

Финансовая инспекция | Правила безопасности
использования интернет-банка



Что нужно иметь в виду при использовании интернет-банка?

При использовании интернет услуг банка нужно быть бдительным и выполнять определенные правила безопасности.

Каждый клиент интернет-банка должен следить за тем, чтобы выход в интернет банк осуществлялся из достаточно защищенного компьютера

Межсетевые экраны

Каждый подключенный к интернету компьютер является потенциальной целью для атак извне. Для защиты компьютера необходимо использовать межсетевой экран (firewall). Межсетевой экран – это набор программных средств или электронное устройство, отслеживающие все исходящие и входящие соединения компьютера. При этом экран пропускает только одобренные пользователем подключения, блокируя все прочие соединения, которые могут быть запущены посторонними лицами извне.

Антивирусные программы и удаление программ-шпионов

Программы, цель которых, как правило, злоупотребление или уничтожение информации, находящейся в компьютере, называют злонамеренным программным обеспечением. К злонамеренным программным обеспечениям относятся вирусы, почтовые черви, трояны и прочие подобного рода программы. Такие приложения могут затруднять работу компьютера, уничтожать записанные на диск данные, собирать и пересылать посторонним лицам вводимые пользователем пароли, открывать доступ к компьютеру для посторонних лиц извне и преследовать прочие злоумышленные цели. Компьютерные вирусы распространяются при сохранении интернет-файлов (при установке, например, программ для общения в реальном времени или программ для обмена файлами), при просмотрении интернет-страниц, также через электронную почту, через CD диски и дискеты.

Для обнаружения и обезвреживания вирусов в каждом компьютере должно быть антивирусное программное обеспечение. Антивирусные программы следует регулярно обновлять.

Программами-шпионами называются программы, которые устанавливаются без ведома пользователя компьютера и которые позволяют незаметно отслеживать действия пользователя. Программы-шпионы могут записывать порядок нажатия пользователем клавиш, отслеживать вводимые пароли, регистрировать посещаемые страницы и запускаемые программы и собирать прочие данные о деятельности пользователя. Программы-шпионы часто попадают в компьютер при установке бесплатных приложений, найденных в интернете. Для удаления программ-шпионов существуют специальные программы-охранники, с помощью которых необходимо регулярно проверять состояние компьютера.

Ниже приведены некоторые ссылки, где можно найти антивирусные программы и программы для установления межсетевых экранов.

Программа	Интернет адрес
Старман – полезные программы для использования интернета	http://helpdesk.starman.ee/est/software.htm
Дополнительные услуги	http://www.elion.ee/wwwmain?screenId=html.citizen-profile.5366.13847
Элион – антивирусы и межсетевые экраны	
Антивирусы	
F-Secure	http://www.f-secure.com/
Trend Micro	http://www.trendmicro.com/
Symantec	
Norton Internet Security	http://www.symantec.com/product/index_homecomp.html
AVG	http://www.grisoft.com/us/us_index.php
ZoneAlarm	http://www.zonelabs.com/store/content/catalog/products/sku_list_zs.jsp?lid=db2_free
McAfee	http://us.mcafee.com/default.asp
Программы для удаления программ-шпионов	
Ada-Ware	http://www.ada-ware.com/
Spybot S&D	http://www.safer-networking.org/

Пользователями домашних компьютеров часто выступают дети, которые общаются в чатах, играют, просматривают интернет-страницы, обмениваются файлами и запускают полученные из интернета программы, назначение которых они не всегда понимают. Детей следует тоже ознакомить с правилами поддержания защиты компьютера, рассказать об возможных опасностях и предостеречь от сохранения и запуска неизвестных файлов. Следует избегать сохранения, запуска или открытия всех подозрительных и неизвестных файлов.

Программы для просмотра интернет-страниц (браузеры)

В операционных системах и браузерах время от времени выявляются незащищенные места и ошибки, поэтому их необходимо регулярно обновлять и устанавливать исправления. Поскольку устаревшие версии программ не обновляются, следует следить за тем, чтобы используемые для просмотра интернет страниц программы не были слишком старыми.

