


Рекомендации по безопасному использованию банковских и иных он-лайн сервисов

Рекомендации по безопасному использованию банковских и иных on-line сервисов и услуг (интернет-банкинг, электронные платежные системы, сервисы электронной коммерции и т.п.)

1. При самом первом использовании on-line сервиса необходимо с клавиатуры ввести в адресной строке Вашего браузера адрес web-страницы on-line сервиса. При дальнейшем использовании Вы можете добавить данную web-страницу в "Избранное" Вашего браузера.
2. Убедитесь, что после ввода адреса в браузер и загрузки страницы, в строке состояния появился значок замка , а в адресной строке присутствует «https». Это означает, что Ваше соединение с on-line сервисом защищено (SSL).
3. Убедитесь, что после загрузки web-страницы в адресной строке появилось "https:", а в строке состояния браузера появился значок замка.
4. Для авторизации в системе on-line сервиса не рекомендуется использовать пароли, которые также используются Вами для авторизации на других интернет-сайтах (особенно развлекательного плана).
5. Не используйте компьютеры общего пользования (интернет-кафе, компьютеры библиотек и т.п.).

Рекомендации по парольной защите

1. Храните Ваш пароль в секрете и не сообщайте его третьим лицам.
2. Запомните Ваш пароль. Не храните пароль в легкодоступном месте. Не храните пароль на компьютере.
3. При формировании пароля используйте большие и маленькие буквы, а также цифры и специальные символы.
4. Избегайте простых паролей. Не используйте распространенные и легко угадываемые слова в качестве пароля. Постарайтесь придумать фразы, легко запоминающиеся для Вас, но не для других.
5. Избегайте коротких паролей. Помните, длина пароля, должна составлять не менее 8 символов.
6. Регулярно изменяйте свой пароль (старайтесь не реже, чем раз в 90 дней).
7. Помните, что ни сотрудник банка, ни иной организации не вправе требовать от Вас сообщить пароль.
8. Если у Вас возникли подозрения в компрометации пароля, немедленно смените его.

Рекомендации по обеспечению безопасности при работе в сети Интернет

1. Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить Ваш браузер на автоматическую блокировку таких окон.
2. Не оставляйте свои персональные данные в блогах, форумах и социальных сетях.
3. Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.
4. При совершении покупок через Интернет, прежде чем ввести данные о своей кредитной карте, убедитесь, что Ваше соединение защищено: после загрузки страницы, в строке состояния появился значок замка, а в адресной строке присутствует «https».
5. Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.
6. Регулярно проверяйте Ваш компьютер на вирусы, как минимум раз в неделю.
7. Не добавляйте персональную информацию в личные страницы в социальных сетях. Это может привлечь внимание злоумышленников.

Рекомендации по обеспечению безопасности электронной почты

1. Не открывайте письма от незнакомых людей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены, что письмо пришло из надежного источника не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы.
2. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл, который имеет файловое расширение ".exe".
3. Не отправляйте свою персональную информацию по почте. Убедитесь в надежности web-сайта перед тем, как оставить на нем адрес электронной почты.
4. Немедленно удалите свой адрес электронной почты с неизвестных сайтов. Используйте спам-фильтр в почтовых клиентах.
5. Не пересылайте т.н. «письма счастья».

Рекомендации по использованию сервисов мгновенных сообщений

1. Заблокируйте в своем списке контактов, людей, которых Вы не знаете, особенно, если они ведут себя необычно. Настройте Ваш клиент мгновенных сообщений таким образом, чтобы только друзья из списка контактов могли писать вам.
2. Не отвечайте незнакомым людям, особенно если их сообщения содержат угрозу или Вас донимают.
3. Не нажимайте на присланные ссылки и не открывайте приложения. Они могут содержать вирусы или шпионское ПО.

Рекомендации по настройке компьютера

1. Старайтесь использовать современные операционные системы. Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий.
2. Своевременно скачивайте и устанавливайте патчи и обновления для операционных систем (ОС). Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.
3. Используйте в работе лицензионное ПО; не загружайте и не устанавливайте ПО полученное из непроверенных источников.
4. Отключите общий доступ к принтерам и файлам на Вашем компьютере, чтобы предотвратить несанкционированные подключения.
5. Используйте широкоизвестные браузеры и вовремя устанавливайте для них обновления.
6. Настройте в Вашем браузере блокировку всплывающих окон.
7. Выключайте компьютер, подключенный к сети Интернет, если не используете его в течение длительного времени.

Рекомендации по использованию средств защиты ПК

1. Использование антивирусного программного обеспечения является обязательным. Обеспечьте своевременное обновление антивирусных баз. Также настоятельно рекомендуется использовать антишпионское программное обеспечение.
2. Для защиты компьютера от угроз из сети Интернет используйте встроенный в операционную систему фаервол (firewall) или установите лицензионный.
3. Блокируйте компьютер, если Вам надо от него отойти.
4. Используйте специализированное ПО для шифрования важных данных на ноутбуках, КПК, телефонах и других переносных устройствах.