Общие рекомендации по безопасности

ОСНОВНЫЕ ВИДЫ ОНЛАЙН-МОШЕННИЧЕСТВА: КАК РАСПОЗНАТЬ И КАК БОРОТЬСЯ

1. Финансовые пирамиды

Обычно мошенники размещают на форумах и досках объявлений подробную информацию о том, как заработать много денег в кратчайшие сроки, практически не прилагая никаких усилий. При этом Вас просят перечислить некоторую, как правило, небольшую сумму денежных средств на один или несколько электронных кошельков, а также скопировать текст объявления и поместить его на подобных форумах и досках объявлений. Зачастую мошенники прикрываются тем, что список подобных кошельков ведется сотрудником самой системы (что в 100% случаев является ложью). Не верьте подобным объявлениям! Не спешите принимать положительное решение о переводе средств! Помните, что в любой схеме "быстрого и легкого заработка" существует лишь один человек, которому гарантировано быстрое обогащение - организатор подобной схемы.

2. Деловые возможности / "надомная работа"

Мошенники часто используют Интернет для рекламы деловых возможностей, которые якобы позволят зарабатывать тысячи долларов в месяц при помощи "надомной работы". При этом они могут предлагать различные варианты трудоустройства: от сборки авторучек или прищепок, до перевода или оцифровки текстов. В таких схемах всегда предусмотрен небольшой первичный платеж – мошенники объясняют его необходимость тем, что их самих могут обмануть, и просят внести задаток в счет первого заказа. Как правило, в дальнейшем не предоставляются ни материалы, ни информация, необходимые для того, чтобы надомная работа начала приносить доход.

3. Продажа "конфискованных товаров"/купленных по ворованным кредитным картам ("кардинг")

В данной схеме мошенники используют в качестве главной наживки дешевизну товара (как правило, составляющую 50% от стоимости и ниже) и легко объясняют необходимость конспирации своего бизнеса нормами действующего законодательства РФ. При этом, как и во всех остальных случаях, мошенники обязуются доставить товар только после полной или частичной предоплаты. После получения денег "магазин" сворачивают, "продавцы конфиската" исчезают с горизонта и перестают выходить на связь.

4. Взлом ICQ /почтовых ящиков

Мошенники могут получить доступ к ICQ или почте Вашего друга, знакомого или родственника и начинают рассылать по списку контактов от его имени просьбу одолжить денежные средства. При этом Вы думаете, что разговариваете с владельцем данного почтового ящика или ICQ-контакта, а не с мошенником. Тем не менее, мошенника можно легко вычислить, задав несколько личных вопросов, ответы на которые может знать лишь настоящий владелец.

5. Генераторы денег на электронных кошельках

Этот способ мошенничества основывается на предложении скачать некую программу, якобы позволяющую клонировать/увеличивать количество денежных средств на электронном кошельке, либо сгенерировать пин-код предоплаченной карты. Данные генераторы не только не работают, но и, как правило, содержат вирусы.

6. Фиктивные лицензии на программное обеспечение

При очередном включении компьютера, как правило, возникает надпись с предложением пройти активацию программного обеспечения (название программного обеспечения, например, Windows) и осуществить оплату лицензии с помощью терминалов или предоплаченных карт. Данный вид онлайн-мошенничества изначально предполагает наличие вируса на используемом компьютере. Помните, что лицензионные версии ПО не требуют активировать себя более одного раза. При малейших сомнениях связывайтесь со службой технической поддержки компании-разработчика программного продукта.

7. "Мобильное" мошенничество

Как правило, мошенники звонят на мобильный телефон заранее выбранной жертвы и представляются:

- родными или знакомыми, якобы попавшими в неприятную ситуацию (участие в ДТП, нахождение под стражей и т.п.), либо сотрудниками правоохранительных органов, помогающими им выпутаться из неприятной ситуации;
- сотрудниками различных компаний (обычно теле- или радиокомпаний) и сообщают Вам о том, что Вы выиграли ценный приз;
- партнерами или клиентами, с которыми у Вас назначена встреча;

- откликнувшимися на Ваше реально существующее объявление о чем-либо (например, о розыске домашних животных, утерянных документов и т. д.).

  Во всех вышеуказанных случаях мошенники постараются максимально быстро убедить Вас в своей правоте, чтобы Вы не успели проанализировать ситуацию. Они будут настаивать на необходимости срочной передачи/перевода денежных средств под различными благовидными предлогами. Будьте внимательны - не совершайте опрометчивых поступков! Не переводите деньги незнакомым людям! В свою очередь, попытайтесь узнать личные данные звонящего. Задавайте наводящие вопросы, пытайтесь ловить собеседника на противоречиях – это поможет вывести мошенников на чистую воду и сохранить Ваши средства в безопасности. При необходимости без промедления обратитесь в правоохранительные органы.

ОБЩИЕ РЕКОМЕДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ И ПОЛНОЦЕННОЙ ЗАЩИТЫ ВАШЕГО КОМПЬЮТЕРА

Помните – злоумышленники постоянно совершенствуют способы проникновения в Ваш компьютер и ищут новые возможности получения доступа к Вашей персональной информации. Следуйте рекомендациям разработчика операционной системы Windows по безопасной работе в сети Интернет:
http://www.microsoft.com/rus/athome/security/viruses/default.mspx
http://www.microsoft.com/rus/athome/security/protect/windowsxp/Default.mspx
Выполняйте несложные рекомендации по своевременному обнаружению вирусной активности и обеспечению безопасности Вашего компьютера:

1. Своевременно устанавливайте критические обновления операционной системы.

