1.«Волшебные» кошельки.

Получая СПАМ по e-mail, ICQ рассылке или каким-то иным способом человек узнаёт о существовании некоего «Супер кошелька», на который нужно отправить сумму денег, а он вернёт обратно сумму намного больше, обычно в 2 раза. Здесь при отправлении суммы есть 2 возможных развития событий: либо деньги уходят безвозвратно, и никто ничего Вам не возвращает, либо подкидывается приманка в виде первой увеличенной суммы. Тут аферисты рассчитывают, что на радостях человек отправит ещё больше денег, которые уж точно не вернутся. Бывает, пролетают на 3 раз, то есть 2 первых раза деньги реально приходят, предлагая отправить совсем заоблачную сумму для полного улёта. В результате человек теряет наголову выше первого своего взноса.

Неистощимы на выдумку русские умельцы! Иногда нам открывают «коммерческую тайну» о существовании интернет счёта крупной компании с баснословной суммой денег. Дальше мошенники несут ахинею типа «В скрипте кошелька найдена ошибка, растаскивай деньги пока не поздно!!» А делится этой тайной якобы бывший сотрудник этой самой компании, решивший отомстить им за предвзятое отношение разглашением важной информации!

Порой можно наткнуться на сайты, ведущие «мониторинг» честно платящих волшебных кошельков! Или же нам предлагают на благое дело обанкротить лохотронщиков и аферистов, снимая с их кошелька деньги сами же аферисты! «Просто отправьте 5 у.е., и Вы получаете 10!», - говорят «борцы за справедливость».

Магические интернет кошельки располагаются в системе WebMoney или Яндекс деньги, чаще всего в последней, т.к. там защита от надувательства слабее.

2.Фишинг

Кроме всем известного значения «рыбная ловля» английское слово fishing в глобальной сети означает поимку на крючок особо доверчивых. Есть ещё конечно такое понятие как Спутниковая Рыбалка, но это не по теме аферы. Рыбачки в интернете отправляют Вам на адрес электронной почты письмо о том, что Ваш счёт или аккаунт заморожен или заблокирован в связи с неполадками на сервере, переездом в другой офис компании, переноса сервера и т.д. Иногда могут сказать, что потеряли Ваш пароль, что кроме смеха, у меня лично ничего не вызывает. Такой ситуации просто не может произойти, тем более даже в случае ЧП проблема будет решаться более цивильным способом. Всё содержание письма сводится к тому, что Вам нужно ввести свой пароль в форму, отправить его в ответном письме или же перейти на сайт точь-в-точь похожий на настоящий и «активировать свой аккаунт». На самом деле сайт принадлежит злоумышленникам, которые, заполучив Ваши конфиденциальные данные, попросту Вас обворуют, зайдя на Вас реальный счёт. В первую очередь следует обратить на адрес сайта, где Вас просят подтвердить логин и пароль. Он отличается от настоящего адреса, а значит – это 100% SCAM!

3.Удалённая работа

Ещё один вид онлайн мошенничества, который, однако, не следует путать с официальным удалённым трудоустройством. Вы каким-то образом попадаете на сайт, где предлагается высокооплачиваемая работа на дому, например набор текста. Информации на сайте куча, вплоть до контактных данных работодателя. Гарантируют финансовую независимость, свободный график и полный социальный пакет! Вы уже готовы получить работу…и тут Вам предлагают отправить деньги,

которые Вам тут же вернут, как только Вы заступите на службу. Говорят, это нужно для того, чтобы подтвердить серьёзность Ваших намерений в отношении работы. Это всё спам и обман. Денег Вы обратно не получите… и работы тоже.

4.«Выигрыш» в конкурсе, лотерее

Вам на почту может прийти письмо…с поздравлениями! Вас объявляют победителем в какой-то лотерее или конкурсе (хотя Вы нигде не участвовали). Ещё на сайтах Вы можете увидеть мигающий зелёным цветом баннер «Вы выиграли! Вы 4 256 892 посетитель, увидевший этот баннер!!» Бред. Так вот, чтобы забрать свой «выигрыш» Вам всего-то нужно либо открыть файл, прикреплённый к письму и получить на свой компьютер трояна или червя, либо перевести небольшую сумму денег на любезно указанный злоумышленниками счёт, а потом Вам тут же отдадут Ваши честно выигранные $100 000 или какой-нибудь другой приз. В данном виде мошенничества аферисты могут представляться крупной реально существующей фирмой или компанией. Как правило, на сайте контактные данные липовые, да и вообще можно найти много подозрительного.

