МБУК Тогучинского района «Тогучинская ЦБС»

МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ



Семеновская сельская библиотека

Проблемы информационной безопасности

Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

В отличие от таких интернет-угроз, как вирусы, троянские программы, программы-шпионы, SMS-блокеры, спам и т.д., мошенничество примечательно вот чем: мишень злоумышленника — не компьютер, защиту которого надо обойти, а человек, у которого, как известно, свои слабости. Поэтому, с одной стороны, ни одна программа не обезопасит пользователя полностью, а с другой — он в значительной мере отвечает за свою безопасность сам.

Виды мошенничества

- В целом, все те же старые схемы махинаций, преследовавшие потребителей и инвесторов в течение многих лет до создания Интернета, сейчас появляются в виртуальном пространстве (иногда им присуща определенная тонкость, вызванная Интернет-технологиями). При стремительном росте Интернета, в особенности электронной коммерции, виртуальные преступники стараются представить свои преступные схемы таким образом, чтобы они как можно более походили на товары и услуги, предлагаемые большинством добросовестных электронных торговцев. При этом они не только наносят ущерб потребителям и инвесторам, но и подрывают доверие потребителя к законной электронной коммерции и Интернету.
- *1) **Схемы проведения аукционов и розничной торговли в режиме он-лайн.** По данным Федеральной торговой комиссии и Общества по предотвращению мошенничества в Интернете, наиболее распространенным видом мошенничества в Интернете являются мошеннические предложения, фигурирующие на сайтах онлайновых аукционов.*
- *2)* **Деловые возможности / «надомная работа».** Мошенники часто используют Интернет для рекламы предполагаемых деловых возможностей, которые якобы позволят людям зарабатывать тысячи долларов в месяц при помощи «надомной работы»
- *3)* **Кража личных данных и мошенничество**. Некоторые махинации в Интернете также связаны с кражей личных данных – незаконным получением и мошенническим использованием чьих-то личных данных, обычно в экономических целях.

ФИШИНГ

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.



ИНТЕРНЕТ - ПОПРОШАЙНИСЧЕСТВО

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

МОШЕННИЧЕСТВО, СВЯЗАННЫЕ С ИНТЕРНЕМ МАГАЗИНАММИ

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.



Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

SMS – МОШЕНИЧЕСТВО В СПАМЕ

Письма, в которых под разными предлогами вас просят послать SMS-сообщение на короткий номер. Сюда же относятся и письма, содержащие ссылки на сайты, на которых в качестве платы за якобы предоставляемую услугу также предлагается послать SMS-сообщение на короткий номер. Что бы в таких письмах ни обещали мошенники, дело кончится тем, что вы заплатите за несуществующую услугу сумму не менее десяти долларов.



