Основные меры безопасности при использовании онлайн-банкинга

Не вводите личные данные

Как правило, для входа в интернет-банк кредитная организация запрашивает от клиента только логин и пароль. Номер телефона, данные паспорта, ПИН-код и другие личные данные – все это требовать от вас не должны.

Проверяйте адрес сайта

Если адрес сайта отличается даже одной буквой – это фишинговый сайт. Если интернет-обозреватель предупреждает, что сертификату безопасности сайта доверять нельзя – не доверяйте.

Пользуйтесь одноразовым паролем

Для защиты от фишеров большинство банков при подтверждении операций просят вводить одноразовый пароль. Это очень важный элемент безопасности, который никому и ни при каких обстоятельствах разглашать нельзя! Кроме того, если вы используете смс-пароль, нужно тщательно сверять реквизиты подтверждаемой операции.

Не входите в свой личный кабинет с чужих компьютеров

Лучше входить в интернет-банк только со своего персонального ПК. А вот рабочее место или интернет-кафе – не лучшее место для этого. Если же в силу определенных причин вам пришлось войти в личный кабинет с чужого компьютера, обязательно по окончании работы нажмите иконку «выход» и очистите кэш-память.

Используйте сложный пароль

Придумайте для входа в онлайн-банкинг сложный пароль и никому его не сообщайте, а тем более, не записывайте на карте. Лучше не ставить такой пароль на запоминание, а каждый раз вводить его вручную.

Обновляйте антивирус

Первое, что нужно сделать, это установить антивирус на ваш компьютер и в дальнейшем его своевременно обновлять. Еще один вариант – разрешить его автоматическое обновление. Далее нужно периодически производить антивирусную проверку для своевременного обнаружения вредных программ;

Установите лимиты на операции в интернет-банке

Можно установить лимиты на онлайн-операции по карте. Так мошенники не смогут снять с карты больше той суммы, на которую установлено ограничение;

Устанавливайте современные операционные системы

Старайтесь не использовать старые операционные программы, лучше отдать предпочтение более своевременным и в дальнейшем их обязательно обновлять. Это относится также к интернет-браузеру и почтовым программам. Дело в том, что последние обновления операционных систем разрабатываются с учетом новых появившихся вирусов.

Применяйте дополнительное программное обеспечение

Используйте «программы-сторожа», персональные межсетевые экраны, программы защиты от спам-рассылок и др. Например, установив персональный межсетевой экран, нужно просто указать в нем весь список программ и доступных им сервисов и портов. Тогда, если какая-то «левая» программа попытается отправить почту, ее действия сразу же будут обнаружены.

Используйте кодированное соединение

Проверяйте, что установлено защищенное (кодированное) соединение с официальным сайтом банка. Самое распространенное – это SSL-соединение, которое поддерживается большинством современных браузеров. Определить, используется ли защищенное соединение, можно по адресу в браузере: там должно стоять https (например, https://online.sberbank.ru).

Не скачивайте на компьютер подозрительные программы

Программы, полученные из непроверенных источников, могут содержать вирусы, сетевых червей или трояны. Самый лучший способ оградить себя от такого вреда – запретить в почте прием писем, содержащих исполняемые вложения. Или хотя бы сначала просматривать заголовки и удалять подозрительные письма сразу же на сервере, не скачивая их на свой ПК. Даже если файл-вложение прислан якобы от друга, следует отнестись к этому с подозрением – возможно, это сообщение отправлено сетевым червем. Сомнительное сообщение следует удалить полностью: сначала в папке «Входящие», потом в папке «Удаленные».

Подключите смс-оповещение

Такая услуга сейчас предоставляется практически во всех банках – клиенту подключается смс-уведомление по операциям с картой. При получении сообщения об операции, которую вы не совершали, следует сразу же обратиться по телефону в Службу поддержки своего банка.

Соблюдая эти правила, вы сможете свести риски при использовании онлайн-банкинга к минимуму.

http://credit-card.ru