Время от времени при просмотрении интернет страниц на экране открываются окна для диалогов, где пользователю задается вопрос или спрашивается разрешение установить какую-либо программу. Прежде чем нажимать в появившемся окне какие-либо клавиши, следует внимательно прочитать появившийся текст. Если текст непонятен, следует закрыть окно используя крестообразный символ в правом верхнем углу. Нажимать клавиши внутри появившегося окна не следует.

Наиболее часто используемые программы для просмотра интернет страниц, такие как Internet Explorer и Netscape, позволяют пользователю автоматически сохранять пароли, используемые на определенных интернет страницах. Эту опцию следует отключить, или же использовать ее крайне осторожно.

Для отключения опции сохранения паролей:

В Internet Explorer

Из меню *Tools* выбрать *Internet Options*. Выбрать меню *Content* и найти клавишу *AutoComplete*. Убрать галочку у опции *User names and passwords on forms*. Клавиша *Clear Passwords* стирает ранее сохраненные пароли. В Internet Explorer можно также проверить, чтобы было запрещено сохранение зашифрованных страниц. Для этого нужно из меню *Tools* выбрать *Internet Options*. Далее выбрать *Advanced* и в открывающемся в нижней части экрана окне *Settings* найти клавишу *Security*. У опции *Do not save encrypted pages to disk* необходимо поставить галочку.

В Netscape

В браузере Netscape управление сохранением паролей происходит посредством меню *Edit* подменю *Preferences*. Там же можно просмотреть страницы, для которых на данный момент сохранены пароли. В открывшемся слева окне найти подменю *Privacy&Security* и в нем опцию *Passwords*. Если удалить галочку у *Remember Passwords*, то пароли в дальнейшем сохранятся не будут. Страницы, для которых пароли были сохранены, а также страницы, для которых сохранение паролей запрещено, можно просмотреть и отредактировать выбрав клавишу *Manage Stored Passwords*.

Вход в интернет банк и завершение работы с интернет банком

Вход в интернет банк

При введении в браузере адреса интернет банка между компьютером пользователя и сервером банка создается соединение при помощи протокола SSL (зашифрованное подключение). Интернет адрес при этом должен начинаться с *https://*. В нижнем правом углу браузера должно появиться изображение замкнутого навесного замка. При двойном щелчке на изображении замка открывается сертификат, который должен принадлежать соответствующему банку.

При возможности следует избегать использования интернет-банка на открытых для общественного пользования компьютерах, в безопасности которых вы не уверены. Если вход в интернет банк осуществляется все же из общественного компьютера, желательно по завершении работы очистить промежуточную (кэш) память компьютера. В промежуточной памяти сохраняются страницы, посещенные во время последних сеансов работы.

Для очистки промежуточной памяти:

В Netscape открыть меню *Edit* и выбрать опцию *Preferences*. Далее выбрать из открывшегося списка категорий *Advanced* и затем *Cache*. В зависимости от версии программы следует нажать клавишу *Clear Memory Cache*, *Clear Disk Cache*, *Clear* или *Clear Cache*.

В Internet Explorer следует в зависимости от версии из меню *View* или *Tools* выбрать опцию *Internet Options*. Далее найти категорию *Temporary Internet Files* и нажать клавишу *Delete Files*.

Выход из интернет банка

По завершении работы необходимо выйти из интернет банка, нажав соответствующую ссылку, и затем обязательно закрыть окно браузера. Ни в коем случае нельзя отходить от компьютера, будучи в среде интернет банка и оставив при этом компьютер открытым.

Имя пользователя и пароль при использовании интернет-банка

Имя пользователя и основной пароль

При заключении договора об использовании интернет-банка Вам выдается имя пользователя и основной пароль. Основной пароль выдается в защищенном конверте или предоставляется возможность задать пароль прямо при заключении договора. Никто, кроме Вас, не должен его знать. При первом вхождении в интернет-банк желательно изменить основной пароль и в дальнейшем пароль следует регулярно менять. Крайне нежелательно использовать основной пароль интернет-банка в качестве пароля или в каком-либо ином качестве в других системах. Пароль нельзя сообщать кому бы то ни было.

Кодовая карта

В дополнение к имени пользователя и основному паролю для использования интернет-банка необходима, как правило, кодовая карта. Если кодовая карта используется уже длительное время, желательно обменять ее в конторе банка на новую.