Данный лохотрон рассчитан на простачков, которые сгоряча от радости отправляют деньги, чтобы получить свой несуществующий выигрыш. Кстати подобная афера есть и вне интернета, когда Вам отправляется похожая смс-ка на телефон, а чтобы забрать выигрышь, нужно положить деньги либо на какой-то номер, либо на счёт.

Лотерейные мошенники

Кто из нас не мечтает однажды услышать «Поздравляем! Вы выиграли и теперь вы богаты»? За редким исключением разбогатеть с лотереей мечтает каждый, но не каждый знает простую истину: выиграть может только тот, кто купил лотерейный билет. Об этом говорил ещё автор культового фильма «Форрест Гамп», Уинстон Грам. Тем не менее, многие доверчивые люди без всяких сомнений следуют указаниям в письме, в котором говорится, что они сорвали куш в лотерею. К сожалению, в превалирующем большинстве случаев подобные письма отправляют лотерейные мошенники с целью получения личных данных и последующей финансовой выгоды. Примером для них послужили так называемые «нигерийские письма», рассылка которых началась еще в 80-ые годы прошлого столетия. В таком письме, как правило, получателя уведомляют о том, что он стал случайным наследником некоего миллионера, и может вступить в права, предоставив финансовую информацию. С развитием лотерейной индустрии, сегодня чаще всего в письмах фигурируют громкие имена тиражных игр. Нередко лотерейные мошенники используют известные бренды, такие как Facebook, Евромиллионы, LaPrimitiva, Powerball, SuperEnalotto и многие другие. Наиболее распространение способы лотерейного мошенничества:

- ***Письмо***
- ***Электронная почта***
- ***Сообщение в социальных сетях***
- ***Телефонный звонок (реже)***
- ***СМС-сообщение***

«Вы выиграли в Евромиллионы»

С этой фразы начинается большинство писем лотерейных мошенников. Но затем говорится, что произошло это благодаря тому, что адрес электронной почты или номер телефона были в случайном порядке выбраны лотерейной организацией. Далее, как правило, автор письма просит вас предоставить данные банковского счета, кредитной карты, паспорта, номер социального страхования и прочую идентифицирующую информацию, которая будет использована якобы для оплаты комиссии за перевод вам выигрыша. Стоит ли уточнять, что в 100% случаев выигрыш доверчивый «победитель» не получает, зато мошенник становится богаче на сотни, а нередко и тысячи долларов, евро и фунтов. Играйте в Евромиллионы официально чтобы стать законным обладателем приза!

Мошенничество с американской лотереей Powerball

Вслед за «популярностью» рассылки писем, сообщающих о выигрыше в панъевропейскую лотерею Евромиллионы, в 2014 очередным инструментом мошенников стала американская лотерея Powerball! Играя на эмоциях простых американцев, многие из которых согласно статистике, хотя бы раз в жизни покупали билет США-Powerball, авторы письма сообщают, что реципиент стал счастливым претендентом на сумму в $750,000, которой щедро поделится один из победителей Powerball. В частности речь идёт об автомеханике из Канзаса, Кевине Карлсоне, который в канун Рождества 2013 действительно сорвал джек-пот $71,500,000. Ещё одним менее распространённым способом стала услуга отправки 100% достоверных выигрышных номеров с предоплатой в $59.Учитывая, что шанс на выигрыш главного приза в Powerball составляет 1 к 175,223,510, если бы угадать номера было бы так просто и дешево, американская лотерея не успевала бы выплачивать джек-поты До появления писем, уведомляющих о «подарке победителя Powerball» схема лотерейных мошенников действовала следующим образом: жертву уведомляли о выигрыше в иностранную лотерей и прилагали чек на сумму от $2,0000 до $5,0000 в качестве аванса. Для того чтобы вложить его на банковский счёт отправитель должен был

оплатить некую комиссию или налог выигрыша. Стоит ли говорить, что чек в последствии оказывался недействительным? По сообщению службы почтовой инспекции США, ежегодно американцы, ставшие жертвами мошенников, теряют до $120 миллионов.