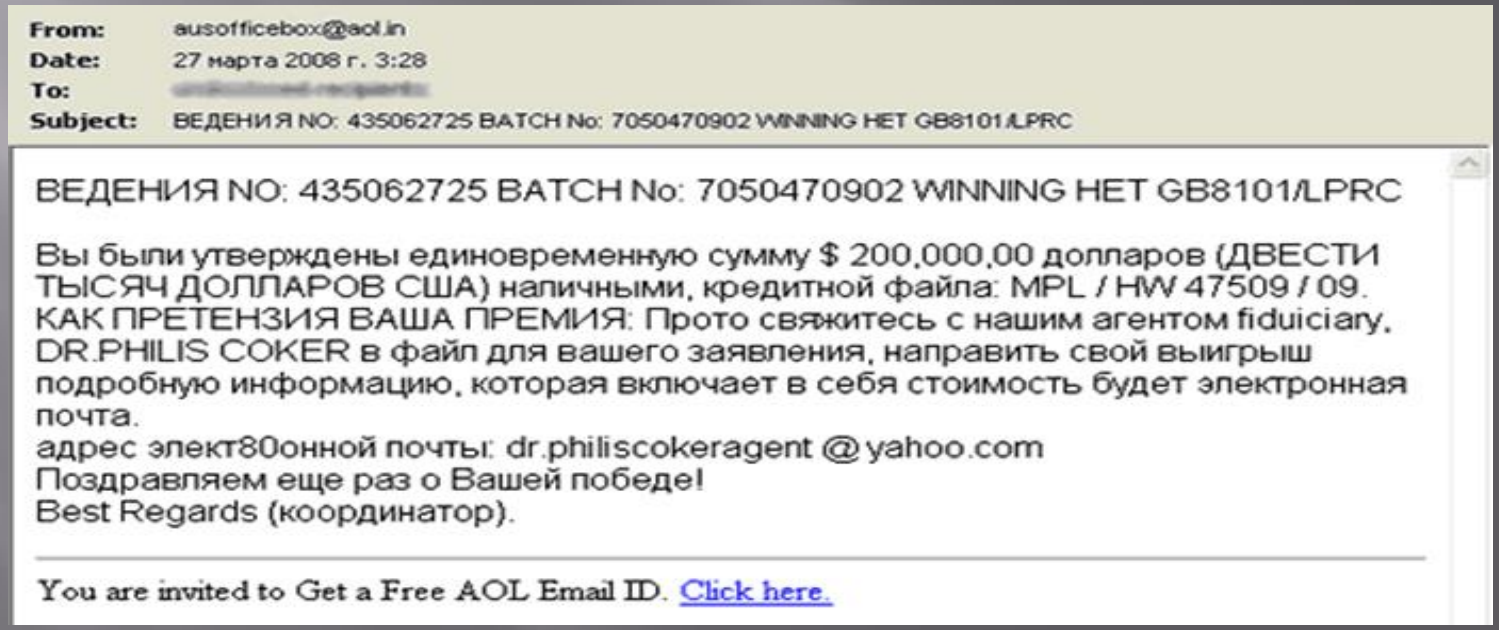
Код разблокировки: 55555

«ГОРЯЩИЕ» ПУТЕВКИ

Здесь мошенничество довольно элементарно - малоизвестные туристические фирмы, постоянно намекающие на "демпинговые" цены на высококлассные туры, на самом деле продают весьма дешевые пакеты услуг, которые совсем не соответствуют описаниям и фотографиям на сайте.

ПОДДЕЛЬНЫЕ УВЕДОМЛЕНИЯ О ВЫИГРЫШЕ В ЛОТЕРЕЮ

В письме сообщается о том, что вы якобы выиграли в лотерею. Цель мошенников — выманить у вас некоторое количество денег за «перевод» вашего денежного приза.



From: ausofficebox@aol.in
Date: 27 марта 2008 г. 3:28
To: [redacted]
Subject: ВЕДЕНИЯ NO: 435062725 BATCH No: 7050470902 WINNING HET GB8101/LPRC

ВЕДЕНИЯ NO: 435062725 BATCH No: 7050470902 WINNING HET GB8101/LPRC

Вы были утверждены единовременную сумму $ 200,000.00 долларов (ДВЕСТИ ТЫСЯЧ ДОЛЛАРОВ США) наличными, кредитной файла: MPL / HW 47509 / 09. КАК ПРЕТЕНЗИЯ ВАША ПРЕМИЯ: Прото свяжитесь с нашим агентом fiduciary, DR.PHILIS COKER в файл для вашего заявления, направить свой выигрыш подробную информацию, которая включает в себя стоимость будет электронная почта.
адрес элект80онной почты: dr.philiscokeragent @yahoo.com
Поздравляем еще раз о Вашей победе!
Best Regards (координатор).

You are invited to Get a Free AOL Email ID. Click here.

ОСТОРОЖНО!!! ВИРУС!!!

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

БОРЬБА С МОШЕНИЧЕСТВОМ

Существуют специализированные организации по борьбе с мошенничеством. В ЕС этим занимается Европейское бюро по борьбе с мошенничеством, ЕББМ (OLAF, англ. European Anti-Fraud Office).

В МВД России борьбу с мошенничеством в основном осуществляют работники отделов по борьбе с экономическими преступлениями УВД. В некоторых ГУВД существуют и специализированные отделы по борьбе с мошенничеством (также см. Бюро специальных технических мероприятий).





ПОДАЧА ЖАЛОБ НА МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

Если вы думаете, что стали жертвой мошенничества с использованием Интернета, вы можете подать жалобу в режиме онлайн в Центр по жалобам на мошенничество в Интернете, совместный проект ФБР и Национального центра по борьбе с преступлениями работников умственного труда. Кроме того, вы можете подавать жалобы по конкретным видам мошенничества в следующие органы:

· Мошенничество, связанное с торговлей товарами: в Комиссию по торговле товарными фьючерсами (CFTC) Commodity Futures Trading Commission (CFTC)

· Обман потребителей: в Федеральную торговую комиссию Federal Trade Commission

· Мошенничество с ценными бумагами: в Центр жалоб при Правоприменяющем отделе SEC SEC Enforcement Division Complaint Center или в органы вашего штата, регулирующие сделки с ценными бумагами state securities regulators.

