КАК за 30 минут стать

Властелином Интернета

Алексей Виноградов © 2012

Содержание

Введение

Привет! Меня зовут Виноградов Алексей, я - автор блога IT-LIKE.RU. В этой книге я хочу рассказать тебе о вреде и пользе, которую может принести интернет. Ты узнаешь зачем люди вообще пользуются интернетом, как извлечь из него больше пользы, какие опасности нас подстерегают и как от них быть подальше.

Ни для кого не секрет, что сегодня Интернет прочно вошёл в нашу жизнь и пронизывает каждую сферу нашей деятельности. Будь то работа, хобби, семья, здоровье или деньги - везде интернет имеет своё влияние. Мы его используем как канал связи и коммуникаций, идём туда за ответами на повседневные вопросы, ищем секреты здоровья и молодости, находим новых друзей, а некоторые умудряются зарабатывать в нём деньги.

Но за кулисами интернета кроется источник опасности. Так же как и в реальной жизни, в интернете есть мошенники, которые только и ждут удобного момента, чтобы засунуть руку в ваш кошелёк. И не надо этот момент недооценивать или упускать из виду. Как говорится «пока гром не грянет, мужик не перекрестится!» Но тогда уже поздно…

Полезные сервисы интернета

Интернет нам даёт массу возможностей, которых небыло у наших родителей. С помощью различных сервисов интернета можно и нужно быть на гребне волны современного мира. А кто этим ещё не пользуется, тот сильно отстаёт. Как сказал Льюис Кэрролл «Чтобы остаться на месте, нужно бежать, а чтобы двигаться вперед, нужно бежать еще быстрее". Вот так и здесь.

Так какие же сервисы или, другими словами, возможности нам предоставляет Интернет? Некоторыми из них, я уверен, вы уже пользуетесь, о других просто слышали, а о некоторых не подозревали или только догадывались. Не буду сейчас рассказывать о невероятных возможностях связи и коммуникаций посредством мировой паутины, это и так все знают. Бумажная почта уже давно «не рулит» для обмена сообщениями с друзьями или родственниками. Скажу лишь, что всего-то за несколько последних лет эта функция вышла на новый качественный уровень. Десятилетиями для этого служили электронная почта и мессенджеры типа ICQ. И только относительно недавно появились крупные социальные сети ВКонтакте, Facebook и Одноклассники. В социальных сетях можно жить, не выходя в Интернет ☺

Также нельзя не упомянуть о голосовой и видеосвязи через интернет с помощью таких программ как Skype и QIP. В последнее время эта функция стала также доступна в социальных сетях. С помощью Skype можно общаться с друзьями и родственниками по всему миру бесплатно! Для этого нужен только интернет и установленный Skype.

Ответы на вопросы и решение проблем

В Интернете можно найти ответ почти на любой вопрос с помощью поисковых систем Яндекс и Google. А если там его нет, то смело задавайте свой вопрос на сервисах ответов и получайте ответ почти сразу! Именно так работают сервисы ответов, например такие как Ответы@mail.ru и Ответы Google. Достаточно задать хоть самый тупой вопрос в подходящую рубрику, и люди начнут отвечать и советовать. За это они получают баллы, а на лучшие ответы и вопросы проводятся голосования. Такие себе мини-социальные сети вопросов и ответов. Существуют и другие сервисы, но эти самые популярные.

Вторым источником решения проблем являются форумы. Это специальные сайты с собственной структурой рубрик для обсуждений. От сервисов ответов отличаются тем, что можно обсуждать решение какой-то проблемы более развёрнуто. На форумах обсуждают всё что угодно: начиная от темы «как продеть иголку в ушко» и заканчивая «как построить дом» и проблемами мирового господства. Обсуждение некоторых тем, бывает, длится годами! Но именно там есть шанс решить проблему от и до. Зачастую можно решить самостоятельно те проблемы, решение которых требует привлечение платного специалиста (сантехника, компьютерщика или мастера чего угодно).

Но здесь нельзя терять бдительность, и сто раз подумать, прежде чем сделать всё так, как посоветовали на форуме, особенно если это касается здоровья! Кстати, что касается здоровья, так на самих порталах онлайн-консультаций, например http://www.eurolab.ua или http://pulsplus.ru есть своё кредо: ни в коем случае не давать 100% рекомендаций, только советы! Считается, что врач онлайн (удалённо) не может точно установить диагноз, поэтому даже не пытайтесь их умолять назначить вам лечение. Вопрос очень

серьёзный, поэтому только рекомендации и совет обратиться к врачу.

Форумы, как правило, тематические в какой-то области, например в компьютерах, медицине, строительстве и т.д. Чтобы найти подходящий вводите в Яндексе или в Google свою тематику и просто добавляете в конце «форум» (без кавычек). Из списка найденных регистрируйтесь в наиболее понравившихся и посещаемых и задавайте свой вопрос в подходящей рубрике. Посещаемым считается форум, в рубриках которого имеется более тысячи ответов.

