АО ПЕРВЫЙ ИНВЕСТИЦИОННЫЙ БАНК

ПАМЯТКА
о безопасном использовании системы «Интернет-банк»

Развитие банковских интернет-технологий и новых платежных систем способствует появлению новых видов мошенничества: посторонним людям становятся известны ваши пароли, номера кредитных карт, номера электронных кошельков и т.д.

В частности, Банк России сигнализирует о появлении в российском сегменте сети Интернет веб-сайтов, имитирующих интернет-представительства ряда российских кредитных организаций. Доменные имена и стиль оформления сайта, как правило, сходны с именами подлинных веб-сайтов банков, а содержание прямо указывает на их, якобы, принадлежность соответствующим кредитным организациям. Однако если присмотреться, окажется, что это не их сайт - адрес отличается, хотя дизайн очень похож. Просто мошенники постарались сделать точную копию настоящего сайта, а введя данные по предложенной ссылке, ваш пароль становится доступным мошенникам. На поддельном сайте вам предложат ввести, например, данные своего аккаунта (логин и пароль клиента) или данные кредитной карты. И несмотря на то, что сайт выглядит почти как настоящий, эти данные пойдут прямиком к мошенникам. Вступление в деловые связи с лицами, фактически представляющими ложные банки, рискованно и может привести к нежелательным последствиям.

В целях противодействия распространению подобных негативных явлений Банк России с 11.06.2009г. регулярно размещает на своем веб-сайте (cbr.ru) список адресов (доменных имен) официальных веб-сайтов кредитных организаций. Чтобы не попасть в неприятную ситуацию, следует выполнять несколько простых рекомендаций.

Итак, что нужно знать о сетевом мошенничестве:

- Будьте предельно внимательными, когда вам приходят письма с запросом какой-либо персональной информации, либо с требованием ее обновить на сайте.
- Если письмо не подписано цифровой подписью, то нельзя быть уверенным, что оно не поддельное.
- Мошенники часто используют специальные приемы, чтобы вызвать реакцию на письмо. Типичными являются фразы с угрозами каких-либо неприятных последствий, в случае если вы не перейдете по ссылке. Либо наоборот, обещания каких-то бонусов от известного сервиса.
- Чаще всего мошенникам требуются логины, пароли, номера кредитных карт и т.п.
- Как правило, данные письма не персонализированы, т.е. не содержат вашего имени в адресе.
- Не открывайте писем и вложений, полученных от неизвестных вам отправителей.
- Никогда не переходите по ссылкам, нажимая их прямо в письме! Гораздо безопаснее набрать вручную нужный адрес в браузере, либо позвонить в ту компанию, от имени которой пришло письмо.
- Никогда не заполняйте персональными данными HTML формы, которые расположены прямо в письме.
- Всегда проверяйте, что для передачи персональной информации используется шифрованное соединение. Чтобы проверить шифруются ли данные, посмотрите на ссылку страницы, где вводятся данные. Адрес должен начинаться с “https://”, а не с “http://”.
- При работе с системой «Интернет-банк» рекомендуется использовать персональный межсетевой экран.
- Всегда используйте лицензионное антивирусное программное обеспечение, регулярно выполняйте полную проверку компьютера, ежедневно обновляйте антивирусные базы, не отключайте антивирусное ПО и не приостанавливайте защиту, помните отключение защиты даже на короткий промежуток времени ставит под угрозу безопасность вашего компьютера.

Следует помнить и учитывать, что большинство случаев хищения ключей и паролей осуществляются:

- лицами, имевшими доступ к Вашему компьютеру, с которого осуществлялась работа в системе дистанционного банковского обслуживания (необходима повышенная внимательность и контроль);
- злоумышленниками путем заражения через сеть Интернет компьютеров Клиентов вредоносными программами с последующим хищением учетных данных и паролей Клиентов (необходима установка программного обеспечения, предназначенного для безопасной работы в сети Интернет (в том числе

антивирусного ПО), его правильная настройка и контроль функционирования, в том числе своевременное обновление операционной системы, антивирусных баз и модулей другого установленного программного обеспечения, реализующего функции информационной безопасности).

Если Вы потеряли мобильный телефон, на который приходят SMS с разовым паролем, немедленно заблокируйте SIM-карту. В случае смены номера мобильного телефона необходимо уведомить Банк.

В случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!