Совсем недавно в одном из киевских ресторанов был обнаружен официант-мошенник - когда клиент отдавал ему карточку, чтобы рассчитаться, он записывал все реквизиты кредитки, а затем продавал эти данные другим мошенникам в интернете. Более изощренную схему использовали жулики в другом киевском ресторане - с помощью видеокамеры, установленной над местом для расчетов, они записывали происходящее, таким образом получая конфиденциальную информацию.

А ведь рассчитываться за товары и услуги с помощью банковской карточки и интернета в нашей стране становится все популярнее. Каждый год количество таких продвинутых пользователей возрастает на 70%. По данным НБУ, за первый квартал текущего года в Украине было проведено 24 миллиона безналичных операций по платежным картам украинских банков. Онлайн-расчеты приобретают все большую популярность не только в столице, но и в регионах: за прошлый год доля региональных пользователей таких услуг увеличилась на 8%.

Однако не спят и мошенники: даже если вы желаете просто пополнить свой мобильный счет на десяток гривен, можно поплатиться всей суммой, которая есть у вас на банковской карточке. Но это не значит, что нужно отказаться от удобства, не выходя из дому, мгновенно оплачивать необходимые счета или делать покупки. Просто, уверяют эксперты, необходимо понимать существующие риски и принимать меры для защиты своей финансовой информации. Система онлайн-платежей не гарантирует вам полной безопасности. Необходимо соблюдать правила безопасного пользования платежными картами и применять технические методы защиты от интернет-мошенничества, такие, как настройки безопасности в браузере и обновленный антивирус.

«В мире системы онлайн-расчетов прошли нелегкий путь развития и наработки методов борьбы с мошенничеством, и Украина сейчас имеет значительное преимущество - использование опыта европейских коллег для максимальной защиты пользователей. Поэтому со стороны банков, платежных систем, авторизованных сайтов системы оплаты защищены. Большинство случаев мошенничества в Украине вызваны недостаточной осведомленностью пользователей с базовыми правилами пользования платежными картами», - отмечает директор системы экспресс-платежей Portmone.com Игорь Горин.

ВИДЫ МОШЕННИЧЕСТВА, КОТОРЫХ СТОИТ ОПАСАТЬСЯ

Наиболее распространенным видом мошенничества в украинском интернете является «фишинг» - маскировка сайта под известную платежную систему или банк с целью получения данных пользователя.

Например, на адрес пользователя поступает письмо якобы от платежной системы, в котором сообщается, что электронный счет заблокирован. Для «разблокирования» клиент вводит свои персональные пароли, не отличая сайт-двойник от настоящего.

А если на вашем компьютере не обновляется операционная система или антивирус - вы первый кандидат на заражение относительно новым видом вредоносных программ - кейлоггерами. Это такие программы или физические устройства, регистрирующее нажатие клавиш на клавиатуре. Кейлоггеры перехватывают данные, которые вводятся при регистрации на сайте или, например, при осуществлении платежей. Затем они отсылаются мошенникам.

Современный пользователь электронной почты со спамом очень часто получает еще так называемые письма счастья с просьбой переслать сообщение по контакт-листу. Мошенники научились пользоваться технологиями социальной инженерии, и часто такие письма содержат просьбу зайти на подозрительный сайт, намеренный выудить личную информацию. Особую опасность представляют так называемые нигерийские письма, названные так потому, что основное распространение такое мошенничество получило в Нигерии. Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты от сумм. После согласия пользователя у него постепенно выманиваются деньги якобы на оформление операций по оформлению сделок. В последнее время такой вид мошенничества был модернизирован и адаптирован для выуживания банковских данных.

Участились и так называемые телефонные случаи мошенничества с международными платежными картами. Выудив номер телефона из открытых источников или у нерадивых работников мобильных операторов либо их дилеров, мошенники звонят на мобильный телефон потенциальной жертвы. С целью получения персональных данных держателя, а также реквизитов самой платежной карты, злоумышленники представляются сотрудниками одного из крупных банков. После подтверждения фамилии, имени и отчества клиента мошенники пытаются под тем или иным предлогом узнать паспортные данные, номер самой карты, PIN-код и код безопасности.

Эксперты напоминают, что сотрудники банка никогда не совершают такого рода звонков, а банк не рассылает электронные письма и SMS-сообщения клиентам - держателям карт банка - с просьбой подтвердить номер платежной карты или другие персональные идентификаторы.

ПРАВИЛА БЕЗОПАСНОСТИ

Для освоения правил безопасности онлайн-платежей украинским пользователям необходимо:

- убедиться, что сайт защищен (в адресной строке браузера адрес обязательно должен начинаться с https:// и в окне браузера появляется значок «закрытый замочек»);

- никогда не вводите PIN-код платежной карты в интернете. На безопасных сайтах он никогда не используется;

- существуют вирусы, которые при заходе на сайт просят сообщить данные карты. Никогда не вводите данные в таком случае;

- убедитесь, что сайт не запоминает ваш пароль при входе в секцию для зарегистрированных пользователей;

- убедитесь, что адрес сайта и название сервиса совпадают;

- перед тем, как вводить данные своей платежной карты, прочитайте условия предоставления сервиса;

- если вы производите оплаты с публичного компьютера, включите режим «приватного просмотра» в браузере;

- используйте обновленную лицензионную операционную систему и обновленное антивирусное программное обеспечение для защиты от вирусов.

Источник: http://smi.liga.net