

Интернет - остров сокровищ? | Internet - l'île au trésor?

Author: Ольга Юркина, [Женева](#) , 06.05.2009.



О чем кредитная карточка может рассказать Интернету? (© Keystone)

Системы дистанционного банковского обслуживания практичны и удобны в использовании, но не защищены от компьютерных пиратов.

| Bien qu'étant pratiques et dits "sécurisés", les systèmes de paiement online ne sont pas à l'abri d'un piratage informatique.

Internet - l'île au trésor?

Швейцарский Центр регистрации и анализа для защиты информационных данных (MELANI) опубликовал очередной отчет о том, как не безопасен Интернет, и что с этим делать. Особенно уязвимы, по мнению MELANI, системы дистанционного банковского обслуживания, или Интернет-бэнкинг. Во второй половине 2008 года количество нападений на программы «e-banking» увеличилось вдвое: слишком уж соблазнительной представляется компьютерным пиратам возможность «перехватить» секретные коды во время открытия Интернет-сессии банковскими клиентами.

Существует несколько пиратских «приемов». Один из них – распространение вредоносного программного обеспечения, которое компьютер перекачивает автоматически и незаметно для пользователя во время открытия сессии. После чего «малварь» (от английского malware, жаргонное слово, обозначающее вирусную

программу) без проблем добывает для злоумышленников необходимую информацию и открывает им доступ к банковским счетам незадачливого пользователя. Печально известный «Троянский конь», специализирующийся на добыче информации, распространяется либо через спам, либо через зараженные сайты. При этом пользователи даже не отдают себе отчета в том, что система перекачивает вредную программу.

Эксперты MELANI предостерегают и от «фишинга». «Фишинговые» электронные письма заманивают пользователей на сайты, специально сконструированные кибер-пиратами для выуживания конфиденциальных данных – паролей и кодов доступа. Нередко подобные сайты в деталях воспроизводят интерфейс официального сайта банка, клиентом которого является жертва. Иногда мошенникам удается пробраться даже в официальные банковские системы и разослать электронные письма с поддельным адресом отправителя. Такие письма открывать не рекомендуется. Впрочем, администрация банков обычно реагирует оперативно и отправляет клиентам предупреждение не открывать то или иное письмо.

Тревогу у швейцарских экспертов вызывают и внешние носители – флеш-карточки и ключи USB, на которые могут содержать замаскированную вредоносную программу, автоматически копируемую информационной системой.

Чтобы предостеречь пользователей, пустившихся в свободное плавание по Интернету, от грозящих им опасностей и «подводных рифов», эксперты MELANI предлагают список полезных советов.

Перед тем, как открыть банковскую Интернет-сессию:

- все время открывать сессию «e-banking» в новом окне, закрыв все остальные окна и сайты на время сессии;
- никогда не переходить на сайт дистанционного банковского обслуживания по ссылкам, указанным в электронных письмах или на любых других сайтах;
- каждый раз полностью набирать адрес банка от руки, не переходя на него по ссылкам;
- регулярно менять пароли;
- никому не сообщать Ваш личный пароль и код доступа к счетам;
- не доверять электронным письмам «от банка» с просьбой ввести Ваши идентификационные данные, не проверив предварительно эту информацию по телефону;
- каждый раз закрывать банковскую сессию в специальном окне «Закреть сессию», а не ограничиваться закрытием главного окна или Интернета;
- перед тем, как открыть сессию, удостовериться с помощью сертификата, что Вы находитесь на официальном сайте банка и все данные передаются в зашифрованном виде.

В принципе, для безопасности Вашего компьютера следует:

- регулярно обновлять информационную систему и версии программ;
- установить антивирусное программное обеспечение и сигнал тревоги;
- не доверять неизвестным провайдерам и подозрительным предложениям перекачать ту или иную программу;
- не открывать подозрительные электронные письма и вложенные в них файлы.

[Официальный сайт MELANI](#)

Статьи по теме:

[Деньги утекают со скоростью света](#)

[Швейцария](#)

Source URL: *<http://www.nashagazeta.ch/news/economie/internet-ostrov-sokrovishch>*