Осторожно мошенники!!!
Не дай себя обмануть!!!

Как и все остальные виды обмана, мошенничество через интернет очень развито. Тем более многие люди просто не умеют пользоваться интернетом и не знают элементарных правил безопасности в сети. Чаще всего целью мошенников являются данные кредитных карт и платежных паролей. Ведь именно с их помощью можно завладеть деньгами незадачливого пользователя.

Следовательно, необходимо уделить наибольшее внимание именно безопасности компьютера и надежности сайта, на котором вы вводите свои данные.

— Так, к примеру, для кражи паролей мошенники очень часть используют keylogger, программу, записывающую все нажатые вами комбинации клавиш и передающие эту информацию мошенникам.

— Другой способ заключается в создании точной копии сайта банка или интернет-магазина. Пользователь, не заметивший подвоха, ведет свои данные, и они будут переданы напрямую мошенники, которые смогут их использовать уже на свое усмотрение. Так, к примеру, если вы введете свой логин и пароль на поддельном сайте интернет-банка, то мошенники получат доступ к вашему счету в банке и смогут перевести все ваши деньги на свой счет. А в поддельном интернет-магазине при оплате покупки вы укажете все данные вашей кредитной карты, после чего мошенник сможет использовать их для перевода денег с вашей карты на свой счет, либо оплате своих товаров по реквизитам вашей банковской карты.

Опознать такие сайты достаточно просто - отсутствие внятной информации и необъяснимая дешевизна товаров в интеренет-магазине, сложный адрес сайта, совершенно не похожий на адрес вашего интернет банка и отсутствие защитной зоны https:// перед адресом. Также подобные сайты могут заражать компьютер пользователя вредоносной программой, которая на этапе ввода платежной информации подменяет реальный сайт на поддельный.

— Также довольно распространено такое мошенничество через интернет,

когда злоумышленники представляются сотрудниками банка или сотового оператора, и под убедительными предлогами получают ваши конфиденциальные данные: пароли, пин-коды или коды CVV2/CVC2

банковских карт.

Вот простой набор правил, используя которые вы сможете в большей степени обезопаситься от перечисленных видов мошенничества:

1) Установите на свой компьютер антивирус с регулярными обновлениями. Так, к примеру, у Антивируса Касперского есть специальная технология “Безопасные платежи” позволяющая обеспечить защиту при пользовании системами интернет-банков и при совершении покупок в интернете.

2) Не стоит пользоваться чужим компьютером. Вы досконально не знаете, как относиться его владелец к вопросам безопасности. Вдруг его компьютер

заражен вирусами? Бывали случаи, когда даже администраторы в интернет- кафе оказывались мошенниками, и собирали логины/пароли своих посетителей.

3) При входе на сайт внимательно проверяйте адресную строку браузера. Адрес сайта должен в точности, до последнего дефиса совпадать с реальным адресом интернет магазина или интернет-банка. Помните, что даже один неверный символ в адресе сайта означает, что вы попали на совершенно другой сайт, возможно поддельный, созданный специально для мошеннических действий. Так же как я упоминал выше, адреса подобных сайтов должны начинаться с https://, а всю финансово значимую информацию браузеры при этом отмечают значками замков слева или справа от адреса сайта.

4) Не сообщайте никому платежные реквизиты своей карты. Не пересылайте реквизиты по электронной почте. И не оставляйте данные в открытом виде в тех местах где их могут подглядеть мошенники. К примеру, если вы пользуетесь бумажным блокнотом для запоминания логинов и паролей, то храните этот блокнот подальше от чужих глаз.

5) Ни в коем случае не ведитесь на звонки из мнимых банков о кредитах, которых вы не брали или SMS о том, что ваша карта заблокирована! Смело звоните в ваш банк по номеру, указанному на обратной стороне карты либо в договоре с банком. Никогда не перезванивайте на номера банков указанных в SMS! Возможно, это поддельные номера и вы попадете вместо банка к мошеннику, который постарается выведать у вас необходимую ему информацию.

6) Заведите отдельную карту для оплаты в интернете карты. Не “светите” свою зарплатную карту на сайтах интернет-магазинов. Так как не исключены случаи взлома баз интернет-магазинов с целью кражи информации. Не стоит рисковать всеми имеющимися у вас деньгами. Для отдельной карты подойдет как стандартная дебетовая, так и виртуальная карта без физического носителя. Можно даже создавать для каждой покупки новую виртуальную карту, а сразу после этого закрыть ее. Многие банки позволяют это делать на чисто символическую плату.

7) Если на карте, которой вы расплачиваетесь в интернете, хранятся крупные суммы, то установите дневной или разовый лимит по расходованию средств. Таким образом, мошенник, даже завладев данными вашей карты, не сможет вывести сразу все деньги. Особенно это актуально для кредитных карт. На них обычно имеются довольно крупные суммы готовые к списанию.

8) Обязательно подключите услугу информирования по SMS об операциях с вашей картой. Если вы получите информацию о списании, которое не делали, то всегда сможете быстро заблокировать карту.

Таким образом, используя эти достаточно простые рекомендации, вы обезопасите себя и свои деньги от кражи. Не пренебрегайте безопасностью ваших денег!

Отдел Министерства внутренних дел
Российской Федерации по городу Пыть-Ях