УТВЕРЖДАЮ
Председатель правления
АО «Ури Банк»

Ким Ин Чжу
«23» октября 2024 г.

ПАМЯТКА КЛИЕНТУ
по соблюдению мер информационной безопасности при использовании системы электронного документооборота «Интернет-Банк»

Уважаемый Клиент!

Обязанность по обеспечению защиты от несанкционированного доступа к установленному в Вашей организации программному обеспечению Системы «Интернет-Банк» и к ключам электронной подписи (ЭП) возлагается на Вас. Выполнение настоящих требований по информационной безопасности позволит обеспечить защиту информационного обмена Вашей организации с Банком и минимизировать риски возможных финансовых потерь.

1 Общие положения

1.1 Кража учетных данных – хищение личных данных клиента Банка и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.2 Задачи защиты информации сводятся к минимизации ущерба и предотвращению злонамеренных воздействий. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Банка, так и на стороне клиента.

1.3 Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

1.4 «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5 Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

1.6 Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2 Рекомендации по защите информации от воздействия вредоносного кода

2.1 На персональном компьютере Клиента должно быть установлено лицензированное антивирусное программное обеспечение (ПО). Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным ПО в автоматическом режиме.

2.2 Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного ПО.

2.3 Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т.п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

2.4 При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

2.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо связаться со Службой технической поддержки и обратиться в Банк для подачи заявления о приостановлении обслуживания по Системе «Интернет-Банк». После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей доступа в Систему «Интернет-Банк» и произвести внеплановую смену ключей ЭП Уполномоченных лиц.

2.6 Старайтесь не использовать компьютер, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.7 Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

3 Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1 Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем.

3.2 Вход в систему необходимо осуществлять только с сайта https://bank.woori.ru/ . Обращайте внимание, что в адресной строке браузера присутствует именно этот адрес, остерегайтесь похожих названий: wooori.ru, woort.ru, wo0ri.ru и т.д. Не вводите аутентификационных данных на любых других сайтах.

3.3 Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.4 Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.5 Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Банк всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.6 Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.7 Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не

переходите по этой ссылке. Стоит обратить внимание на **владельца сайта**, воспользовашись сервисом «Whois», например (https://www.nic.ru/whois/). **Важно!** Если сайт, маскируется под корпоративный, появился недавно, а вкачестве владельца указано частное лицо, то высока вероятность, что сайт мошеннический.

3.8 Обращайте внимание на графу «Последний визит» на главной странице системы «Интернет-Банк». Там отображается информация о последнем входе в систему «Интернет-Банк». Если время входа или реквизиты устройства с которого осуществлялся вход кажутся Вам подозрительными, обратитесь в Службу технической поддержки или в подразделение Банка, с соответствующим заявлением и заблокировать доступ к Системе «Интернет-Банк».

3.9 При компрометации/подозрениях на компрометацию пароля/логина, ключей электронной подписи необходимо самостоятельно произвести смену пароля/логина, выполнить процедуру перегенерации ключей в Системе «Интернет-Банк» и обратиться в Службу технической поддержки или в подразделение Банка, с соответствующим заявлением и заблокировать доступ к Системе «Интернет-Банк».

4 Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1 Рекомендуем регулярно менять пароль для работы со своими учетными данными в Системе «Интернет-Банк». Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.2 Необходимо хранить ключевую информацию на RuToken (eToken) и хранить его в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа.

4.3 Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем банковском счете и т. д.).

4.4 В том случае, если Вы обнаружили, что Ваш пароль от банковской системы скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.1 .

4.5 Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Банк для получения инструкций по смене пароля.

4.6 Никому не разглашайте пароль от банковской системы. Банк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).

4.7 Не пересылайте файлы с конфиденциальной информацией для работы в банковской системе по электронной почте или через SMS-сообщения.

4.8 Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе, посторонних лиц.

4.9 Незамедлительно обращайтесь в Банк в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

4.10 Ежедневно проверяйте выписку по счетам организации.

4.11 Поддерживайте актуальность e-mail адресов для рассылки уведомлений об операциях. При изменении e-mail адреса предоставьте в Банк дополнительное Заявление по форме Приложения 2 к Соглашению об организации системы электронного документооборота «Интернет-Банк».

4.12 При внезапном нарушении работоспособности компьютера, с которого осуществляется доступ в Систему «Интернет-Банк», необходимо немедленно сообщить об этом в Службу технической поддержки банка и проверить санкционированность последних проведенных в Системе «Интернет-Банк» платежей.

4.13 Персонифицированные ключи ЭП должны формироваться Уполномоченными лицами организации самостоятельно.

4.14 RuToken (eToken) с ключами ЭП необходимо подключать к компьютеру только на время работы в Системе «Интернет-Банк».

4.15 Покидая рабочее место, обязательно блокируйте компьютер и извлекайте RuToken (eToken) с ключами. В нерабочее время он должен храниться способом, исключающим несанкционированный доступ к нему.

4.16 Необходимо выключать компьютер, с которого осуществляется доступ в Систему «Интернет-Банк», по окончании рабочего дня.

Выполнение данных правил позволит минимизировать риски несанкционированного доступа к информации по Вашим счетам.