trešdiena, 2018. gada 15. augustā 10:25

Рекомендации по защите компьютера

1. **Для работы с интернет банком рекомендуется обезопасить компьютер или мобильное устройство, с которого происходит работа, антивирусными программами.** В случае если установлен антивирус то необходимо производить обновление антивируса.

Также рекомендуется установка программ брандмауэров (firewall) и/или имеющиеся в наличии другие аппаратные средства, такие как - система по предотвращению проникновения вредоносного кода, система контроля доступа к конфиденциальной информации и т.д (IPS/IDS, DLP).

Брандмауэр (firewall) — программа для защиты компьютера от атак и несанкционированного доступа по сети.

IPS - программная или аппаратная система сетевой и компьютерной безопасности, ***обнаруживающая вторжения или нарушения безопасности и автоматически защищающая*** от них.
IDS - программное или аппаратное средство, предназначенное ***для выявления фактов*** неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.
DLP - ***технологии предотвращения утечек конфиденциальной информации*** из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.
Полезные ресурсы:

- http://www.esidross.lv/ - информационный портал безопасности.
- http://windows.microsoft.com/lv-lv/windows/security-essentials-download — антивирус Microsoft
- http://www.antivirus.lv/ - антивирус Касперского
- https://www.avira.com — антивирус Avira
- http://avg.com – антивирус AVG
- https://www.virustotal.com — бесплатная on-line проверка на вирусы
- http://secunia.com/ - аудит безопасности компьютера
- http://www.zonealarm.com/ - антивирус, брандмауэр (firewall)
- www.zemana.com – антикейлогер, для борьбы с программами-шпионами
- www.malwarebytes.org — программа для обнаружения и удаления вредоносных программ

2. Защита компьютера или мобильного устройства при помощи пароля. В случае если вам необходимо оставить компьютер без присмотра, то необходимо пользоваться парольной защитой экрана. На компьютерах с операционной системой Windows, обычно блокировка экрана происходит при помощи нажатий клавиш Win (кнопка с изображением Windows logo, между Alt и Ctrl) +L.

3. На устройстве с которого происходит работа в интернет банке необходимо регулярно обновлять программное обеспечение — операционную систему, браузер,

антивирусное программное обеспечение.

4. Ограничить доступ третьих лиц к устройству с которого происходит работа в интернет банке. Не рекомендуется использовать публично доступные устройства — такие как компьютеры в интернет кафе, гостиницах, библиотеках. В случае если вам все-таки пришлось воспользоваться публично доступном компьютером то по завершению работы в интернет банке необходимо выйти, нажав кнопку «Выход», и закрыть окно интернет браузера.

5. Используйте возможность разделение прав пользователя на компьютере

Разделение прав пользователей на компьютере позволяет пользователю, работающему с правами администратора разрешать/запрещать использование программ и ресурсов компьютера. Для повседневной работы не рекомендуется использовать пользователя с правами администратора, так как данный пользователь имеет полный доступ к ресурсам компьютера — установка программ (в том числе и вредноносных), удаление программ (в том числе и антивирусные программы), отключение программ (антивирусы, брандмауэр), доступ к данным других пользователей компьютера. Для повседневной работы рекомендуем использовать пользователя с ограниченными правами доступа — запрещена установка программ, запрещена возможность отключения антивируса. В случае если необходимо установить какую-либо программу можно переключится на пользователя с правами администратора.

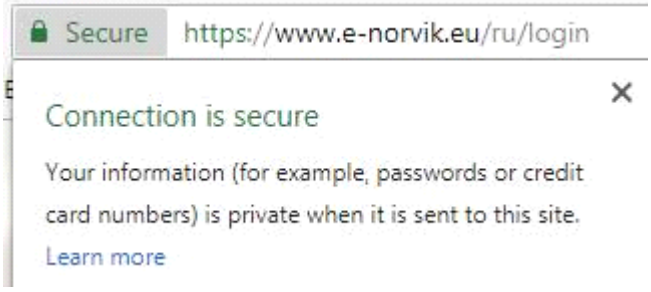
Рекомендации по безопасной работе в интернет-банке

Безопасная работа с интернет банком является обоюдной ответственностью, которая обеспечивает с одной стороны *Norvik Banka*, с другой — пользователь интернет банка.