Видеосервис Youtube - как мощный поисковик

Я не открою Америку, если расскажу про сервис YouTube от Google, но не все понимают всю его мощь! На самом деле, YouTube это не просто свалка видео, но и мощный поисковик! Вспомните, как часто не получается найти нужную информацию в Яндексе или Google? А ведь можно забить свой поисковый запрос в строку поиска YouTube и получить серию видео-ответов! Как покрасить дом, как заплести косичку – можно бесконечно об этом читать статьи и смотреть фотографии, но лучше один раз увидеть и сделать!

Конкурсы, призы, викторины

Многие недооценивают возможности интернета для получения приятных подарков. Каждый день где-то проводится какой-то конкурс! И вероятность выигрыша намного более чем в лотерее, например 1 из 30, нормально? Можно найти какие угодно, например на лучшую историю, на лучшую фотографию, или розыгрыш среди правильно ответивших на вопросы. Есть даже

специальные форумы, где участники делятся ответами на вопросы викторин. Так что вам даже не нужно думать над ответами, а просто найти их через поиск. Примером такого форума является http://www.prizolovy.ru, там же можно черпать информацию о самих конкурсах и где они проводятся.

Обучение в интернете

Нет, я не имею ввиду книги и статьи в интернете. Сегодня бурно развивается удалённое обучение, которое позволяет стать мастером в выбранной области и получить вторую специальность (неофициально).

Это различные онлайн-школы, тренинги, вебинары и коучинг. А теперь расскажу подробнее как это работает.

В онлайн-школах можно пройти курсы с помощью обучающих материалов, видеоуроков, аудиокастов и, конечно же, обратной связи. Обычно производится набор на курс и дальше с ним идёт работа. Вам даются материалы, проводятся онлайн-встречи с преподавателями для ответа на вопросы и происходит общение с «одноклассниками». Эффективность таких школ находится на высоком уровне, но очень многое зависит от личного отношения к занятиям. Так как оценок никто вам не ставит и выгнать не может, то некоторые расслабляются и «подзабивают» на задания... В итоге не получают ожидаемых результатов и пишут «говноотзывы».

Лучше всего работают платные школы. Не только из-за того, что платный материал и обратная связь более качественные, а и потому, что отношение к платному курсу совсем другое. Ведь вы уже заплатили деньги (а в среднем это около 100$), и теперь точно будете брать от обучения всё, чтобы небыло жалко денег! И это работает, и чем дороже обучение - тем лучше.

Сюда же относятся различные онлайн-тренинги. Они могут быть разной длительности - как один день, так и несколько недель. Призваны развить какую-то способность, например делать больше за меньшее время, или обучить новому делу, например научиться продавать в социальных сетях.

И школы и тренинги используют для обучения вебинары. Это такие места в интернете, где тренер может рассказывать и вещать видео для участников вебинара. Участники могут задавать вопросы в чате и получать ответы. Вебинары проводятся не только в рамках какого-то тренинга, но и сами по себе. Это похоже на лекцию по абсолютно любому вопросу, например «как уехать жить за границу» или «как поднять продажи в бизнесе». А можете сами провести вебинар на волнующую тему. Популярные порталы вебинаров: http://webinar.ru, http://webinar.ua.

Последняя ступенька получения знаний в интернет – это коучинг, т.е. метод непосредственного обучения менее опытного более опытным в процессе работы. В этом случае с вами непосредственно работает наставник (коуч). От обычного репетитора отличается тем, что его задача не ограничивается впихиванием необходимых знаний. Коучинг – это ведение до результата. Т.е. ваш коуч от вас не отстанет, пока вы не получите результат за который заплатили. Если результатом должен быть работающий бизнес, значит пока у вас не будет своего работающего бизнеса коуч будет вас вести до результата. Правда, стоит коучинг весьма дорого, в среднем от 1000$.

Личные консультации через интернет помогут решить наболевшие индивидуальные вопросы, сдвинуться с мёртвой точки и двигаться дальше. Консультации можно получать у специалистов с помощью программы Skype. Найти нужного специалиста можно через поиск или на специализированных форумах. Например здесь

http://health-club.org.ua/konsultaciya-online.html можно проконсультироваться по поводу здоровья, а здесь http://mnepsiholog.com.ua можно получить консультацию психолога. Очень удобно, никуда не надо ехать, нужен только интернет и микрофон!

Путешествуем по всему миру и Солнечной системе лёжа на диване!

Многие знают об этой возможности системы Google Планета Земля, но немногие пользуются. А ведь там можно определиться с выбором куда поехать отдыхать или где лучше всего купить недвижимость. Или просто попутешествовать по миру лёжа на диване! Google Earth – это отдельная программа, которая устанавливается на компьютер и в режиме реального времени получает информацию с сервера Google. С её помощью можно переместиться в любую точку Земного шара и обследовать её так, как будто вы сами там находитесь! Всегда было интересно каково прогуляться по пустыне? или как бы было прикольно провести уикенд в Антарктике? а может просто пройтись по самым сексуальным пляжам в Испании? Не вопрос! Всё это можно сделать с помощью Google Earth. И даже обследовать другие планеты Солнечной системы!

