Интернет мошенничество с кредитными картами

Интернет-мошенничество и хищение данных кредитной карты. Интернет-мошенничество может осуществляться с помощью фальшивых электронных писем, в которые включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом будет использована с ущербом для пользователя. Поэтому, посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта и не пользоваться ссылкой, содержащейся в подозрительном электронном письме.

И до России потихоньку доходит волна осуществления афер через интернет, а также считывания информации о данных с пластиковых кредитных карт. Если быть достаточно проинформированным в этом вопросе можно избежать многих проблем.

С помощью интернета чаще всего мошенники используют так называемую технику «phishing», заключается она в том, что на ваш электронный адрес приходит письмо с ссылкой на популярный сайт, но на самом деле это копия сайта специально сделанного мошенниками для того, чтобы обманным путем узнать ваши личные данные.

Обманным путем они узнают пароли, номера кредитных карт, пин коды, которые в последующем используют в собственных корыстных целях.

К сожалению, интернет магазины и интернет в целом это не единственная лазейка для хакеров. Банкоматы, телефоны, даже супермаркет, в котором вы или ваш ребенок расплачиваетесь через терминал кредитной картой, они тоже представляют угрозу. Прежде чем принять у вас оплату, любое учреждение должно проверить ваши данные через сервер, на котором они находятся. Однако некоторые хакеры способны такие сервера взламывать.

Как не попасться.

1. Переходя с веб-сайта на другой веб-сайт, лучше набирать названия самому, не пользуясь автоматической подсказкой, или пользоваться меню «избранное».
2. Не открывать даже сомнительные письма, спамы.
3. Если вдруг вы или ваш ребенок предоставили вашу личную информацию ненастоящим работникам сайта, об этом нужно сразу же сообщить действительным его сотрудникам.

Если быстро среагировать, есть возможность свести нанесенный ущерб к минимуму.

4. Всегда следите за состоянием баланса на ваших кредитных и лицевых счетах. Это сейчас очень просто с услугой SMS информирования при изменении количества денежных средств на ней. Такой сервис есть во многих банках России.

Что делать в случае кражи.

Если вы подозреваете, что ваши личные данные украдены, немедленно принимайте меры:

Измените пароли.

Поставьте в известность отдел обслуживания клиентов соответствующих организаций.

Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.

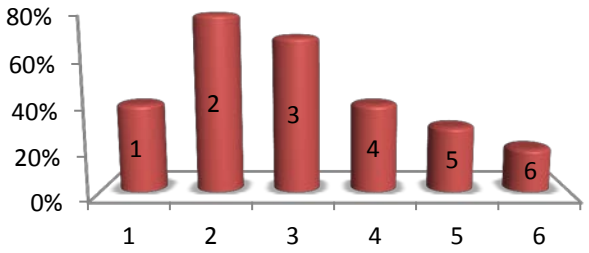
Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

Записывайте и сохраняйте абсолютно все.

После выполнения всех действий всегда делайте копии документов.

Многие дети гораздо лучше владеют компьютером, чем их родители. Однако, им они по-прежнему нуждаются в советах и защите при использовании интернета и мобильных технологий.

ДЕТИ И ИНТЕРНЕТ



1.Более 40% детей сталкиваются с сексуальными изображениями в интернете.

2.80% школьников имеют аккаунты в социальных сетях.

3.70% в своих аккаунтах указывают свою фамилию, точный возраст и номер школы.

4.40% российских детей готовы продолжить он-лайн общение в реальной жизни.

5.У 30% школьников данные аккаунта открыты всему миру.

6.Более 20% детей становятся жертвами нападок со стороны сверстников.

7.Младшие школьники сталкиваются с сексуальными изображениями реже, чем старшие, но испытывают больший стресс.

8.Прилежные дети в 2 раза чаще попадают на «плохие» сайты в силу природной любознательности.

ВНИМАНИЕ!!!

• **Никогда** не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

• **Используйте** нейтральное экранное имя, не содержащее непристойных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

• **Выключите** компьютер, если вас что-то пугает в его работе. Расскажите об этом родителям или другим взрослым.

• **Всегда** сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

• **Используйте** фильтры электронной почты для блокирования спама и нежелательных сообщений.

• **Никогда** не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

• **Прекращайте** любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие непристойные намеки.

Расскажите об этом родителям!

Автор-составитель: Канахнова Г. Б.

МБОУ ДОД Дом детского творчества
Первомайского района г. Ижевск

Руководство интернет-безопасности для родителей

В ногу с детьми в интернете

Интернет мошенничество с кредитными картами