Только совместно можно обеспечить наивысший уровень безопасности!
Помните, что банк никогда не запрашивает данные для авторизации в интернет банке по электронной почте, телефону или любым иным способом. Никому не сообщайте пароль от интернет банка, коды идификационных устройств. В случае если к вашей карте кодов, кодовому калькулятору, мобильному устройству (авторизация SMS-Пин) получили доступ третьи лица или у вас возникли подозрения в угрозе безопасности, необходимо незамедлительно обратиться в службу безопасности банка (+371) 6704 1100.

Наши советы, чтобы Ваша работа в Интернет-банке была безопасной:

1. При работе с интернет банком необходимо убедиться, что сертификат подлинности (SSL) действителен. У действительного сертификат часть адреса https в адресной строке должна отображаться зеленым цветом.



Так же название в адресной строке должно соответствовать набранному вами адресу — www.e-norvik.eu.

В сертификате подлинности в поле «Выдано для» (Issued to:) должно быть значение www.e-norvik.eu, в поле «Выдано кем» (Issued by:) указанно значение thawte Extended Validation SSL CA.

Сертификат подлинности (SSL) так же обеспечивает шифрованное соединение между клиентом и интернет банком.

В случае если часть адреса https: отображается красным цветом или в браузере появилась ошибка SSL сертификата, это означает возможную угрозу безопасного соединения. В таком случае необходимо обратиться в службу безопасности банка (+371) 6704 1100.

2. Рекомендуем регулярно контролировать историю банковских платежей и остатки счетов. Используйте возможность контроля операций в интернет банке при помощи SMS сообщений.

3. Для входа в интернет банк используйте сложные пароли от 8 до 16 символов. В пароле должны содержаться строчные и заглавные символы, цифры, спецсимволы. Не используйте в пароле легко угадываемые значения, такие как ФИО, номер машины, клички животных, название городов, дату рождения, регистрационный номер предприятия и др. Не записывайте ваш пароль на бумаге или карточке кодов. При смене пароля не используйте предыдущий пароль в качестве нового. В случае если у вас возникли подозрения что ваш пароль могли похитить, необходимо связаться со службой безопасности банка (+371) 6704 1100, так же необходимо сменить пароль, осуществлять смену пароля желательно с другого компьютера или устройства.

4. По завершению работы в интернет банке необходимо нажать клавишу «Выход». И закрыть браузер. В случае если вам пришлось воспользоваться публично доступным компьютером, то тогда необходимо очистить кеш и историю браузера, удалить файлы выписки по счету или других файлов загруженных из интернет-банка.

Основные угрозы при работе пользователя с интернет-банком

1. **Фальшивые письма, звонки**

   Самым популярным считается «phishing» – рассылка ложных писем или звонки от имени банка с просьбой сообщить авторизационные данные. Так же злоумышленники пытаются получить данные кредитных карт (номер карты, CCV2, PIN код, срок действия карты) или персональные данные клиента. В фальшивых письмах злоумышленники могут копировать корпоративный стиль банка.

2. **Фальшивые сайты**

   Не редко в поддельных письмах используются ссылки с предложение авторизоваться в интернет банке или получить дополнительную информацию, эти ссылки перенаправляют пользователя на фальшивые сайты похожие на сайт интернет банка, при помощи которых злоумышленники пытаются получить доступ к авторизационным данным пользователя. На фальшивых сайтах могут содержаться вредоносные программы для инфицирования компьютера пользователя вирусом или шпионской программой.

3. **Фальшивый сертификат подлинности**

Фальшивые сертификаты подлинности (SSL/https) используются злоумышленниками для нарушения шифрованного канала передачи данных или перенаправления пользователя на фальшивые сайты. В случае если пользователь согласился использовать не доверенный сертификат, злоумышленник может не только перехватить и расшифровать данные отсылаемые пользователем, но и изменять эти данные. При работе с интернет банком необходимо убедиться, что сертификат подлинности настоящий.

В случаях получения писем, звонков с просьбой сообщить реквизиты для работа с интернет банком необходимо немедленно сообщить об этом в службу безопасности банка (+371) 6704 1100.