Виртуальная флешка и виртуальный офис

Приходилось ли вам таскать флешку с документами из офиса в офис? Или в нужный момент самого важного документа не оказывалось под рукой? Если ответ «да», значит специальные сервисы интернета облегчат вашу жизнь. Эти сервисы позволяют закидывать файлы на так называемую виртуальную флешку, которая находится на сервере. Процедура максимально упрощена

и после первоначальной регистрации и настройки аккаунта (учётной записи) становится не сложнее обычного копирования файлов на флешку.

Для работы устанавливается небольшая программка и в вашем компьютере создаётся виртуальная папка. Если перекинуть файл в эту папку, то он автоматически копируется на сервер в ваш аккаунт. Соответственно, открыть файл можно из любого места с доступом в интернет, зайдя в свой аккаунт. Классическим представителем этого сервиса является DropBox.

А вот, если под рукой нет пакета Microsoft Office или другого похожего, то есть сервисы которые позволят не только перекидывать файлы, но и редактировать документы прямо в окне браузера, как будто вы это делаете в своём привычном Word или Excel. Эта технология получила название «Облака». Т.е. данные как бы летают в облаках, и не зависят от вашего местонахождения. Google даже сняли прикольный видеоролик, в котором уничтожают 25 ноутбуков различными способами: разбивают, сжигают, замораживают и чего только ещё ни делают, чтобы донести: с данными ничего не произойдёт!

На своём сайте я уже писал об одном таком сервисе SkyDrive от Microsoft, но существуют и другие, например Документы Google.

Делаем работу чужими руками

В интернете можно сделать чёрную работу чужими руками! Если у вас есть работа, которую делать лень, и вы её постоянно откладываете, то лучше делегировать её выполнение так называемым фрилансерам. Биржи работы фриланса собирают у себя тысячи желающих сделать работу за небольшую плату. Какую работу можно делегировать? Практически любую, не требующую

вашего личного присутствия. Например, это может быть создание сайта, размещение объявлений, написание продающих текстов, перевод текстов, придумывание названий, слоганов, логотипов компании, программирование, рефераты, дипломы, разработка дизайна чего угодно. В общем, желающие найдутся на любую работу. Оплата находится в различных пределах – от символической до очень высокой, в зависимости от профессионализма и амбиций исполнителя. Популярные биржи фриланса: http://www.free-lance.ru, http://freelance.ru/, http://web-lancer.ru, http://workzilla.ru. Кстати, можете и сами там подзаработать деньжат в свободное время.

Покупаем вещи с БОЛЬШИМИ скидками

С помощью интернета можно здорово экономить на покупке вещей и услуг. Существуют сотни сервисов по продаже купонов скидок. Необходимо лишь походить по таким сайтам и выбрать интересующее предложение. Это как ярмарка распродажа, где продают что угодно. Можно выгодно купить путёвку на отдых, услуги, например по макияжу или массажу, скидку 50% на романтический ужин в ресторане, или просто вещи со скидками. Механизм действия простой:

- выбираете свой город и интересующее предложение
- читаете описание и механизм получения товара или услуги
- оплачиваете купон
- распечатываете его и идёте получать желанное

Самые популярные сервисы: Biglion, Выгода.Ру, Групон. Немного особняком стоит сервис КупонГид, который объединил в себе десятки других сервисов купонов. Вам не надо будет

регистрироваться на каждом из них и перебирать предложения на каждом сайте отдельно. Просто регистрируетесь на КупонГид и получаете всё в одном флаконе.

Такие купоны скидок даже получили своё название – групон, от названия американского сервиса Groupon, который первый распространил идею коллективных скидок в 2008 году. Кажется, это слово даже включили в словарь, а если нет, то скоро точно включат.

Переводим тексты ONLINE

Для перевода текстов уже давно не нужно покупать и устанавливать громоздкие программы типа ПРОМТ, достаточно зайти на один из онлайн-сервисов по переводу, вставить в окошко свой текст и нажать кнопку, всё! Самые популярные переводчики: Google Translate, Яндекс-Перевод, Промт-онлайн. Можно найти и другие через поиск. Обычно поддерживается 7-9 языков перевода в обе стороны, это: английский, испанский, итальянский, немецкий, португальский, русский, украинский, турецкий и французский. Но Google знает намного больше – десятки различных языков и позволяет переводить не только тексты, но и иноязычные сайты. Чтобы перевести сайт достаточно просто вставить в окно перевода ссылку на страницу и вы получите такую же страницу, но уже переведённую на нужный язык.

Удалённая помощь от друзей

С помощью интернета можно получить помощь по компьютерным вопросам от своих друзей. Достаточно установить на обоих компьютерах программу TeamViewer и запустить её. Пользоваться программой очень просто. В результате помощник сможет

управлять вашим компьютером так, как будто он сам за ним сидит. Он будет видеть на мониторе то, что видите вы, и сможет управлять вашей мышкой и клавиатурой. На первый взгляд смотрится необычно и даже смешно – мышка сама двигается по экрану, программы сами открываются и вообще происходит какая-то движуха ☺

Получается очень удобно, если самостоятельно справится с проблемой не выходит. Не нужно никому ехать к вам домой, нужен только интернет. Но если компьютер вообще не загружается, то удалённая помощь невозможна, потому что интернет ещё не подключён и программа TeamViewer не запущена. А в остальных 90% случаев можно решить проблему с места.

