Как избежать мошенничество в интернете?

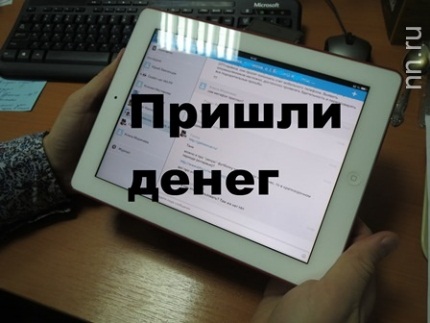
Мошенники в Интернете всегда существовали, существуют и будут существовать. Каждый год жулики разных мастей изобретают новые способы для обмана рядовых пользователей компьютера и всемирной сети. И главная опасность здесь кроется в том, что ни одна программа не в состоянии защитить Вас от мошенников, так как цель злоумышленника не компьютер, который имеет свою защиту, а человек, который имеет свои слабости.

Распространенные виды мошенничества.

**Работа на дому**

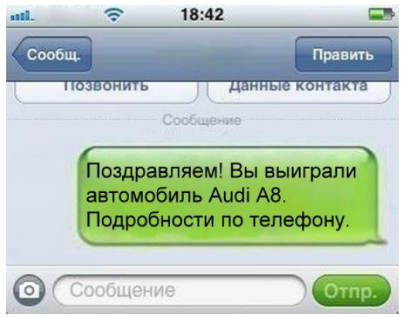
Тут схема такая: Вам приходит письмо с предложением о работе на дому, например, по набору текста, сборке бус, упаковке дисков, обработке изображений или что-то в этом роде. Затем Вас просят оплатить разовый взнос за услуги курьера, или за регистрацию, или за то, чтобы подтвердить серьезность своих намерений, или за какой-либо пакет документов. После перечисления денег, естественно, Вы никакой работы не получите. В лучшем случае Вам пришлют какую-нибудь инструкцию, чтобы начать работать. Например, посоветуют дать объявление типа: "Предлагаю работу на дому" и получив оплату предлагать людям давать объявления типа: "Предлагаю работу на дому" ))).

**Просьба**

Часто мошенники в интернете рассылают письма с просьбой о помощи вида: "Помогите собрать денег на операцию!", или "Помогите собрать денег, чтобы меня не посадили!", или что-то в этом роде. Самое печальное здесь то, что из-за таких мошенников люди перестают верить реальным просьбам о помощи. Но если Вы, все же, решили помочь человеку, обязательно установите с автором личный контакт (хотя бы по телефону), установите фамилию нуждающегося, диагноз и в какой больнице лежит. Кроме этого, помните, что обычно в таких случаях открывается специальный благотворительный счет.

**Чудо - инвестиции**

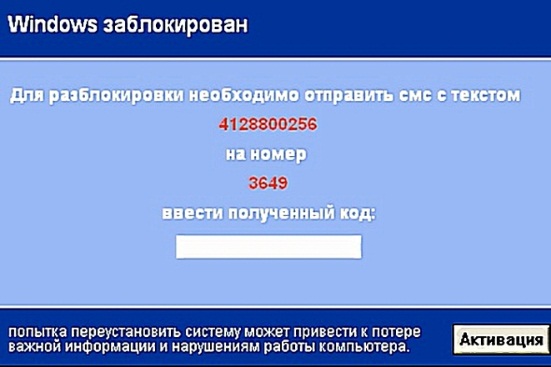
В этом варианте, Вам предлагают перечислить деньги на указанный кошелек и получить обратно удвоенную сумму. Или сообщают о новой высокодоходной инвестиционной компании, выплачивающей 100% прибыли в месяц. В любом случае - это либо полный "развод", либо очередная финансовая пирамида.

****

**Лотереи**

Удивительно, но еще остались люди, которые и сегодня верят сообщениям типа: "Вы выиграли 1 000 000 рублей! Чтобы получить деньги перечислите 1 000 рублей на счет №ххххххх."

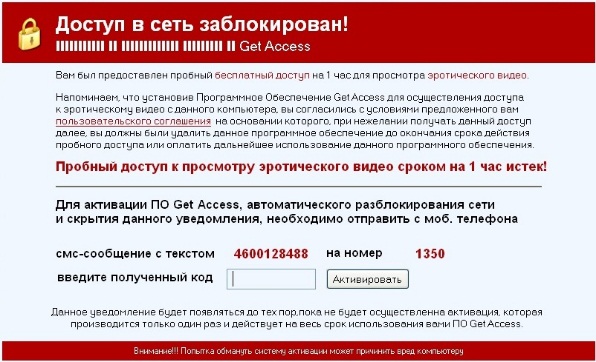
**Антиспам проверка SMS**

Очень распространенный вид мошенничества в наши дни. Применяется, практически, повсеместно. Суть его заключается в следующем: Для получения какой-либо услуги Вам предлагается пройти бесплатную проверку, что Вы реальный человек, посредством бесплатного SMS-сообщения. Затем на указанный Вами номер телефона приходит SMS с просьбой ответить на сообщение каким-либо словом. Часто это слово "Да" или Ваш возраст. Вместе с этим ответом с Вашего баланса уходит N-ная сумма денег.

