Рекомендации по обеспечению информационной безопасности
для клиентов ООО «КЭБ ЭйчЭнБи Банк»

1. Термины и определения

Термин	Определение
Вредоносный код	Часть программы, действие которой выходит за пределы разрешенных функциональных возможностей и позволяет считать всю программу наносящей вред
Вирус	Вид вредоносного ПО, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи

2. Общие положения

2.1. 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.

2.2. 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.

2.3. 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.

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

2.5. Антивирусная защита осуществляется с целью исключения возможностей появления на средствах вычислительной техники, с которых осуществляется работа с системой, компьютерных вирусов и вредоносного кода, направленных на разрушение, нарушение работоспособности или модификацию ПО либо на перехват информации, в том числе паролей.

2.6. 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.

3. Рекомендации по защите информации от воздействия вредоносного кода

3.1. На средстве вычислительной техники клиента должно быть установлено антивирусное ПО при наличии технической возможности.

3.2. 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 средством в автоматическом режиме.

3.3. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная

проверка средства вычислительной техники на предмет наличия вирусов и вредоносного кода. Проверка должна осуществляться согласно расписанию, выставленному в настройках антивирусного средства.

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

3.5. При использовании сети Интернет для обмена почтовыми сообщениями должно применяться антивирусное ПО, разработанное специально для почтовых клиентов.

3.6. 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.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

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

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

4. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети интернет

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

4.2. 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.

4.3. 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.

4.4. 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.

4.5. 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.

4.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический веб-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается

4.7. с http:// вместо https://), не переходите по этой ссылке.

4.8. Всегда проверяйте, что сайт имеет сертификат безопасности, и проверяйте название сайта. Особенно обращайте внимание на замены букв на похожие символы, изменение домена (.cc вместо .ru).

4.9. Рекомендации по предотвращению осуществления несанкционированного доступа

третьими лицами

4.10. Рекомендуем регулярно менять пароль для работы со своим аккаунтом. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

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

4.12. В том случае, если Вы обнаружили, что Ваш пароль скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 5.1

4.13. Не разглашайте свой пароль от системы никому, даже близким друзьям или членам семьи. Банк не рассылает электронных писем, СМС- или других сообщений с просьбой уточнить Ваши конфиденциальные данные.

4.14. Не пересылайте файлы с конфиденциальной информацией для работы в системе по электронной почте или через СМС-сообщения.

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

4.16. Незамедлительно обращайтесь в Банк, если Вы обнаружили операцию, которую Вы не проводили.

5. Рекомендации по предотвращению осуществления несанкционированного доступа третьими лицами

5.1. Рекомендуем регулярно менять пароль для работы со своим аккаунтом. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

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

5.3. В том случае, если Вы обнаружили, что Ваш пароль скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 5.1

5.4. Не разглашайте свой пароль от системы никому, даже близким друзьям или членам семьи. Банк не рассылает электронных писем, СМС- или других сообщений с просьбой уточнить Ваши конфиденциальные данные.

5.5. Не пересылайте файлы с конфиденциальной информацией для работы в системе по электронной почте или через СМС-сообщения.

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

5.7. Незамедлительно обращайтесь в Банк, если Вы обнаружили операцию, которую Вы не проводили.

6. Рекомендации по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента.

6.1. Если на Ваш мобильный телефон звонят с незнакомого номера, представляясь сотрудником правоохранительных органов (главное управление МВД, следственный комитет, ФСБ), технической поддержки Банка и сообщают о якобы имевших место попытках несанкционированного перевода денежных средств или оформления кредита по доверенности или на несуществующих родственников, незамедлительно прервите разговор. При необходимости самостоятельно перезвоните по номеру телефона, указанному на официальном сайте Банка.

6.2. Если на Ваш мобильный телефон звонят с незнакомого номера, представляясь сотрудником правоохранительных органов (главное управление МВД, следственный

комитет, ФСБ), технической поддержки Банка и сообщают о якобы имевших место попытках несанкционированного перевода денежных средств или оформления кредита по доверенности или на несуществующих родственников, незамедлительно прервите разговор. При необходимости самостоятельно перезвоните по номеру телефона, указанному на официальном сайте Банка.

6.3. Не сообщайте кому-либо, в том числе родственникам и знакомым свои логины, пароли от личных кабинетов и учетных записей, PUSH-коды, SMS-коды и коды доступа, одноразовые пароли, реквизиты банковских карт и счетов, ПИН-коды, CVV/CVC-код (цифры на обратной стороне банковской карты).

6.4. Внимательно читайте текст сообщений, которые Вам приходят от государственных сервисов («Госуслуги», «mos.ru» и прочие) или от Банка. Если сообщение содержит фразу, смысл которой «не сообщайте содержимое кому-либо...», значит оно предназначено только Вам.

6.5. Если Вам позвонили и сообщают, что Вы стали участником какой-то мошеннической схемы или тяжких противоправных деяний, требуют незамедлительного выполнения каких-либо действий – незамедлительно прервите разговор. Не принимайте решения, не предпринимайте действий на эмоциях, в состоянии шока или растерянности.

6.6. Не переходите по сомнительным ссылкам, полученным по электронной почте, в SMS-сообщениях, мессенджерах или социальных сетях.

6.7. Не устанавливайте программное обеспечение, обновления, антивирусы и прочие программы защиты из непроверенных/неофициальных источников. Банк не направляет ссылки для установки ПО и обновлений в мессенджерах и SMS-сообщениях.

6.8. Не используйте незащищенные беспроводные WiFi сети для выполнения операций по переводу денежных средств (например, WiFi сети в интернет-кафе, транспорте, общественных местах и т.д.).

6.9. После завершения работы в личном кабинете Вашего финансового приложения обязательно завершайте сессию, для этого выберите в меню пункт «Выход». После того как Вы вошли в Ваше финансовое приложение не оставляйте его работающим в фоновом режиме. Не оставляйте электронное устройство с установленным и работающим на нем финансовым приложением без присмотра.

6.10. При переводе денежных средств через Ваше финансовое приложение внимательно проверяйте реквизиты платежных распоряжений. Например, мошенники могут указать в договоре одни реквизиты контрагента (например, проверенного надежного поставщика), а в платежных документах (например, в счете на оплату) совпадать будет только наименование получателя платежа, при том, что иные реквизиты (ИНН, ОГРН и прочие) могут быть отличными.

6.11. Соблюдайте требования по обращению с ключами электронной подписи (КЭП) и средствами криптографической защиты информации. Храните КЭП в надежном месте и никому их не передавайте. При возникновении подозрения на компрометацию КЭП незамедлительно сообщите об этом в Банк, выпустите новый КЭП.

6.12. Устанавливайте сложные пароли на электронные устройств, КЭП и в личном кабинете Вашего финансового приложения. Регулярно, не реже раза в три месяца, меняйте эти пароли.

6.13. Используйте только лицензионное программное обеспечение. Настройте автоматическое обновление системного и прикладного программного обеспечения, включая средства антивирусной защиты, настройте автоматическое обновление антивирусных баз.

6.14. Не доверяйте обслуживание и настройку программного обеспечения Ваших электронных устройствах случайным или посторонним лицам.

6.15. Не устанавливайте на свои электронные устройства средства удаленного доступа и управления.

6.16. Не используйте автосохранение паролей в браузерах.