Защитные элементы, используемые для входа в интернет-банк (имя пользователя, основной пароль, кодовая карта), нельзя передавать кому бы то ни было, в том числе членам Вашей семьи. При желании членам семьи можно дать доступ к Вашему личному счету и получить для них в банке персональные элементы защиты.

Основной пароль и имя пользователя нельзя записывать на кодовой карте или хранить их на бумаге вместе с кодовой картой.

ID-карта и PIN-калькулятор

Пользователи, которые желают использовать интернет-банк посредством более защищенных методов аутентификации, могут использовать вместо кодовой карты ID-карту или PIN-калькулятор.

ID-карта первое в Эстонии удостоверение личности, при помощи которого можно удостоверить свою личность и через электронные каналы. Если банк предоставил такую возможность, то ID-карту можно использовать при вхождении в интернет-банк вместо кодовой карты. Для использования ID-карты необходимо приобрести считывающее устройство и наладить соответствующим образом компьютер. Карту следует ввести в считывающее устройство до начала использования интернет услуг, и карта должна оставаться в устройстве в течение всего времени пребывания в интернет-банке. После выхода из интернет-банка следует закрыть все окна браузера и изъять карту из считывающего устройства. Отходить от компьютера оставив ID-карту в считывающем устройстве нельзя.

Более подробную информацию об использовании ID-карты и наладке компьютера можно найти по адресу:

www.pass.ee

www.id.ee

PIN-калькулятор это электронное устройство, которое генерирует изменяющиеся во времени коды. Образованные коды можно использовать для вхождения в интернет-банк только в течение определенного времени, по истечении которого код теряет действительность. При получении в банке PIN-калькулятора он защищен первичным PIN-кодом, который следует сменить при первой возможности. В качестве нового PIN-кода следует выбрать тяжелоугадываемую для посторонних лиц комбинацию цифр. PIN-код следует запомнить. PIN-код нельзя ни в коем случае хранить в записанном виде в одном месте с PIN-калькулятором.

Лимиты

Обычно в договоре об использовании банковских интернет услуг предусмотрены стандартные дневные и месячные лимиты. Если предусмотренные лимиты слишком велики по сравнению с Вашими ежедневными операциями, желательно заменить стандартные лимиты на более подходящие. При необходимости лимиты всегда можно увеличить, в тоже время сравнительно небольшие лимиты существенно снижают возможный ущерб от злоумышленной деятельности.

Если без использования больших лимитов не обойтись, желательно использовать более защищенные методы аутентификации, такие как ID-карта и PIN-калькулятор.

Блокирование банковских интернет услуг

Если у Вас возникло подозрение, что Ваш пароль или коды кодовой карточки стали известны посторонним лицам, или же потеряны, свяжитесь немедленно с Вашим банком по телефону и приостановите договор об использовании банковских интернет-услуг. Все банки в Эстонии предоставляют возможность блокирования интернет-услуги круглосуточно. Для восстановления интернет-услуг необходимо обратиться в банк, где будут выданы новый основной пароль и кодовая карта.

На интернет-страницах банков публикуются всевозможные рекомендации по повышению защиты услуг интернет-банка для пользователей. Там же приведены контактные данные банков.

■ AS Hansapank

Телефон обслуживания клиентов: 6310 310; www.hanza.net

■ AS Eesti Ühispank

Тел.: 6655 100; www.eyp.ee

■ AS Sampo Pank

Тел.: 6800 800; www.sampo.ee

■ AS Eesti Krediidipank

Блокирование банковских карточек и интернет-банка: 6616 039; 08004 050; www.krediidipank.ee

■ Nordea Bank Finland Plc Eesti filiaal

Блокирование интернет банка: 6283 283; www.nordea.ee

■ Tallinna Äripanga AS

Тел.: 6 688 040; 6688 000; www.tbb.ee

* Финансовая инспекция не берет на себя обязательств по обновлению приведенной в настоящем материале информации либо по сообщению о введенных в нее изменениях. Приведенная в настоящем материале информация не может рассматриваться как дача информации или высказывание мнения по конкретному имущественному вопросу. По конкретному имущественному вопросу мы рекомендуем проконсультироваться с соответствующими специалистами.