Как пользоваться интернетом бесплатно и заработать на этом

Пользоваться интернетом бесплатно или условно бесплатно можно тремя способами:

- Бесплатный коммутируемый доступ
- Бесплатный Wi-Fi
- Самоокупаемый интернет

Бесплатный коммутируемый доступ годится разве что для чтения электронной почты и общения с помощью интернет-мессенджеров таких как QIP и Mail.ru Агент. Но такой способ существует и о нём надо упомянуть. Работает это с помощью модема через телефонную линию. Такую услугу можно найти во многих городах, а в Москве сервис http://www.internetbesplatno.ru/ даже платит за то, что вы пользуетесь их интернетом бесплатно! Платить только прийдётся за телефон. Так что этот метод подойдёт весьма

ограниченному кругу людей. Остановимся на том, что это способ существует.

Бесплатный Wi-Fi сегодня можно найти в любом городе, в самых разнообразных местах: в барах, в местах отдыха, в парках, в торговых центрах. Если в некоторых заведениях вас попросят сделать минимальный заказ или купить хотя бы чашечку кофе, то в других - это полностью бесплатно. Особенно приятно когда бесплатный интернет работает где-нибудь просто на лавочке ☺

Благодаря бесплатному Wi-Fi в моду входит работа вне дома. Фрилансеры, программисты, интернет-предприниматели предпочитают выбираться из надоевшей домашней обстановки куда-нибудь подальше и работают там. Согласитесь, заманчивая перспектива работать там, где тебе нравится.

Сегодня Wi-Fi настолько распространён, что практически в любой квартире многоэтажного жилого дома можно поймать чью-то сетку, подключиться к ней (если не просит пароль) и пользоваться интернетом бесплатно. Я, конечно, не могу рекомендовать этот способ, да и не надёжно это. А вот скооперироваться с соседом и пользоваться одним интернетом на двоих в пол цены – вполне рабочее предложение. Многие так и делают.

Кабельным интернетом бесплатно пользоваться не получится, но можно вывести его на самоокупаемость. Т.е. надо заработать в интернете столько же или больше, чем стоит месячная абонплата.

Есть простые методы, которые позволят каждому заработать несчастных 100-200 рублей в месяц практически не прилагая усилий. А если понравится, то можно будет двигаться дальше в этом направлении.

Для новичков: платные опросы. Заработок заключается в заполнении анкет-опросников за деньги. Компании тратят

баснословные деньги на маркетинговые исследования и готовы платить за ответы на вопросы. В интернете мы и так частенько заполняем анкеты бесплатно, так почему же за это не получать деньги? Требуется всего лишь зарегистрироваться на сайтах специализирующихся на платных и опросах и ждать когда к вам начнут поступать предложения. Во время регистрации вы указываете на какие тематики согласны проходить опросы. Темы очень разные, и нужно выбирать действительно те, в которых более-менее разбираетесь. Тогда и вам будет приятно и пользу принесёте. Если приглашения пройти опрос будут приходить всего лишь раз в неделю, то этого хватит чтобы окупить интернет, а по времени один опрос займёт от 10 мин до получаса.

Поскольку компаний которые проводят платные опросы сотни, то имеет смысл их искать не через поиск, а на сайтах-агрегаторах, например http://www.platnyeoprosy.ru/ Там вы сможете выбрать подходящую компанию и зарегистрироваться. Для продвинутых существует платный сервис http://www.surveysguide.com, на котором за небольшую плату от 10$ до 13$ можно получить доступ к базе из сотен компаний.

Я не буду советовать зарабатывать на интернет с помощью кликов, партнёрок, написания статей, угадывания картинок или платного общения на форумах. Все они требуют затрат времени или глубокого вникания в вопрос.

Для продвинутых или желающих действительно зарабатывать в интернете прямая дорога в бесплатную школу онлайн-бизнеса «Твой Старт». Всего за 3 недели вам расскажут как создать сайт и зарабатывать на нём. Если тема интересна, то уверен что вы будете в восторге от полученных навыков и заряженной позитивом атмосферы! Советую хотя бы записаться на курс и послушать гуру интернет-бизнеса, а там уже понятно будет – подходит вам или нет.

Насколько я знаю, дополнительный источник денег (а для некоторых основной) никому ещё не помешал ☺

Как не остаться без штанов

В этом разделе я хочу поведать о безопасности в сети Интернет. О том как можно легко потерять все свои кровно нажитые электронные деньги или важные данные. Ведь не секрет, что уязвимость электронных денег на порядок выше обычных бумажных, которые лежат в кошельке или даже тех, которые лежат на депозите в банке. Злоумышленникам потребуется не больше одной минуты, чтобы прихватить все деньжата с собой, как только у них будет вся необходимая информация.

