ТЕХНИЧЕСКИЕ УСЛОВИЯ ИНТЕРНЕТ-БАНКА

Технические условия пользования Интернет-банком LHV
Для полного использования возможностей Интернет-банка LHV, пользователю необходимо идентифицировать себя при помощи ID-карты, Mobiil-ID или PIN-калькулятора.

С **ID-картой** хорошо работают**:**

(i) В операционных системах Microsoft **Windows** (начиная с версии XP) браузеры Microsoft **Internet Explorer** (начиная с 7-ой версии) и **Mozilla Firefox** (начиная с 3-ей версии).

В других браузерах вход и/или подтверждение платежей подписью может не удастся.

(ii) В операционных системах Apple **Macintosh** (начиная с версии 10.6.x) - только **Firefox** (начиная с 3 версии).

Вход в интернет-банк при помощи ID-карты посредством Safari, вероятнее всего, не удастся.

(iii) В операционных системах **Linux** - браузер **Firefox** (начиная с 3-ей версии).

Войти в интернет-банк при помощи ID-карты посредством Lynx не удастся.

Для идентификации пользователя и подтверждения платежей при помощи **Mobiil-ID** и **PIN-калькулятора** в используемом браузере должен работать также **JavaScript**.

Безопасность в Интернет-банке LHV

В ходе работы по дальнейшему развитию Интернет-банка LHV, безопасность является фактором первой степени важности. Важную роль также играет сам пользователь Интернет-банка и используемое им программное обеспечение и оборудование. Использование Интернет-банка является настолько безопасным, насколько безопасно самое слабое звено во всей системе.

1. В целях обеспечения безопасности интернет-банка Банк делает следующее:

(i) Информация между пользователем и банком шифруется (при помощи метода SSL3 или TLS1 в протоколе HTTPS).

(ii) Пользователь интернет-банка идентифицируется при помощи уникального признака, а также ID-карты, mobiil-ID или PIN-калькулятора.

(iii) Если пользователь делает более 5-ти безрезультатных попыток входа, то его PIN-калькулятор блокируется.

(iv) Время сессии интернет-банка истекает.

2. Клиент/пользователь должен, со своей стороны, действовать следующим образом:

(i) Открывая Интернет-банк LHV, убедиться, что в адресной строке браузера отображается правильный адрес (https://www.lhv.ee), а также, что соединение шифруется.

Подлинность и шифрование подтверждает отображающееся в адресной строке браузера в зеленом цвете наименование сертифицируемого лица(AS LHV Pank [Ee]), наименование сертифицирующего лица (Thawte) и закрытый навесной замок (который может находиться также в нижней части окна).

(ii) Хранить свое имя пользователи и средства идентификации в безопасности.

Идентификация пользователя Интернет-банка LHV при помощи ввода имени пользователя и PIN кодов происходит только в электронной среде Интернет-банка. Представители LHV Pank никогда не спрашивают Ваших паролей и PIN кодов. Если кто-то пытается узнать Ваше имя пользователя или PIN коды по телефону, электронной почте или иным способом, откажитесь и сразу сообщите о произошедшем в службу поддержки клиентов LHV.

О потере ID-карты следует незамедлительно сообщить по телефону службы поддержки ID-карты 1777, в случае потери mobiil-ID - выдавшему SIM карту поставщику услуги, а о потере PIN-калькулятора - в службу поддержки клиентов LHV.

(iii) Назначать разумные и не превышающие собственные возможности лимиты на сумму операций, разрешенных в течение одного дня или месяца.

(iv) Защищать используемый для входа в Интернет-банк компьютер и его программное обеспечение (см. «Об Интернете и безопасности в общем»).

(v) При завершении пользования Интернет-банком, выйти из интернет-банка - кнопка ВЫХОД в шапке страницы интернет-банка.

3. Защитные элементы

Идентификация пользователя Интернет-банка LHV происходит при помощи защитных элементов. Выдаваемые Банком защитные элементы - это предоставляемые в утвержденном Банком порядке уникальные имя пользователя и PIN-калькулятор и, при помощи которых пользователь может заходить в Интернет-банк. Помимо PIN-калькулятора, пользователь может идентифицировать себя посредством Mobiil-ID и ID-карты.

При желании можно установить для себя временный пароль для торгов и временный пароль для использования форумов LHV. LHV не рекомендует использовать пароли. Если Вы все же желаете воспользоваться временными паролями, пароль должен быть как можно длиннее, должен содержать множество различных знаков и не должен содержать личной информации, которую можно было бы легко отгадать. В то же время пароль должен хорошо запоминаться, чтобы не было необходимости его записывать.

Если у Вас есть подозрения по поводу того, что Ваш счет использует кто-либо другой, или Вы обнаружите, что у Вас возникли проблемы с безопасностью Интернет-банка LHV, пожалуйста, сразу позвоните в нашу службу поддержки клиентов (+372 6 800 400).

Об Интернете и безопасности в общем

Интернет как опасность
Когда-то Интернет был закрытой сетью, соединяющей надежные компьютеры и образованных пользователей. Логические основы этой инфраструктуры были описаны в 70-х годах, исходя из доверия и простоты, и на безопасность тогда обращали мало внимания.

Сегодня в той же самой, но ставшей всемирной, среде действуют, помимо прочих, киберпреступники, чей успех зависит от эффективности использования компьютеров, в том числе и Вашего компьютера, и эффективного применения похищенной информации (в том числе данные Вашей кредитной карты, пароли Интернет-банка и т.д.)

Деятельность киберпреступников упрощает тот факт, что логические основания инфраструктуры интернета являются сегодня, по сути, такими же небезопасными как и пару десятилетий назад, когда в сети находились только надежные пользователи, и все доверяли всем.

