Правила безопасности Системы «Интернет-банк»

Термины, используемые в настоящих Правилах, имеют то же значение, что и в Условиях.

Вход и регистрация

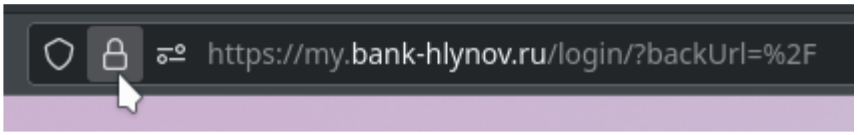
1. Для входа в Систему «Интернет-банк» нужны: логин, пароль и уникальный код из SMS-сообщения, которое приходит на ваш номер телефона при первом входе или авторизации с нового устройства. Никому и никогда не передавайте эти данные, даже сотрудникам Банка и специальным органам.
2. В случае, если на странице Вас просят ввести любую другую персональную информацию, например, Номер мобильного телефона, ИНН или прочие личные данные, не выполняйте никаких операций и свяжитесь с сотрудниками Банка по номеру телефона Единого сервисного центра 8 800 250 2 777.
3. Полный номер вашей банковской карты и также паспортные данные требуются только для процедуры регистрации и восстановления доступа.
4. Сотрудники Банка никогда не попросят вас установить какое-либо дополнительное приложение для помощи или решения вопроса, кроме самого официального приложения Интернет-банка.

Коды в SMS-сообщениях

1. Никому не говорите Ваш пароль и Разовый код безопасности операции. Если Разовый код безопасности можно сообщить менеджеру — мы сразу напишем это в SMS-сообщении с кодом.
2. Сотрудники Банка никогда не просят сообщить данные учетной записи или коды подтверждения операций перевода.
3. Банк никогда не отправляет коды подтверждения для отмены операций. Все направляемые вам коды – это коды подтверждения операции. Если сомневаетесь, то для отмены операции достаточно никуда не передавать такой код.
4. Внимательно проверяйте параметры операции в SMS-сообщении, содержащем Разовый код безопасности. Информация в нем должна совпадать с вашей операцией в Системе «Интернет-банк», которую вы хотите подтвердить. Если эта информация не совпадает, не вводите Разовый код безопасности и сообщите об этом сотрудниками Банка по телефону Единого сервисного центра 8 800 250 2 777.
5. Отключите отображение текста SMS-сообщения на экране смартфона или смарт-часов, установите код для его разблокировки, даже для кнопочного телефона. Это позволит сохранить в тайне от злоумышленников коды подтверждения операций.

Общие рекомендации

1. Установите и обновляйте антивирус на вашем компьютере. Желательно использовать антивирусные программы и на мобильных устройствах.
2. Никогда не устанавливайте на телефон приложения из недостоверных источников.
3. Не устанавливайте на смартфон и компьютер программы для удаленного управления устройством.
4. Своевременно устанавливайте обновления операционной системы своего компьютера и мобильного устройства.
5. При входе в Систему «Интернет-банк» убедитесь, что установлено защищенное соединение именно с Официальным сайтом Банка — https://my.bank-hlynov.ru



6. Если у Вас есть подозрения, что кто-либо использует Ваш пароль или исполняются операции, которые Вы не совершали, незамедлительно обратитесь в Банк, например, по вышеуказанному телефону Единого сервисного центра.
7. Все сообщения об активности мошенников важны. Банк использует их для пресечения деятельности мошенников. Ваша активная позиция помогает нам в этом.
8. Не подключайте к общедоступным беспроводным сетям (Wi-Fi) во время работы с банковскими и государственными сайтами/мобильными приложениями (Интернет-Банки, Госуслуги, Личный кабинет налоговой и прочее). Ведь даже в других ситуациях их использование небезопасно. Через них злоумышленники могут скопировать введенные вами конфиденциальные данные, как минимум логин и пароль.

Как придумать надежный логин и пароль?

Хороший пароль состоит из заглавных и строчных букв, цифр и знаков препинания. Чем длиннее пароль, тем сложнее его подобрать. Рекомендуем придумывать пароли не менее 8 знаков. Например, так может выглядеть надежный пароль длиной в 16 знаков — jcX5C1%vj-AyuMaR. Такие пароли невозможно подобрать с помощью словаря, а на перебор уйдут месяцы и годы.

Как запомнить пароль?

Лучше всего пароль запоминается тогда, когда вы его часто вводите. Если вы только придумали пароль, отключите галочку «запомнить меня», и вам придется вводить его каждый раз при входе в Систему «Интернет-банк». Так ваши руки научатся вводить его автоматически.

Специалисты по безопасности не советуют записывать пароли в открытом виде, даже если вы будете держать их в сейфе. Если вам необходимо записать пароль, сделайте это так, чтобы только вы знали, как его прочитать.

Ни в коем случае не держите пароли на стикерах на мониторе. Не носите их в бумажнике. Не записывайте в заметки в телефоне.

Как не рассекретить пароль?

1. Используйте правило: один ресурс — один пароль. Не устанавливайте одинаковые пароли на социальные сети, электронные ящики, и, тем более, банковские аккаунты.
2. Постарайтесь использовать двухфакторную авторизацию везде, где это возможно. Работает это очень просто: при каждом новом входе ресурс будет запрашивать у вас код из SMS-сообщения. А так как телефон всегда рядом с вами - мошенники до него просто так не доберутся.
3. По возможности, не вводите пароли на чужих компьютерах и мобильных устройствах. Особенно, если эти компьютеры находятся в публичной зоне использования: интернет-кафе, площадки на фуд-кортах, игровые клубы, библиотеки. Если все-таки пришлось, проверьте, чтобы функция «запоминания» вводимых данных была неактивна, а по окончании сеанса использования сайта/мобильного приложения найдите функцию «выхода» из учетной записи и воспользуйтесь ею. Не лишним будет сменить пароль.
4. Надежно защитите сложным паролем домашнюю беспроводную сеть.

5. Если беда произошла и ваш пароль попал в руки к мошенникам - меняйте его на новый только в безопасной среде. Например, только дома и только с того устройства, которое является лично вашим.
6. Обязательно установите PIN-код на свою SIM-карту. Любой современный оператор мобильной связи позволяет устанавливать такой код. Обычно, PIN можно установить в разделе настроек SIM-карты.
7. Не используйте простые пароли и легкие графические ключи на своем мобильном устройстве.
8. При потере мобильного телефона, на который Вы получаете SMS-сообщения с разовым кодом безопасности, сразу же обратитесь к оператору мобильной связи и заблокируйте SIM-карту. В случае утраты банковской карты, заблокируйте ее через Официальный Сайт Банка/Мобильное приложение Банка и/или уведомите Банк по телефону.