**Фишинг**

Еще один очень распространенный прием, который используют мошенники в интернете. Вам приходит поддельное письмо, например, от банка или электронной платежной системы, с просьбой перейти по ссылке на фальшивый сайт, который по своему виду не отличается от настоящего, и ввести свои личные данные (указать логин, пароль и т.д.). После того, как Вы введете необходимую информацию, Вы будете перенаправлены на настоящий сайт, а введенные данные попадут в руки к мошенникам. Или, как вариант, Вы можете совершить оплату на таком поддельном сайте, и Ваш платеж уйдет на счет мошенников.

**Банеры - вымогатели**

[](http://safecomp.me/files/internet_lan/170714/1.jpg)В данном случае на компьютер скачивается вирус. Возможно скачать вирус с какой то программой или зайдя на недоброжилательный сайт или перейти по незнакомой ссылке. У Вас во весь экран или в центре экрана появляется баннер, в котором может быть написано что Вы неправомерно просматриваете тот или иной материал или у Вас закончилась подписка на что-либо или другой подобный бред. И Вас просят отправить на номер телефона определённую сумму денег для разблокировки баннера.

**СМС - рассылка**

[](http://safecomp.me/files/internet_lan/170714/4.jpg)Вам Приходит смс-сообщение о том что Вам поступил платёж через QIWI-кошелёк. Сообщение внешне похоже на то что присылает QIWI при пополнении баланса телефона. Вслед за первой смс приходит другое, якобы извините ошиблись номером, не могли бы Вы вернуть деньги на такой-то номер телефона. Всё выглядит вполне реально, за исключением двух нюансов. Во-первых мне не приходило уведомление о пополнениии счёта и другой это то что вместо буквенного обозначения адреса отправителя был обычный номер телефона, с которого прислали сообщение.

Первое что должно насторожить это номер, с которого пришло смс. Он должен быть буквенный, а не цифровой. И второе, Вы можете проверить поступал ли платёж в личном кабинете Вашего сотового оператора.

**Главные отличительные признаки мошенничества**

 Как правило, все схемы мошенников построены на том, чтобы сыграть на таких человеческих чувствах, как жалость или желание заработать.

 Ни один серьезный работодатель не требует предоплату с работника, работодатель платит вам, а не наоборот!

 Все серьезные компании имеют сайты с доменами второго уровня вида: www.company.ru. Мошенники обычно в своих целях используют бесплатные хостинги, поэтому их сайты выглядят как www.site.narod.ru или www.site.by.ru.

 Немаловажное значение имеет возраст домена. Мошеннические сайты редко работают более 2-3 месяцев. Они либо закрываются сами, собрав деньги, либо их блокируют из-за жалоб потерпевших.

 На серьезных сайтах всегда есть возможность связаться с администратором.

 Ни один банк и ни одна электронная платежная система никогда не будет просить Вас сообщить свой логин и пароль.

 В случае просьбы о помощи у нуждающегося должен быть открыт и зарегистрирован благотворительный счет в банке.

**Советы по защите от мошенников**

 Не открывайте ссылки в тех письмах, которые приходят от незнакомых Вам людей.

 Внимательно смотрите на какую страницу Вас отправляет ссылка.

 При вводе своих персональных данных обращайте внимание на адрес страницы, на которой Вы находитесь. Например, адрес страницы "Вконтаке" выглядит так: http://vk.com, но не в коем случае не так: http://wk.com и не так: http://vkk.com

 Получив письмо от платежной системы о проблемах с Вашим счетом, удаляйте его, т.к. техническая поддержка никогда не рассылает таких писем.

 Не храните свои личные данные (логины, пароли, пин-коды) на жестком диске компьютера.

 Всегда проверяйте отзывы о том или ином сервисе, прежде чем совершить там оплату.

 Свяжитесь с администратором сайта и задайте какой-либо вопрос.

**Однако, самый верный способ защиты от мошенников в Интернете - это Ваше здравомыслие. Помните известную пословицу на счет бесплатного сыра?**