

## Распространенные способы хищения денег с использованием банковских карт

Способы мошенничества	Чего и зачем добиваются	Способы защиты
<p>Как правило, по телефону от, якобы, сотрудника банка поступает предложение:</p> <ul style="list-style-type: none"> <li>- обезопасить деньги на счете, переведя их удаленно на защищенный расчетный счет;</li> <li>- реструктуризировать долг по кредиту;</li> <li>- установить программу удаленного доступа (или сторонние предложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки;</li> <li>- зайти в онлайн-кабинет по ссылке на СМС-сообщения или электронного письма, чтобы узнать о проблеме по счету;</li> <li>- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.</li> </ul>	<p><b>1. Напугать</b> возможностью утраты денег.</p> <p><b>2. Установить доверительный контакт</b>, что позволит получить:</p> <ul style="list-style-type: none"> <li>- номер карты;</li> <li>- срок ее действия;</li> <li>- идентификационный код клиента из 3-х цифр, указанных на обороте банковской карты (CVV или CVC-код);</li> <li>- ПИН-код, дающий возможность совершать операции по счету;</li> <li>- код из СМС-сообщения на мобильный номер, к которому привязана банковская карта, что также обеспечит доступ к деньгам на счете.</li> </ul> <p><b>3. Похитить деньги.</b></p>	<p>1. Не сообщайте звонящему никаких данных.</p> <p>2. Прервите разговор.</p> <p>3. Проверьте информацию, связавшись со своим банком по телефону на оборотной стороне карты или на сайте банка.</p> <p>4. Отслеживайте операции по счету, подключив услугу мобильного банка.</p> <p>5. При наличии подозрительных операций немедленно звоните в банк.</p> <p>6. Помните! Банк может инициировать общение с клиентом только для консультации по предложению собственных услуг.</p>