Эта мера обеспечивает закрытие найденных уязвимостей операционной системы, при помощи которых злоумышленники могут получить доступ к Вашему компьютеру. Настройте ежедневное автоматическое обновление операционной системы (Пункт меню Пуск - Панель Управления - Автоматическое обновление). Если автоматическое обновление включено, операционная система Windows регулярно проверяет веб-узел Windows Update на предмет наличия обновлений, которые помогут защитить компьютер от различных угроз безопасности. К таким обновлениям относятся обновления безопасности, критические обновления и пакеты обновлений. В зависимости от Выбранного варианта Windows автоматически загружает и устанавливает первоочередные обновления, которые требуются для компьютера, или уведомляет пользователя о наличии этих обновлений. Если для подключения к сети Интернет Вы используете медленные каналы, и автоматическое обновление затрудняет Вашу работу, регулярно заходите на сайт Microsoft Update, скачивайте и устанавливайте все критические обновления операционной системы и прикладного ПО.

2. Запустите и не выключайте встроенный брандмауэр (файрвол, межсетевой экран) операционной системы, либо установите специально разработанный брэндмауэр.

Брандмауэр обеспечивает безопасное подключение компьютера к интернету, закрывая не используемые Вами сетевые соединения, блокирует соединения шпионских и других вредоносных программ, внедряемых злоумышленниками на Ваш компьютер различными способами (через поддельные или специально взломанные сайты, распространяемые по электронной почте, скаченные под видом различных полезных программ). Возможно, окажется более эффективным установить специально разработанные файрволы. Перед установкой данных файрволов, не забудьте остановить встроенный Брандмауэр Windows, во избежание конфликтов в работе

Бесплатные файрволы:

- Jetico Personal Firewal
- Outpost Firewall FREE
- Zone Alarm Free
- Online Armor Free
- Comodo Firewall Pro

  Пробные версии платных продуктов с ограниченным сроком годности:

- avast! 4 Professional
- Dr. Web

- BitDefender Antivirus
- Eset NOD32
- Kaspersky Antivirus
- McAfee VirusScan Plus

3. Установите антивирусное ПО и как можно чаще обновляйте его вирусную базу

- Помните – некоторые компьютерные вирусы начинают определяться антивирусным программным обеспечением спустя 10-15 дней после их появления.
- Производители антивирусного программного обеспечения иногда делают до 3-5 обновлений вирусных баз в сутки, поэтому регулярно обновляйте вирусные базы.
- Устанавливайте только одну антивирусную программу по Вашему выбору на своем компьютере, установка и запуск нескольких антивирусных пакетов не рекомендуется. Антивирусные программы будут мешать друг другу и замедлят работу компьютера (вплоть до нарушений в работе системы).
- Перед установкой другой антивирусной программы обязательно удаляйте предыдущую, поскольку большинство антивирусных программ устанавливает резидентный модуль, для удаления или остановки которого требуется обязательная перегрузка компьютера.

  Установите антивирусное программное обеспечение, рекомендуемое разработчиком операционной системы http://www.microsoft.com/protect/viruses/xp/av.mspx. В крайнем случае, Вы можете воспользоваться бесплатным программным обеспечением или пробными версиями платных продуктов с ограниченным сроком бесплатного использования.

  Бесплатное антивирусное программное обеспечение:

- avast! 4 Home Edition
- AVG Antivirus Free
- AntiVir PersonalEdition Classic
- Clam Win Free Antivirus

  Пробные версии платных продуктов с ограниченным сроком годности:

- Dr.Web
- BitDefender
- Eset NOD32
- Kaspersky
- McAfee

4. Установите и регулярно обновляйте ПО, обнаруживающее шпионские программы

Существует специально разработанное ПО для обнаружения шпионских программ, при помощи которых злоумышленники крадут пароли и другую информацию с Вашего компьютера. В некоторых случаях эти программы оказываются более эффективными в поиске и обезвреживании троянских программ по сравнению с антивирусами. Кроме того, работа этих программ не столь загружает операционную систему. Однако лучше всего использовать антишпионское ПО вместе с антивирусом, поскольку вместе они работают вполне корректно. При установке антишпионского программного обеспечения обязательно следуйте рекомендациям разработчиков по совместному использованию антивирусного и антишпионского программного обеспечения. Установите антишпионское ПО, рекомендуемое разработчиком операционной системы Windows Defender.

Бесплатное антишпионское программное обеспечение других производителей:

- a-squared Anti-Malware
- Ad-Aware Personal
- AVG Anti-Spyware Free Edition
- Spybot S&D
- SpywareBlaster

  Пробные версии платных продуктов с ограниченным сроком годности:

- a-squared Anti-Malware
- AVG Anti-Spyware
- Spy Sweeper

5. При посещении сомнительных сайтов используйте браузер с максимальными настройками безопасности или используйте альтернативный браузер.

Большинство компьютерных вирусов написано для наиболее распространенного браузера Internet Explorer. При посещении сомнительных сайтов установите максимальную настройку безопасности браузера Internet Explorer (Меню - Сервис - Свойства обозревателя - Закладка безопасность - Уровень безопасности "Высокий") или используйте альтернативный браузер с максимальными настройками безопасности.

Альтернативные браузеры:

- Mozilla Firefox (Имеет отдельный "Безопасный режим" запуска программы, с максимальными настройками безопасности)
- Opera