Рекомендации по информационной безопасности  
в соответствии с правилами сервиса «Faktura.ru»

Для работы с ЭП:

1. Храните ключевые носители (смарт-ключи, флэш-карты и другие носители с записанными ключами) в месте, недоступном посторонним лицам. Исключите хранение ключей на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах.

2. Храните в тайне пароль доступа к ключу, исключите его запись на стикерах, носителях ключей и т.п.

Для работы с ПРОСТОЙ ЭП / АСП:

1. Запомните, что для входа в Интернет-банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Интернет-банке!

2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет-банк или для подтверждения платежей, а также номера ваших карт и CVV2/СVС2 коды.

3. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.

4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокируйте SIM-карту / войдите в Интернет-банк и удалите телефон из списка зарегистрированных устройств для получения PUSH-сообщений.

5. Запишите контактный телефон банка в адресную книгу или запомните его. В случае если в личном кабинете Интернет-банка вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в банк по ранее записанному вами телефону. Также для этих целей подойдет телефон, указанный на вашей банковской карте.

6. Устанавливайте мобильные приложения Faktura.ru только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является Center of Financial Technologies. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего телефона/смартфона.

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

Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах:

1. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным ПО и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.

2. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

3. Используйте виртуальную клавиатуру для ввода пароля.

4. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в банк с целью оперативного блокирования доступа!

5. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

6. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

7. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагировать на ошибки.

8. Запретите в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешите соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы ваши электронные почтовые ящики.

9. Не давайте разрешения неизвестным программам выходить в Интернет.

10. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

С дополнительными требования к информационной безопасности можно ознакомится в разделе «Безопасность» на сайте сервиса Faktura.ru в сети Интернет - https://faktura.ru.