС. Они используют разные сценарии и пытаются сыграть на вашем доверии к Банку и госорганам.

1) **Звонок из МВД, прокуратуры, ФСБ или Центрального Банка**

«Сотрудник госорганов» сообщает, что на вас незаконно оформлен кредит и предлагает срочно перевести средства на «безопасный счёт». Далее он пытается завладеть персональной информацией: данными карты и кодами из СМС для подтверждения операций. Не сообщайте ваши данные и прервите разговор.

2) **Звонок сотрудников соцзащиты или ПФР**

Мошенник сообщает, что вам полагается дополнительная выплата от государства. Для её оформления предлагает перейти по ссылке в СМС или мессенджере. Далее он пытается завладеть персональной информацией: предлагает ввести на сайте или продиктовать данные карты и коды для подтверждения. Не переходите по ссылкам и не сообщайте ваши данные. Прервите звонок.

3) **Звонок «из Банка» о блокировке карты**

Мошенники звонят или отправляют СМС под видом сотрудников Банка. Суть звонка или СМС — блокировка карты из-за подозрительных операций. Прервите разговор и самостоятельно перезвоните на номер Единой службы поддержки держателей карт, который указан на обороте карты. Служба работает круглосуточно.

4) **Звонок по объявлению в интернете**

Мошенники звонят по вашему объявлению о продаже в интернете и для перевода денег за товар просят сообщить реквизиты карты и код из направленного СМС. Прервите разговор, для оплаты товара эта информация не нужна.

5) **Звонок о несчастном случае**

Мошенники пытаются сыграть на эмоциях: сообщают о несчастном случае, произошедшим с кем-то из близких и просят перевести деньги на карту или счёт. Прервите разговор и позвоните близкому человеку, чтобы убедиться, что с ним всё в порядке.

Специалисты Банка «РОССИЯ» и сотрудники госорганов никогда:

- не запрашивают по телефону персональные данные клиентов,
- не предлагают перевести деньги на «безопасные счета»,
- не переключают клиента во время разговора на полицию, Следственный комитет или Центробанк.

Если вам поступил подозрительный звонок, прервите его. Перезвоните в Банк по телефону 8 800 100-11-11 и сообщите о звонке мошенников специалистам службы поддержки.