СОВЕТЫ ПО ОПРЕДЕЛЕННЫМ СХЕМАМ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ

- АУКЦИОНЫ И РОЗНИЧНАЯ ТОРГОВЛЯ В РЕЖИМЕ ОНЛАЙН

· Тщательно изучите потенциального продавца. Если у вас нет личного (притом положительного) опыта взаимодействия с продавцом, предлагающим определенные товары с аукциона или в розницу в режиме онлайн, ищите источники информации на веб-сайте, где размещено предложение продавца, и на других сайтах. Некоторые сайты онлайновых аукционов предоставляют своим участникам возможность «обратной связи», то есть обмена информацией о результатах взаимодействия с определенными продавцами (хотя некоторые продавцы пытаются манипулировать «обратной связью», размещая позитивные, но заведомо ложные сообщения о себе).

· Если возможно, платите кредитной картой или через доверительный счет. Если вы оплачиваете свою виртуальную покупку кредитной картой, эмитированной одним из крупных банков США, ваша ответственность может быть ограничена суммой в 50 долларов США при любых обстоятельствах, притом что уже один эмитент кредитных карт недавно указал, что откажется от права вычета 50 долларов. Альтернативным вариантом могут быть доверительные услуги, оказываемые некоторыми сайтами интернет-аукционов (за небольшой процент) и гарантирующие доставку заказанного товара до того, как ваш платеж будет перечислен продавцу.

Как поступать, чтобы не пострадать от мошенничества в Интернете?

Судя по количеству настойчивых предложений и требований «не упустить возможность», которые вы каждый день находите в своем электронном почтовом ящике, на досках объявлений или веб-сайтах, Интернет-надувательство может казаться неизбежным. И хотя вы не можете полностью избежать настойчивых предложений по Интернету, которые могут оказаться мошенническими, ниже приводится несколько советов о том, как обезопасить себя от них.

ОБЩИЕ СОВЕТЫ ОТНОСИТЕЛЬНО ВОЗМОЖНОГО МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ

Не судите по внешнему виду. Это может представляться само собой разумеющимся, но потребителям необходимо помнить о том, что информация в Интернете – независимо от того, насколько впечатляюще и профессионально выглядит веб-сайт – не обязательно является достоверной. Наличие программного обеспечения, которое дает возможность каждому, при минимальных затратах, создать профессионально оформленный сайт в Интернете, означает, что преступники могут придать своему сайту впечатляющий внешний вид с тем же успехом, что и добросовестные электронные торговцы.

