Приложение к Приказу № 2099/3 от 17.11.2017г.

Акционерное общество коммерческий банк «Пойдём!»

Служба информационной безопасности

Основные меры безопасности при использовании онлайн-банкинга

Используйте только доверенные компьютеры с лицензионным программным обеспечением.

Если у вас на счете значительные денежные суммы, которыми вы управляете в Интернет-банке, то правильным решением может быть выделение отдельного компьютера, который используется только и исключительно для Интернет-банкинга.

Для этих целей не нужен «навороченный» компьютер. Операционная система такого компьютера должна быть получена у надежного поставщика, и должна своевременно обновляться. Никаких дополнительных программ, кроме необходимых для Интернет-банка, а также антивируса и фаервола, на такой компьютер ставить не стоит.

Фаерволом следует запретить любые соединения с ресурсами сети Интернет, кроме самого банка, и сетевых адресов для обновления системы и необходимых программ. Физический доступ к такому компьютеру должен быть предельно ограничен. В идеале работать за таким компьютером может только владелец банковского счета. А для исключения несанкционированного доступа к информации посторонних лиц во время отсутствия владельца, можно зашифровать жесткий диск компьютера с предзагрузочной аутентификацией. Если это нетбук или ноутбук, то в случае полнодискового шифрования информация не будет скомпрометирована даже при утере компьютера.

При соблюдении таких жестких условий компьютер может считаться доверенной средой.

Не входите в свой Интернет-банк 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.

Регулярно проводите полную антивирусную проверку компьютера и мобильного устройства.

Регулярно делайте полную проверку компьютера программой-антивирусом. Установите автоматическое обновление антивирусных баз и операционной системы.

Своевременно обновляйте операционную систему, браузеры, антивирус и другие программы для защиты от хакерских атак.

Не используйте старые операционные системы и программы, лучше использовать более своевременные и в дальнейшем их обязательно обновлять. Это относится также к интернет-браузеру и почтовым программам. Последние обновления операционных систем и программ разрабатываются с учетом новых появившихся угроз и вирусов.

Проверяйте адрес сайта

Если адрес сайта Интернет-банка отличается даже одной буквой – это подставной фишинговый сайт мошенников. Внешне он может быть почти неотличим от настоящего, название сайта – практически аналогичное, мало кто будет разбирать по буквам. В итоге – перехват персональных данных и кража денег.

Если интернет-обозреватель предупреждает, что сертификату безопасности сайта доверять нельзя – не доверяйте. Проверьте, что веб-адрес в адресной строке браузера начинается с "https". Не с «http», а именно с «https». Иначе вы находитесь на незащищенном веб-сайте, и вводить данные нельзя! Буква «**s»** после «**http»** означает, что при обмене информацией с сайтом Интернет-банка используется специальный защищённый протокол TLS, обеспечивающий безопасность передачи данных.

Используйте сложный пароль

Придумайте для входа в Интернет-банк сложный пароль длиной не менее 8 символов букв, цифр и спецсимволов и никому его не сообщайте, а тем более, не записывайте на карте. Лучше вообще его не записывать. А если забыли, воспользоваться сервисом по восстановлению пароля. Не ставьте такой пароль на запоминание, а каждый раз вводите его вручную. Используйте виртуальную клавиатуру для ввода пароля.

Никому не сообщайте пароли для входа в Интернет-банк

Даже своим близким и сотрудникам банка. Для входа в Интернет-банк кредитная организация запрашивает от клиента только логин и пароль. Номер телефона,

данные паспорта, ПИН-код и другие личные данные – НИКОГДА не запрашиваются. Если эти данные требуют от вас, это мошенники. Немедленно покиньте этот сайт и сообщите в ваш банк.

Ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет-банк или для подтверждения платежей, а также данные ваших банковских карт. Злоумышленники могут представляться сотрудниками банка, государственных органов, служб, сотовых компаний и др.

Будьте осторожны при использовании мобильного телефона.

В случае утери мобильного телефона, на который приходят SMS с разовым паролем, немедленно свяжитесь со своим сотовым оператором и заблокируйте SIM-карту.

Избегайте регистрации номера вашего мобильного телефона, на который приходят SMS с разовым паролем, в социальных сетях и других открытых источниках.

Если вам пришло SMS с паролем для платежа, который вы не совершали, известите об этом банк! Если вас под любым предлогом просят ввести/назвать пришедший по SMS пароль, **ни в коем случае не вводите и не называйте его**, кем бы ни представился ваш собеседник.

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

При получении сообщения об операции, которую вы не совершали, следует сразу же обратиться по телефону в Службу поддержки своего банка.

Установите лимиты на операции в Интернет-банке

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

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