

## **Требования и рекомендации по безопасному использованию системы «ИНТЕРНЕТ-БАНК»**

1. Запомните, что для входа в Интернет-Банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего номера мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Интернет-Банке (за исключением ввода номера телефона и карты при первичной самостоятельной регистрации в Системе)!
2. Никогда и ни при каких обстоятельствах не сообщайте никому свой пароль и PIN-код для входа в Интернет-банк или для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды.
3. Обязательно сверяйте текст SMS/PUSH-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS/PUSH-сообщении 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 SMS/PUSH-сообщения с Разовым секретным паролем, немедленно заблокируйте SIM-карту и /или сообщите об утере в Банк для осуществления блокировки системы.
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/PUSH-сообщения с Разовым секретным паролем, в социальных сетях и других открытых источниках.
8. Следуйте иным рекомендациям информационной безопасности, размещенным на сайте Системы [www.faktura.ru](http://www.faktura.ru) и Сайте Банка.

### **Общие правила безопасности**

1. Обязательно используйте только доверенные Устройства с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением (на компьютерах и при наличии технической возможности — на телефонах и планшетах) и персональным межсетевым экраном (на компьютерах). Своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку Устройств на наличие вредоносного программного обеспечения. Своевременно обновляйте операционную систему и браузеры, незамедлительно устанавливайте обновления безопасности. По возможности используйте разные устройства для формирования платежей и получения подтверждения платежей.
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. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!
4. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
5. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.
6. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.
7. 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.
8. Не давайте разрешения неизвестным программам выходить в Интернет.
9. Не оставляйте Устройство с активной системой Интернет-Банк без присмотра.
10. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.
11. Не используйте вход по отпечатку пальца в Мобильное приложение, если в Устройстве зарегистрированы отпечатки пальцев других людей. В противном случае указанные люди смогут выполнить вход и выполнять платежи и другие операции в Мобильном приложении от вашего имени.

## Рекомендации по составлению пароля

Правильно составленный пароль для входа в систему — одно из важнейших препятствий на пути злоумышленников.

Составляйте пароль с учетом следующих рекомендаций:

- Пароль должен содержать не менее 8 символов;
- Пароль должен включать буквы верхнего и нижнего регистра, цифры и спецсимволы (@, #, \$, %, <, ^, &, \*).

## Что такое слабый пароль/PIN-код

Слабый пароль/PIN-код — это пароль/PIN-код, который может быть угадан или вычислен методом перебора по словарю/словарям за приемлемый для злоумышленников срок.

К слабым паролям/PIN-кодам относятся следующие:

- Пароли, содержащие в том или ином виде Логин или часть Логина;
- Личная информация, которая относительно легко может стать известной злоумышленникам, например, даты рождения, номера телефонов, клички домашних животных, имена детей и др.;
- Слова, которые можно найти в словаре;
- Слова компьютерной терминологии, например, команды операционной системы, названия оборудования, программ и др.;
- Комбинации расположенных рядом символов клавиатуры, например, qaz, qwerty, 123456 и др.;
- Любое из указанного выше, набранное в транслитерации;
- Любое из указанного выше, дополненное цифрами;
- Любое из указанного выше, набранное в обратном порядке;
- Любое из указанного выше, набранное в верхнем регистре.

## Несколько способов составить хороший пароль

Хороший пароль — это пароль легкий для запоминания и в то же время достаточно хорошо защищенный от угадывания или вычисления методом перебора по словарю/словарям.

Существует ряд способов составить хороший пароль:

- Придумайте в качестве пароля хорошо запоминающуюся осмысленную фразу;
- Измените чередование строчных и прописных знаков, используйте вместо пробела знак подчеркивания: sANTA\_cLAUS;
- Набирайте ваш пароль на клавиатуре со сдвигом на одну клавишу, например, вправо: dSMYS+l:SID;
- Можно использовать в качестве пароля какую-нибудь стихотворную фразу (например, «Мне нравится, что вы больны не мной») и из каждого слова включить в пароль первые две буквы, при этом поставив английскую раскладку клавиатуры (например, в данном случае получится пароль Vyuhxnds,jytvy);
- Взять какое-нибудь сложное, но известное вам профессиональное слово (например, цистрансизомерия) и вставить в его середину какой-нибудь цифровой код, при этом установив английскую раскладку клавиатуры;

В этих случаях вам придется помнить лишь ключевую фразу и то, что с ней надо сделать. Это проще запоминания набора случайных символов и в то же время данные преобразования дают достаточно стойкий пароль.

## Управление паролями/PIN-кодами

- Смена пароля/PIN-кода должна производиться минимум раз в три месяца;
- Избегайте использования одинаковых паролей/PIN-кодов к разным системам;
- Не производите установку флажка «Запомнить пароль».

## Основные меры для предотвращения получения пароля/PIN-кода злоумышленником:

- Никогда не входите в систему и не набирайте пароль/PIN-код с незнакомого Устройства, или с Устройства, на который имеют доступ лица, незнакомые вам или не вызывающие полного доверия;
- Никогда ни при каких обстоятельствах не называйте свой пароль/PIN-код, даже если вы сами звоните в Службу информационной поддержки клиентов Банка или по контактному телефону службы технической поддержки Сервиса, а также помните, что администрация Сервиса не рассылает сообщений по email и не звонит клиентам по телефону с просьбой предоставить пароль для совершения каких-либо действий;
- Обязательно проверяйте антивирусным программным обеспечением email-сообщения и содержимое ваших дисков.