Приложение № 8
к Правилам универсального банковского обслуживания
физических лиц в АО «Датабанк»
(на публичных условиях) (УДБО)»

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ПРИ РАСЧЕТАХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

1. Рекомендации по повышению безопасности при использовании банковских карт:

- Никогда не позволяйте другим лицам пользоваться вашей банковской картой;
- Никогда не принимайте рекомендации, советы, помощь от третьих лиц при пользовании банковской картой. Выполнение этого правила особенно важно при использовании банкоматов (за исключением случаев, когда Вы прибегаете к помощи работников Банка-консультантов);
- При пользовании банкоматом не позволяйте третьим лицам (включая друзей и родственников) находиться в непосредственной близости от Вас, так чтобы были видны ваши действия на клавиатуре банкомата;
- Никогда никому не передавайте свой PIN-код и храните их отдельно от карты;
- Никогда не записывайте PIN-код на карте;
- Помните, что операции, проводимые с картой без Вашего присутствия, несут в себе больше риска, чем те, которые кассир производит у Вас на глазах. Это правило особенно важно для стран Азиатско-Тихоокеанского региона, Бразилии, а также развивающихся стран, где более высока вероятность того, что данные Вашей карты могут быть недобросовестно использованы;
- Втройне аккуратно используйте банковскую карту для оплаты в ресторанах, барах, клубах, в мелких магазинах (электроники, ювелирных, сувенирных). Обязательно проверяйте предоставленные Вам чеки указанных сервисных организаций, сличайте суммы в чеке в суммами транзакций по Вашей карте, с суммой, Ваших расходов (их заявленным продавцом размером);
- Осуществляйте контроль за Вашими операциями, подключитесь к сервису SMS/puch-уведомления для получения информации обо всех операциях с Вашим спецкартсчетом через SMS/push- информирования на ваш мобильный телефон.

2. Рекомендации по обеспечению безопасной работы в Интернете:

Следите за сообщениями, приходящими по электронной почте. Эти сообщения могут быть похожи на сообщения, отправленные вашими деловыми партнерами или друзьями, однако фактически их цель — обманным путем заставить Вас загрузить программу, содержащую вирус, или зайти на определенный сайт и раскрыть конфиденциальную информацию.

Не отвечайте на послания по электронной почте с запросом ваших личных данных или данных о Вашей банковской карте.

Относитесь с подозрением к любой компании или лицу, запрашивающим Ваш пароль, номер паспорта, номер банковской карты и ее PIN-код, размер кредитного (овердрафтного) лимита, информацию о последних пяти операциях по банковской карте или другую конфиденциальную информацию. АО «Датабанк» никогда не запрашивает информацию такого рода по электронной почте!

Открывайте послания, пришедшие по электронной почте, только в том случае, если Вы знаете отправителя. Будьте особенно осторожны при открытии посланий с приложениями. Если Вы не знаете, что за файл прикреплен к письму, не открывайте его. Даже друг может случайно прислать сообщение с вирусом.

Будьте аккуратны со ссылками, содержащимися в электронных посланиях. Ссылки могут вести совсем не туда, куда указывает текстовая информация. Не отправляйте конфиденциальную личную или финансовую информацию, если только она не зашифрована (при работе на защищенном сайте).

Обычные письма, отправляемые по электронной почте, не шифруются. Ведите дела только с компаниями, которые Вы знаете и которым доверяете. Будьте внимательны! Некоторые сайты похожи на сайты крупных компаний, но они — фальшивые и предназначены для обмана клиентов и сбора их личной информации. Убедитесь, что сайты, с которыми Вы работаете, содержат заявления о соблюдении конфиденциальности и безопасности и внимательно их изучите.

Проверяйте адрес каждого сайта. Убедитесь, что необходимый вам URL-адрес появляется в поле «Адрес» или «Узел» вашего браузера. Некоторые сайты могут казаться похожими на

необходимый Вам, но в действительности быть фальсифицированными. Потратьте несколько лишних секунд и напечатайте в адресной строке URL-адрес лично.

При передаче конфиденциальной информации ищите символ замка в правом нижнем углу веб-страницы — этот символ указывает на то, что сайт работает в защищенном режиме. Вы должны увидеть его прежде чем введете конфиденциальную информацию.

При выходе из программы делайте это в соответствии с установленными процедурами. Не закрывайте браузер просто так! Выполняйте инструкции по выходу из программы для обеспечения вашей безопасности.

Осуществляйте контроль за Вашими операциями. Проверяйте подтверждения заказов, кредитную карту и выписки с банковских счетов по мере их получения, чтобы убедиться, что с Вас взысканы платежи только по произведенным операциям. Немедленно сообщайте о любых несоответствиях.

Поставьте на Ваш домашний компьютер самое современное антивирусное программное обеспечение. Антивирусное программное обеспечение необходимо часто обновлять для защиты от новых вирусов. Ставьте новые антивирусные программы, как только узнаете об их наличии.

Избегайте осуществления любых банковских операций в местах, где интернет-услуги являются общедоступными, например в интернет-кафе. Очень трудно определить, отсутствуют ли на таких компьютерах хакерские программы, которые фиксируют Вашу личную информацию и сведения о счете.

Распечатайте эти рекомендации и держите их при себе, чтобы пользоваться ими при проведении банковских или онлайновых операций.