Если вы думаете, что у вас нечего взять, то вы глубоко ошибаетесь! Хакеры никуда не спешат и действуют по принципу – возьму своё когда будет чё брать. Они закидывают вирус-троян или вы его сами где-то цепляете и начинается слежка! Если у вас нечего взять, но ничего не происходит, хакер себя никак не проявляет и вы живёте ни о чём не подозревая. Читаете страшные истории о потерянных деньгах, и думаете что беда обойдёт стороной. Но как только на вашем кошельке появляется n-ная сумма, как бац! И ваше очко уходит в зрительный зал… Поймите, хакерство это целый бизнес с начальниками-хакерами и подчинёнными. Сидит целая комната мальчиков, которые делают чёрную работу: взламывают почтовые ящики, следят за кошельками, выжидают.

Вопрос не в том взломают вас или нет, вопрос только в том – когда вас взломают. Очень многие не сознательно относятся к своей безопасности. Взламывают всех и всегда с разными целями. Чем больше людей приходит в интернет, тем больше становится лакомых кусочков. И людей, которые хотят всё это забрать, становится всё больше, для совершенно различных целей. Кому то

нужны банально деньги, а другому конфиденциальная информация или пароли доступа. Проблема стара как мир, но есть решение, которое работает по принципу: лучше сделать прививку от болезней, чем потом бороться с последствиями.

Последствия хоть какой-нибудь мошеннической схемы, я думаю, многие уже прочувствовали на своей шкуре. Взлом электронных денег, почты, социальных сетей, скайпа. Любой взлом это не только шок и порушенные планы, а ещё чувство потерянности и неуверенности в завтрашнем дне. И самое главное – контроль вернуть не всегда удаётся. Если неправильно вести дела, то вернуть контроль будет очень сложно. Доказать администрации какого-то сервиса что хозяином являетесь именно вы очень сложно.

Многие знают про это, и про вещи которые нужно и не нужно делать, но откладывают годами, пока что-то не случится. Мало знать, надо ещё внедрять. Итак, поговорим об основных ошибках не только новичков, но и заядлых интернет-пользователей.

Безопасные пароли

Тема избитая до посинения, но до сих пор является очень слабым звеном в безопасности. Наверное, только на заборах не пишут что использовать нужно сложные пароли, особенно для аккаунтов так или иначе связанных с деньгами. Понимаю, что велик соблазн в качестве пароля вбить свой день рождения или день свадьбы. Но это категорически запрещено! Потому что любые цифровые пароли взламываются элементарно методом подбора за несколько суток.

Что такое сложный пароль?

Сложный пароль должен быть не меньше 8 символов, содержать большие и маленькие буквы, цифры и спецсимволы (значки ~!@$ %#}{()”). Добавлением в пароль любого из этих элементов, вы

усложняете его подбор в тысячи раз! В идеале пароль должен быть бессмысленным, т.е. он не должен напоминать какое-то слово.

Где хранить пароли?

Сложный пароль не будет иметь никакого смысла, если он будет записан в тестовом файле «пароли.txt» ☺ Любой вирус обнаружит такой файл, и будет уже не важно какой сложности пароль. А если не обнаружит, то даст доступ хакеру, который найдёт файл без проблем. Поэтому пароли точно нельзя хранить в текстовых файлах или в любых других форматах документов. А если храните, то этот файл точно не должен находиться на компьютере, но это тоже плохо. Позволительно хранить пароли в заархивированном и запароленном текстовом файле, а ещё лучше в записной книжке (настоящей бумажной). Но и тут есть косяк. Специальные хакерские программы «кейлоггеры» умеют записывать все нажатия кнопок с клавиатуры, после чего несложно проанализировать лог-файл чтобы достать оттуда пароли.

Также, нельзя сохранять пароли с помощью менеджеров паролей браузеров. Это когда браузер сам предлагает сохранить введённый пароль. Удобно конечно, но не безопасно. А при поломке компьютера все ваши пароли улетят в трубу.

Выход из ситуации

Кажется, что получается безвыходная ситуация – какой бы сложный ни был пароль, и где бы мы его ни хранили, всё равно при желании хакеры смогут его найти! Но выход есть, это программа RoboForm, или ей подобные. RoboForm встраивается во все популярные браузеры (Internet Explorer, Chrome, Opera, FireFox и другие) и автоматизирует процесс заполнения форм. С этой чудо-программкой вам больше не прийдётся париться с паролями, искать их в незащищённых текстовых файлах или в записной книжке. Программа избавляет вас от запоминания паролей (она

хранит их в специальных пасс-картах), имеет интуитивно понятный интерфейс и плюс отправляет на сервер резервные копии. Т. е. если вы с другого компьютера запустили эту программу, то тут же можете стать владельцем всё тех же паролей, синхронизировав их с компьютером.

Для доступа ко всем паролям нужен только один «Главный пароль», который нужно помнить. Программы-кейлоггеры не смогут считать пароль, потому что RoboForm сам вводит его в поле, без участия клавиатуры. А чтобы кейлоггеры не смогли считать главный пароль предусмотрена виртуальная клавиатура.

Правда, программа платная, но стоит копейки – около 9.95$ за год пользования. Даётся тестовый 30-ти дневный период, после которого я не смог отказаться от предложения приобрести продукт, потому что очень удобно. Получается, сделал рекламу для RoboForm, но что же поделаешь, как-то надо рассказывать о полезных вещах ☺ Ради справедливости приведу ещё один похожий сервис LastPass. Я лично им не пользовался, можете поставить и сравнить с RoboForm.