Поэтому Вам, пользователю интернета, во избежании возможного ущерба целесообразно следовать принципам, о которых подробно, но на простом языке, написано на странице arvutikaitse.ee.

Атаки, не зависящие от Ваших привычек

Присоединенный к интернету или местной сети компьютер может быть довольно незащищенным - даже свежеустановленная операционная система MS Windows «прослушивает» исходящие из сети сообщения и при необходимости отвечает на них. Такой услугой является, например, «*File and Printer Sharing*».

При помощи целенаправленно созданного запроса умелый преступник может обмануть охрану компьютера (т.н.*remote exploit*) и получить доступ к документам владельца компьютера, установить вредоносные программы или полностью искалечить компьютер.

Как себя защитить?

Как правило, защититься от таких атак помогает правильно настроенный брандмауэр (*firewall*) и действующая антивирусная программа. Поставщиков предотвращающего появление вирусов программного обеспечения много, но пользователям MS Windows мы рекомендуем выбирать, например, из числа этих.

Кроме того, обязательно следует устанавливать обновления как операционной системы, антивирусной программы, так и используемого программного обеспечения.

Операционные системы Microsoft автоматически предлагают установить обновления программного обеспечения (если пользователь отдельно не запретил этого). Установить их вручную можно здесь.

Дополнения используемого на компьютере программного обеспечения можно скачать на домашней странице производителя программного обеспечения или при помощи программы по обновлению.

Например, в случае Adobe Reader выбор *check updates* в меню *help.*

Обязательно следует обновлять Adobe Flash, поскольку его ошибки очень часто используются для атак в интернете. Текущую версию можно проверить здесь, а скачать самую свежую - здесь.

Если Вы используете, к примеру, LHV Trader, то на Вашем компьютере обязательно должна быть установлена Java. Свои обновления программа Java предлагает сама, и их следует обязательно устанавливать.

Для обновления **Mac OS X** нужно время от времени выбирать в меню с изображением яблока «Software Update...» и позволять компьютеру установить необходимые дополнения.

В случае **операционной системы Linux** методика установки обновлений зависит от используемого дистрибутива. Как правило, в интерфейсе командной строки пользователь, обладающий правами root, должен запустить соответствующие команды. Например:

(i) Ubuntu (в одной строке 4 команды, все необходимы)
aptitude update && aptitude safe-upgrade && aptitude dist-upgrade && aptitude safe-upgrade

(ii) RedHat
yum update

(iii) Mandriva
urpmi-update -a

Атаки, использующие Ваши привычки

Самыми опасными и распространенными на сегодняшний день являются атаки, происходящие при (неведомом) содействии пользователя (т.н. *client side attack*). Например, Вам отправляется электронное письмо, к которому приложен файл с расширением .pdf, .doc, .jpg, .xlsx или иным расширением, открывать который Вы привыкли и программное обеспечение для открытия которого у Вас есть.

Содержание письма кажется правдоподобным (например, Вас приглашают на семинар, а программа находится в документе .pdf), Вы открываете приложенный файл при помощи Adobe Acrobat Reader, знакомитесь с содержанием, закрываете файл и через минуту забываете о нем.

Однако при открытии документа программа запустила содержавшийся в ней секретный код, который установил на Ваш компьютер программу, отслеживающую нажатие клавиш, и скрытую дверь, посредством которой автор атаки получает власть над Вашим компьютером. Ваша антивирусная программа не видит в этом проблемы, поскольку использованный для атаки метод программа еще не может различить - эта информация попадет в антивирусную программу только через несколько часов или в худшем случае - через несколько месяцев.

Содержащие вредоносный код файлы не всегда приходят только посредством электронной почты. Распространены также атаки, происходящие через MSN, Facebook и прочие используемые каналы общения, в которых Ваш друг (как будто) отправляет Вам файл, который советует открыть, или адрес, на который советует зайти при помощи браузера. При открытии файла происходит то же самое, что было описано выше, при открытии веб-адреса для атаки используется брешь в защите Вашего браузера.

Пользователь, то есть Вы, как правило, не узнает о хорошо проведенной атаке до того момента, пока с Вашей кредитной карты или банковского счета не начнут пропадать деньги.

Как себя защитить?

(i) Прежде чем открыть пришедший по электронной почте файл подумайте, является ли его отправитель надежным и сообщил ли он Вам об отправке файла.

(ii) Если Вы пользуетесь интернетом, подумайте, является ли страница, на которую Вам советуют зайти, надежной.

(iii) Если Вы находите внешне привлекательную программу, скринсейвер или новый *toolbar* для своего браузера, подумайте, действительно ли он Вам нужен, и и перевешивает ли это возможность потерять имеющиеся на банковском счете деньги.

(iv) Если дома есть несколько компьютеров, используйте для входа в Интернет-банк, совершения кредитных платежей и пр. важных дел только один из них. В отношении этого компьютера особенно внимательно следите за тем, что Вы делаете - какие странице посещаете, какие файлы открываете, какое программное обеспечение устанавливаете.

Ваша ID-Карта, Mobiil-ID и PIN-калькулятор

ID-карта является относительно безопасной, поскольку, если преступник и отслеживает Ваши нажатия клавиш (и узнает как Ваш код PIN1, так и код PIN2), он все же не получит доступа к Вашему банковскому счету, поскольку для авторизации необходим физический предмет - Ваша ID-Карта. Похитить её посредством электронных каналов он не сможет.

То же самое действует и в отношении Mobiil-ID и PIN-калькулятора, однако в отличие от ID-карты, PIN-калькулятор или mobiil-ID не нужно подключать к компьютеру.