**ПАМЯТКА**

**как обезопасить свой банковский счет от хищений**

* **никому ничего не сообщать, особенно номера карт и любые коды (у банковских работников и так есть все нужные данные);**
* **для выхода в интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы
с вредоносной активностью, своевременно обновляйте его;**
* **используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения;**
* **при использовании известных Вам сайтов, обращайте внимание на их внешний вид. Возможно Вы зашли на их поддельные копии;**
* **вводите личную информацию только на веб-сайтах, работающих
с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);**
* **не используйте одинаковые логины и пароли на различных сайтах;**
* **не используйте слишком простые пароли, либо те, о которых легко догадаться (даты рождения, номера телефонов и т.д.);**
* **по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо ввести временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;**
* **остерегайтесь неожиданных или необычных электронных сообщений, даже если Вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;**
* **с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным интернет-каналам;**
* **при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно проверяйте данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь). В крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;**
* **если не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;**
* **при осуществлении интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Viza и MasterCard или интернет-пароль для платежной системы БЕЛКАРТ;**
* **никому не сообщайте коды подтверждения операций, приходящие от банков по SMS;**
* **рассказывайте о новых способах противоправных действий пожилым
и несовершеннолетним родственникам.**