Анекдот в тему: *У BMW есть три подушки безопасности, а у Лады – три иконки.* Выбирайте себе BMW и спите спокойно.

Электронная почта

Вторым важным элементом в цепочке вашей безопасности является электронная почта. Не секрет, что во многих сервисах есть услуга «Напомнить пароль», который приходит на ваш ящик. Поэтому злоумышленнику достаточно иметь доступ к ящику, чтобы завладеть всеми остальными аккаунтами.

Обычная электронная почта плохо защищена от взлома. Есть куча вариантов как взломать электронную почту. Есть прямо инструкция

для хакеров. Раньше малолетки на спор проводили такие системы взлома почты. И у таких дилетантов-школьников всё получалось в 98-2000 годы. Сегодня популярные почтовые сервисы работают над улучшением безопасности электронной почты, но не все пользуются новыми возможностями.

Популярные почтовые службы типа Mail.ru, Яндекс, Рамблер ввели привязку ящика к номеру мобильного телефона, как способ защититься. Это позволяет вернуть доступ к своей почте, но не более того. Если вы поздно заметили что не можете войти в свой аккаунт, то восстановление пароля может уже не принести много радости.

Особняком стоит почтовый сервис Gmail, в котором разработчики Google внедрили алгоритм двухэтапной аутентификации. По умолчанию она выключена, и включается в настройках почтового ящика. Рекомендую это сделать обязательно! Работает двухэтапная аутентификация следующим образом: при первом заходе с неизвестного компьютера, кроме пароля, требуется ввести код, который прийдёт на телефон по SMS. Далее код прийдётся подтверждать каждые 30 дней. Если вы потеряете или не сможете воспользоваться своим телефоном, например за границей, то на этот случай существует список резервных кодов. Данный список нужно распечатать и носить с собой. Сломать такую связку очень сложно и слишком дорого чтобы вами занимались. Только если вы очень большая шишка, и вами захотят заниматься, подделывать сим-карту и перехватывать сообщения. Gmail с двухэтапной аутентификацией – это хорошо, а без неё – не сильно лучше чем другая почта.

Ещё пару моментов, касающиеся электронной почты. Во-первых, если вы используете сбор почты с помощью почтовых программ, например Microsoft Outlook, The Bat! или Mozilla Thunderbird, то

настоятельно рекомендую включить в настройках вашего почтового аккаунта защищённое соединение HTTPS (на любом популярном сервисе). Дело в том, что по незащищённому протоколу HTTP ваши логин и пароль передаются в незашифрованном виде, а это брешь в безопасности. Установите защищённое соединение в настройках почтового аккаунта и обязательно в настройках почтовой программы. Если этого не сделать, то аутентификация будет и дальше происходить в незащищённом режиме или почта вообще перестанет работать. Для усиленной безопасности лучше вообще отключать возможность сбора почты почтовыми программами (отключить в настройках протокол POP3, если такое есть), если вы ими не пользуетесь.

Кстати, если у вас есть несколько почтовых ящиков и вы всё ещё не пользуетесь одной из почтовых программ (Microsoft Outlook, The Bat!, Mozilla Thunderbird), то настоятельно рекомендую начать ими пользоваться. Это сильно упрощает и ускоряет работу с корреспонденцией, хоть и немного снижает уровень безопасности. Рекомендую почтовик The Bat! или Mozilla Thunderbird.

Во-вторых, уделите внимание дополнительному почтовому ящику, если вы его указываете в настройках почты. Этот ящик может использоваться для восстановления забытого пароля. Соответственно, если злоумышленник узнает об этом ящике, а он будет хуже защищён чем основной, то какой в нём смысл?

Стандартные модели взлома

За время существования интернета было придумано множество схем мошенничества. Каждый выдумывает свои варианты, но стандартные модели примерно одинаковы.

Фишинг для взлома почты

Самый простой, самый быстрый и действенный метод который применяют для взлома почты – это фишинг. Это когда фальшивый сайт имитирует почтовый сервис, пытаясь ввести вас в заблуждение. Например присылают очень похожее письмо на Google с текстом примерного содержания: «Вас приветствует команда Google! Мы заметили что ваш аккаунт был практически взломан, и как можно быстрее требуется подтвердить свои права на почтовый ящик, поэтому введите свой пароль…» Причём писать будут очень натурально, от души. Вы заходите по ссылке и видите привычный интерфейс Google, но это ни разу не страница Google. Сайт будет очень похож на оригинал, но если посмотреть на адресную строку браузера (это первое что нужно проверять), то сразу видно, что сайт называется не «google.com», а как-нибудь типа «goggle.com», «goooggle.com» или «goooggl.com» (все написаны с ошибкой). Будет похоже, но не правильно. Вы просто вводите свой пароль для взломщика.

Этого достаточно, чтобы распознать мошенника, но для большей уверенности можно поискать текст присланного письма в интернете. Просто введите часть текста, там где нет вашего имени, в Google или Яндекс, и посмотрите на похожие сообщения. Обычно сразу всплывают сообщения с форумов с похожими письмами.

