КБ «Геобанк» (ООО)
Россия, 105066, г. Москва, ул. Нижняя Красносельская, д. 40/12, кор.20
Тел. + 7 (495) 660-08-88 | 8 800 333 99 19

ПАМЯТКА КЛИЕНТУ
О РИСКАХ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Уважаемые клиенты! КБ «Геобанк (ООО) информирует: в последнее время в российском сегменте сети Интернет появились web-сайты, имитирующие Интернет-представительства ряда российских кредитных организаций. Доменные имена и стиль оформления таких сайтов сходны с именами подлинных web-сайтов банков, при этом посетителям таких сайтов сообщают заведомо ложные банковские реквизиты и контактную информацию. Также участились сетевые атаки на сайты и серверы (далее - ресурсы) кредитных организаций и попытки неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи, ПИН-коды и номера банковских карт, а также персональные данные их владельца).

В целях противодействия распространению подобных негативных явлений Банк России регулярно размещает на своём web-сайте www.cbr.ru список адресов (доменных имён) официальных web-сайтов кредитных организаций (http://www.cbr.ru/credit/CO_SitesFull.asp). О случаях выявления ложных web-сайтов КБ «Геобанк (ООО) или проявлениях интернет-мошенничества убедительно просим сообщать в наш банк по электронному адресу: info@geobank.ru или по телефону: 8 800 333-99-19, +7 (495) 660-08-88

Считаем необходимым проинформировать о наиболее частых попытках проявления мошенничества и основных способах их предотвращения.

Виды мошенничества:

- При посещении пользователями страниц сети Интернет или при взаимодействии с другими информационными ресурсами без включенного антивирусного программного обеспечения. В это время на компьютер клиента с web-сайта могут передаваться вредоносные программы, являющиеся компьютерными вирусами или "закладками", выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей систем дистанционного банковского обслуживания.
- По электронной почте направляются сообщения, в которых под какими-либо предлогами (техническое переоснащение организации, обновление или сверка каких-либо баз данных и т.п.) предлагается сообщить конфиденциальные данные. Как правило, в этом же письме Пользователю передается ссылка для захода якобы в клиентский Интернет-банк. Чтобы выглядеть более правдоподобно, мошенники могут написать, что никакой другой адрес не доступен (например, после аварии). Смысл в том, что ссылка ведет не на настоящий сайт Интернет-банка. В результате Пользователь, который не следует строгим инструкциям безопасности, переходит на сайт мошенников, думая, что перешел на подлинный сайт Интернет-банка, и вводит свои данные для авторизации на сайте. После этого ему может быть выдано сообщение об ошибке, и он будет отправлен на сайт настоящего Интернет-банка, где сможет увидеть всю необходимую ему информацию. При этом, Пользователь может даже не догадываться, что зайдя на подложный сайт, он уже передал свои данные злоумышленникам.
- При проведении операций через банкоматы используются накладные устройства на клавиатуру для ввода ПИН-кода или на устройство для приема карт в банкомат, а также специально приспособленные для этих целей “фальшивые” банкоматы, которые незаконно устанавливаются, как правило, в неконтролируемых

ИНН 1102008681 КПП 770101001 ОГРН 1021100000393
КОР.СЧЕТ 30101810645250000775 в ГУ БАНКА РОССИИ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
БИК 044525775 ОКПО 16937128 ,РЕГ.НОМЕР № 2027

банковскими/кредитными организациями местах и внешне не отличаются от банкоматов, легально используемых банковскими/кредитными организациями

- При телефонном мошенничестве на мобильные телефоны клиентов направляются SMS-сообщения о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат банку. Также имеют место звонки с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п., тем самым, провоцируя к вступлению в контакты с мошенниками.
- Путем несанкционированного доступа к идентификационной информации клиентов банка (пароли, ключевые носители, секретные ключи ЭП и т.д.), используемой ими при осуществлении финансовых операций через системы дистанционного банковского обслуживания, такие как Банк-Клиент, Банк–Клиент через Интернет.

Способы мошенничества могут быть самыми разнообразными и далеко не ограничиваются перечисленными выше!

Основные способы предотвращения мошенничества:

- всегда использовать только лицензионное программное обеспечение с последними его обновлениями.
- не передавать персональную/конфиденциальную информацию посторонним/неуполномоченным лицам.
- соблюдать режим информационной безопасности, регламентов доступа к компьютеру и секретным ключам ЭП.
- игнорировать электронные сообщения с просьбой ввести персональную (конфиденциальную) информацию, так как уполномоченные сотрудники Банка не занимаются подобной рассылкой.
- игнорировать SMS и телефонные сообщения автоинформаторов, преследующих целью последующее разглашение персональной/конфиденциальной информации, так как уполномоченные сотрудники Банка не занимаются подобной рассылкой.
- всегда использовать антивирусные средства защиты с последними обновленными базами данных при взаимодействии с сетью Интернет и другими информационными ресурсами.
- использовать в организации программные средства по обнаружению и предотвращению несанкционированного доступа (файрволы, средства обнаружения вредоносного кода и т.д.) с последними их обновлениями.
- в случае компрометации или подозрения на компрометацию секретных ключей ЭП системы дистанционного банковского обслуживания “Банк-Клиент” и «Банк-Клиент через Интернет» необходимо незамедлительно обратиться в Банк для блокирования скомпрометированного секретного ключа ЭП.
- использовать банкоматы, установленные в безопасных местах (в госучреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
- не использовать банковские карты в организациях торговли и обслуживания, не вызывающих доверия.
- при совершении операций с банковской картой без использования банкоматов не выпускать ее из поля зрения.
- осуществлять информационное взаимодействие с банком и другими кредитными организациями только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные WEB-порталы/сайты, обычная и электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в банке или других кредитных организациях.
- при утере/краже карты немедленно сообщите об этом в банк.