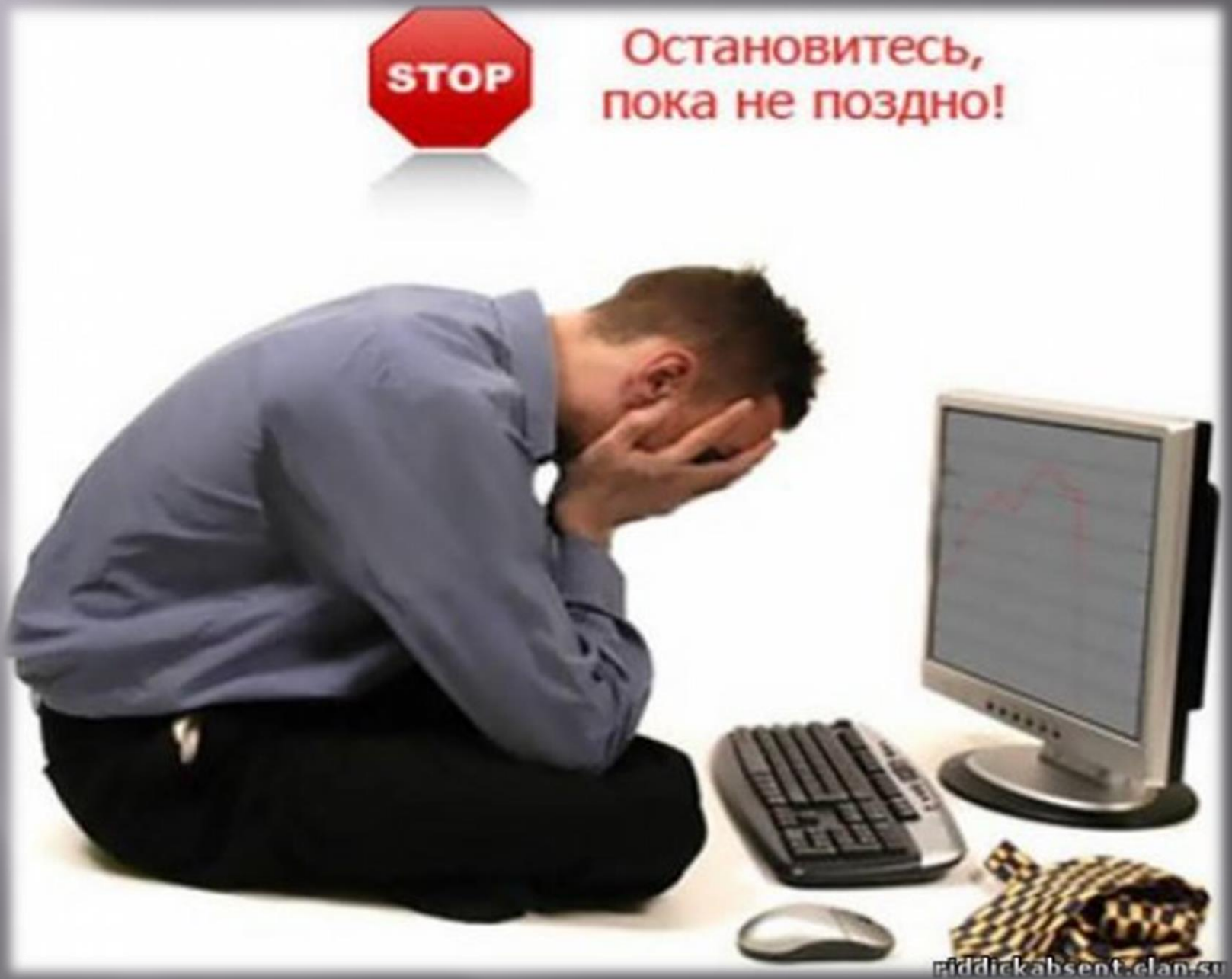
· Будьте осторожны, сообщая свои личные данные по Интернету. Если в каком-либо электронном сообщении от не известного вам лица запрашиваются ваши личные данные – такие как номер удостоверения личности, номер кредитной карты или пароль – не высылайте такие данные, не наведя справки об авторе такого сообщения. Известно, что преступники высылают сообщения под видом, например, системных администраторов или представителей Интернет-провайдера, чтобы убедить людей сообщить свои личные данные. Хотя операции с известными сайтами электронной торговли надежны, особенно если вы используете кредитную карту, этого нельзя сказать о предложениях неизвестных адресатов.

· Будьте особенно осторожны в общении по Интернету с теми, кто скрывает свою личность. Если кто-либо присылает вам сообщение, где отказывается назвать свое полное имя и принадлежность к определенной компании или использует электронный адрес, в котором не содержится полезной идентификационной информации (например, W6T7S8@provider.com), это может означать, что такое лицо не желает оставить о себе никакой информации, которая позволила бы вам связаться с ним впоследствии, если у вас возникнет спор о непоставке товара, за который вы уплатили. Следовательно, советы таких лиц должны вас сразу настораживать, если они попытаются убедить вас доверить им ваши деньги.

· Вас должно настораживать требование предоплаты. В целом вы должны настороженно относиться ко всем продавцам товаров или услуг в Интернете, которые требуют, чтобы вы немедленно выслали чеки или денежные переводы на адрес абонентского ящика, до того, как вы получите товары или услуги, которые вам обещают. Конечно, добросовестные начинающие "dot.com” компании могут не иметь такой солидной репутации как компании, давно существующие на этом рынке, но при этом могут доставить вам все необходимое по справедливой цене. Но даже и в этом случае было бы осмотрительно с вашей стороны, используя Интернет, собрать информацию о неизвестных вам компаниях, до того, как вы доверите им значительную денежную сумму.



Мошенничество, увы, неискоренимо. И на просторах интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.


STOP
Остановитесь,
пока не поздно!
riddickabsent.clan.su