Могут быть вариации на тему, например кто-то рассказывает что «узнал как взломать чужую почту» и пишет, что надо прислать письмо в специальном формате на специальный «засекреченный» ящик. В письме надо указать ящик от своего пароля, ящик для взлома, и свой номер кошелька!

НЕ ВЕДИТЕСЬ! Никогда и никому не высылайте свой пароль!

Волшебные кошельки

Очень изощрённая фишка, на которой наварились мошенники на заре электронных денег, но как ни странно, схема работает и по сей день. Рассчитана на исконно русскую жажду халявы. Как правило, появляется объявление, сообщение на форуме или приходит письмо по электронной почте от некого «доброжелателя», который типа работал в WebMoney или Яндекс деньгах, а его там обидели. И вот теперь он хочет разорить систему, и знает как это сделать! Оказывается, он узнал номера «волшебных кошельков», которые удваивают или утраивают присланные на них деньги. Предлагается отправить какую-то сумму, и она вернётся вам в увеличенном размере! Расписывается всё очень правдоподобно, от души. Не верьте никогда таким сказкам! Это чисто-мошенническая схема, которая обогатит только аффтора.

Сюда же можно отнести программы, которые «генерируют» деньги на ваших счетах. Это не более чем вирусы, которые украдут все ваши деньги.

Обмани лохотронщика

Потом мошенники пошли дальше, и стали появляться сообщения от, якобы, попавшихся на «волшебные кошельки» и узнавшие секрет как разорить их владельцев. Предлагается действовать по особому алгоритму, отправлять только конкретную сумму, не более двух раз и только в полную луну и тому подобная чушь. Я думаю суть вы поняли, никогда не введитесь на подобные сообщения.

Пирамиды

То же что и в реальной жизни, типа «МММ». Вкладываете деньги под бешенный процент – до 1000% в месяц или 300% в день (и такое видел). Чем больше процент и сумма депозита – тем выше шанс не получить обратно ни копейки. Никогда не вкладывайте деньги в пирамиды, как бы хвалебно они не расхваливали себя. В некоторых случаях и вправду можно «навариться», но риск очень велик, лучше купите лотерейный билет. В худшем случае ваш кошелёк будет заблокирован только за то, что вы приняли участие в пирамиде.

Другие способы обмана

Если вам предлагают купить конфискованный товар по супер выгодным ценам, если кто-то представляется вашим знакомым и просит срочно выслать деньги (аккаунт знакомого могли взломать), если вас просят прислать деньги на доставку, якобы, выигранного приза или за возможность устроиться на очень классную работу – не верьте! В крайнем случае – тщательно проверяйте, звоните, узнавайте.

Включайте здравый смысл!

Защита электронных кошельков

В нашем сегменте интернета распространены системы электронных денег WebMoney и Яндекс.Деньги. Это основные кошельки, которые имеют большинство. Предлагаю вам выделиться из этого большинства и задуматься о безопасности. С каждым днём в интернет приходит всё большее число людей, и всё большее число мошенников.

Безопасность кошелька Яндекс.Деньги

По умолчанию, для доступа к кошельку требуется просто ввести платёжный пароль и всё. Это самый небезопасный способ. Поэтому рекомендую всем переходить на усиленную авторизацию через таблицу кодов. Усиленная авторизация через таблицу – это воплощение технологии одноразовых паролей, т.е. для каждой операции требуется вводить новый пароль. Это надёжный способ защитить свой кошелёк.

Работает это следующим образом: вы распечатываете специальную таблицу кодов с координатами, похожую на шахматную доску. Затем, при совершении операций со счётом, Яндекс просит ввести числа в клеточках по указанным координатам, как в морском бое, например: A5-B2-C7. Это совсем не сложно. Количество использованных комбинаций для одной таблицы ограничено и составляет 55 - для распечатанной таблицы и 100, если вы закажете специальную пластиковую карту с изображённой таблицей.

Второй механизм усиленной авторизации – это электронный токен. Специальное устройство в виде пластиковой карточки с небольшим экраном и кнопкой. Для совершения операций по счёту надо будет вводить пин-код. Чтобы его получить надо просто нажать на кнопку и ввести пин-код с экрана карточки. Электронный токен работает от батарейки, которой хватает на 4 года. И конечно же он платный, на данный момент стоит 739 рублей.

Если вы решили перейти на усиленную авторизацию, то только с помощью таких таблиц, карт и токенов вы сможете проводить платежи. Обратного пути нет, т.е. перейти на использование обычного платёжного пароля будет нельзя. Кстати, переход на усиленную авторизацию стоит 30 рублей. Это единоразовый

платёж. Потом можно будет менять способ авторизации – через таблицу или через электронный токен.

В Яндекс деньгах ещё есть привязка к номеру телефона, которую нужно обязательно активировать. Если вы ранее привязывали телефонный номер к почтовому ящику, то это не значит что он автоматически привяжется к кошельку. Эту операцию прийдётся проделать вручную. Привязка к номеру телефона позволит восстановить потерянный доступ к кошельку.

