

Правила интернет транзакций

1. Защити свой компьютер.

Своевременно проверяйте обновления программного обеспечения. Обязательно установите антивирусное и антишпионское ПО. Никогда не отключайте firewall. Защитите свой wi-fi роутер паролем и используйте usb-накопители с осторожностью.

1



2. Используйте только сложные пароли.

Самые эффективные пароли – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Вам в любом случае будет намного проще и главное безопаснее создать свой сложный пароль, чем злоумышленникам такой пароль разгадать. Пароль «Denis1986» взламывается очень просто, поэтому мы советуем Вам придумать 2 вида паролей:

2

- 1) длинные и сложные пароли для платежных систем;
- 2) простые и легко запоминающиеся для форумов и других, не представляющих опасности для ваших денег.

Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail или в социальных сетях.

3. Не переходите по ссылкам. Набирайте адрес сайта самостоятельно.

При переходе по ссылке из сомнительных источников (e-mail, форумы, сообщения в соц.сетях, всплывающие окна), Вы рискуете попасть на «фишинговый сайт».

3

4. Всегда проверяйте, установлено ли защищенное соединение.

В сети Интернет используется в основном два протокола: HTTP и Secure HTTP. Перед тем как ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обратите внимание на адресную строку, убедитесь, что имя протокола имеет вид https://, а не http ("s" – значит secure. англ. «защищенный»). Сертификаты подлинности получают только законопослушные компании, проверенные специалистами. Также о защищенности интернет-соединения свидетельствует значок амбарного замка на зеленом фоне рядом с адресной строкой.

4

5. Совершайте транзакции только на домашнем компьютере.

Никогда не оплачивайте счета, не проверяйте баланс личного счета, не совершайте покупки и другие операции с банковскими картами или электронными деньгами на компьютерах с общим доступом, а также на других мобильных устройствах (планшетах, телефонах), подключенных к публичным точкам доступа WiFi.

5



Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям, номерам кредитных карт, электронной почте и т.д.). Суть заключается в том, что мошенник создает интернет-страницу, идентичную настоящей, на которой у пользователя запрашивается конфиденциальная информация с целью ее получения мошенником. В первую очередь при переходе на сайт обращайте внимание на адресную строку. Зачастую мошенники подменяют одну или несколько букв в названии сайта (пример: <http://www.sberbank.ru/> - <http://www.sbenbank.ru/>).