СМС-сообщение. С развитием технологий лотерейные мошенники также смогли усовершенствовать свои методы. Теперь им достаточно приобрести пакет многоразовой смс-рассылки, в расчёте на то, что наивный получатель перезвонит по указанному номеру.

Письмо по электронной почте. Классический вариант лотерейного мошенничества, тем более, что достоверности ему можно придать, использовав логотип известной лотерейной организации, как видно на примере этого письма:

Признаки того что с вами связались лотерейные мошенники:

- ***Вам сообщают о выигрыше в лотерею, в которой вы никогда не принимали участие***
- ***От вас требуют личные данные или финансовые данные***
- ***Вам обещают перевести выигрыш на банковский счёт***
- ***Вам сообщают, что один из победителей лотерей, выбрал вас в качестве получателя части его выигрыша***
- ***От вас требуют оплатить стоимость услуг/ комиссию/налог до получения выигрыша***
- ***В письме не указан номер тиража и выигрышные номера, препятствуя проверке достоверности.***

- ***Номер телефона, адрес, указанные в качестве контактной информации неверны/контактные данные отсутствуют.***
- ***Вам предлагают услугу предоставления выигрышных номеров с 100% достоверностью за некую сумму.***

5.Выгодный обмен

Всё начинается с того, что в интернете Вы находите интересную статью, что существуют такие обменники валют, на которых можно поменять деньги и заработать на этом. Вам указывают ссылку на чудо-обменник, очень яркую и заметную, чтобы Вы обязательно туда зашли! Всё, что от Вас требуется, обменять к примеру рубли на доллары, а потом обратно доллары в рубли и получить с этого прибыль. Запомните, ни один обменный сервис не будет работать себе в убыток, только идиот способен на это, а идиотов вроде как среди админов ещё нет. Ни один, кроме….кроме того, который создан специально для аферы, а автор статьи про обогащение на обмене ни кто иной, как владелец этого обменника. При обмене валюты у Вас как положено снимут деньги, только вот другая валюта не придёт. Липовые контактные данные и невозможность обменять другие валюты из-за «технического сбоя», кроме тех, что «по выгодному обмену» первые признаки, что Вас дурят.

6.*Суперпрограммы для быстрого заработка*

Вам предлагают вложить свой капитал в покупку программы за 10-20 баксов, которая сама, автоматически (!) заработает Вам гораздо больше, скажем, 200 $! Таких программ нет и быть не может. Купив программу, она будет просто открывать Вам сайты (да ещё и с вирусами и порнографическим содержанием) и показывать заработок 1$, 5$, 20$.... но когда набирается минимальная выплата для вывода, ничего не происходит. Вам не заплатят несуществующий заработок, ибо всё что показывала программа были лишь красивые и греющие душу картинки. Иногда такая «лампа Алладина» Вам предлагается абсолютно бесплатно, вот только Джин внедрит на Ваш компьютер кучу вирусов, и на этом всё закончится.

Недавно появился новый вид псевдозаработка, а точнее аферы в интернете в этой сфере:Вы регистрируетесь на сайте и в день Вам даётся 4 простых математических примера (3+5=?). За каждый из них Вы получаете 1,2$. Минималка для вывода 70$. Шибко «умные» знатоки сами дозревают до идеи, что можно положить сумму денег на счёт, которая не ограниченна по размеру, а потом снять всё сразу вместе с заработком, чтобы не ждать, пока так наберётся 70 зелёных. Деньги уходят бесследно. После такого кидалова словно помоями облили, не попадитесь!

Ещё один вариант «обогатится» - это купить программу-взломщик ВебМани, которая будет доставать Вам пароли от чужих счетов, а Вам только останется заходить и переводить оттуда денежки! Если кто не знает, WM – очень защищённая система. Да там если ip уже меняется, с которого заходят, просят предоставить идентификационные ключи. Геморрой случается по этому поводу даже у законных владельцев. Подобрать пароль через Брутфорс «Brutforce» очень долго, почти нереально…на взлом 1 аккаунта таким макаром могут уйти месяцы…сомнительный заработок, если учесть, что потом придётся возиться с идентификационными ключами ещё…несколько лет. В общем – SCAM!