РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

12.03.2020 г. г. Махачкала

**«О рекомендациях клиентам
по безопасному использованию
системы ДБО «iBank2»**

В целях снижения рисков воздействия вредоносного кода и повышения уровня безопасности при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) Комитет по информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) информирует клиентов системы ДБО «iBank2» о необходимости применения рекомендаций по защите информации от воздействия вредоносного кода (Приложение 1 к данному письму). В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в Комитет по информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления **К.А.Абдурахманов**

Приложение 1
к информационному письму
«О рекомендациях клиентам
по безопасному использованию
системы ДБО «iBank2»»

МЕРЫ БЕЗОПАСНОСТИ ПРИ ПОЛУЧЕНИИ ПОДОЗРИТЕЛЬНОЙ КОРРЕСПОНДЕНЦИИ

1. Работая с электронной почтой, убедитесь в том, что антивирусное программное обеспечение Вашего компьютера функционирует и своевременно обновляется.
2. Никогда не переходите по ссылкам в сообщениях, если содержание сообщений либо адрес отправителя кажется Вам подозрительным.
3. Читая сообщение, будьте внимательны. Как правило, сообщения, отправляемые мошенниками, содержат ряд вышеупомянутых признаков, по которому их легко распознать. Проще всего это сделать, внимательно просмотрев (не открывая) присланную ссылку.

МЕРЫ БЕЗОПАСНОСТИ ПРИ ОБЩЕНИИ ПО ТЕЛЕФОНУ

Непосредственное общение по телефону в последнее время активно используются мошенниками для сбора персональной информации и убеждения Клиента в необходимости осуществления немедленных действий, направленных на незаметный для Клиента перевод денежных средств в пользу третьих лиц под различными предлогами. Цель мошенника – хищение денежных средств со счета Клиента путем любых доступных приемов психологического воздействия на человека (страх, жалость, обещание ценного выигрыша). Основное и наиболее эффективное средство от такого вида мошенничества – немедленно прекратить разговор и перезвонить в Банк самостоятельно (если собеседник представился сотрудником РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)) по номерам, указанным на официальном сайте http://www.psib.ru/.

ХАРАКТЕРНЫЕ ПРИЗНАКИ МОШЕННИЧЕСТВА ПО ТЕЛЕФОНУ

1. Собеседник требует от Вас принятия немедленного действия или срочного ответа. В качестве причин, как привило, приводятся следующие причины: техническое блокирование Вашего доступа к системе ДБО «iBank2», обновление баз данных, иные нестандартные причины.
2. От Вас требуют назвать Ваши персональные данные (логин и пароль в систему ДБО «iBank2»). Запомните, РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) никогда и ни при каких обстоятельствах не запрашивает эту информацию у Клиентов.
3. Собеседник путается или ведет себя нетерпеливо при уточнении с Вашей стороны его фамилии, имени, отчества, контактного номера, цели звонка, подразделения (отдела), в котором он работает, фамилии руководителя.
4. При разговоре Вас просят произвести вход в систему ДБО «iBank2», сменить ПИН-код на usb-ключе iBank2 Key. В этом случае спросите у собеседника контактный номер телефона Банка, по которому Вы сможете перезвонить позже, закончите разговор и обратитесь в РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) (если Вам представились сотрудником РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)) по номерам, указанным на официальном сайте http://www.psib.ru/. Ваше обращение позволит предотвратить инциденты мошенничества в будущем.