Обязательно включите email-информирование по операциям с вашим счётом и, по желанию, SMS-информирование. Последняя услуга платная – 20 рублей в месяц. Таким образом, вы сразу узнаете о несанкционированных операциях со счётом.

Безопасность кошелька WebMoney

Программа WebMoney Keeper Classic умеет анализировать положение вещей и сообщать о дырах в безопасности. В идеале в самом низу окна программы должно быть написано «Нет замечаний по настройкам безопасности».

Для лучшей безопасности используйте активацию WebMoney Keeper Classic только с помощью SMS на телефон. Активировать WM необходимо один раз на каждом новом компьютере.

Для пользователей WM Keeper Light отключите использование сертификатов, используйте только вход с помощью SMS-подтверждения. А заводить WM Keeper Mini вообще опасно, лучше им не пользоваться.

Используйте обязательно SMS-подтверждение операций с кошельками. Даже если кто-то получит доступ к вашим кошелькам, то не сможет без телефона перевести деньги.

Включите блокировку по IP-адресу. Это позволит ограничить вход в систему только под вашим IP-адресом. IP-адрес это уникальный идентификатор вашего компьютера или провайдера в интернете. Если кто-то попытается войти в аккаунт с другого IP-адреса, то ваш WMID будет заблокирован. Для его разблокировки используется email или телефон. Настоятельно рекомендую использовать разблокировку ТОЛЬКО по телефону.

Всё что можно разблокировать или подтвердить с помощью электронной почты является ненадёжным по определению!

Для продвинутых – используйте сервис E-num Storage. Это улучшенная система входа в WM Keeper, которая позволяет не хранить файл ключей на компьютере. В этом случае вы устанавливаете на свой телефон программу E-num, которая генерирует пин-коды для входа в WM Keeper Classic. Но учтите, что если вы используете WM Keeper Mini, то E-num вряд ли поможет.

Если не используете E-num, то хотя бы храните ключи на отдельной флешке, которую будете подключать только во время совершения операций с кошельками.

Всегда используйте последнюю «залатанную» версию WM Keeper Classic. И дам бесплатный совет – не храните большие суммы в электронных кошельках. Как можно быстрее тратьте или выводите деньги.

Если вы не следовали моим рекомендациям и вас всё-таки взломали, то восстановить право владения своим WMID можно только имея персональный аттестат. Иначе восстановить доступ к кошельку будет очень сложно. Если вы не аттестировались, то кошелёк принадлежит анониму. Им может быть любой человек с улицы. Доказать что это именно ваш кошелёк будет крайне сложно. Можно, но сложно, намного сложнее чем с персональным аттестатом. Если ваш кошелёк всё-таки взломали и вы это вовремя

заметили, то можно написать или лучше позвонить в службу поддержки чтобы заблокировать кошелёк. Как сделать персональный аттестат написано на сайте WebMoney. Как правило эта процедура стоит 5-10$. С персональным аттестатом у WMID изменится статус и ему будут больше доверять другие люди. Также это пропускной билет во многие места, этакая своеобразная этика электронной коммерции.

Персональная защита

Если вы проделали все вышеперечисленные операции для обеспечения своей электронной безопасности, то осталось только уделить внимание персональной защите вашего компьютера.

Вопрос персональной защиты компьютера это тема отдельной книги, поэтому я просто обозначу основные моменты, которые обязательно должны быть.

Всегда используйте хороший антивирус. Хорошим можно считать любой платный антивирус, например Dr.Web или Антивирус Касперского. Из бесплатных или условно бесплатных антивирусов можно взять AVG или Avast!

Важно понимать, что насколько бы ни был хорош антивирус, ни один из них не может гарантировать 100% безопасности! Тем не менее, очень важно иметь работающий антивирус с последними базами вирусов, и лучше если он будет платный. Вы можете ни за что не платить, использовать только бесплатные программы, но антивирус лучше купить. В этом случае у вас не будет болеть голова «свежие ли базы» и антивирусная безопасность компьютера будет на максимально возможном уровне.

Вторым важным звеном в обеспечении персональной безопасности является фаервол (он же брандмауэр). Это

межсетевой экран, который защищает наш компьютер от вторжений из вне и от утечки информации в сеть. Вообще, слово firewall в переводе с английского означает «стена от огня», а брандмауэр это тоже самое, только на немецком.

Неплохой брандмауэр уже встроен в Microsoft Windows. Но по нормальному, это должен быть отдельный программный продукт, например Outpost Firewall, Comodo Firewall или Norton Internet Security. Также, почти все популярные антивирусы имеют встроенный межсетевой экран. Если не используете сторонние программы, то хотя бы не отключайте встроенный.

Всегда устанавливайте последние обновления операционной системы. Особенно это касается пользователей пиратских версий, которые не обновляются автоматически.

Заключение

В этой книге мы познакомились с необузданным миром интернета. Вы узнали какие полезные сервисы скрывает в себе интернет. Наверняка о некоторых вы уже знали ранее, но не использовали их выгоды в повседневной жизни. Используйте возможности интернет по максимуму! Находите новые сервисы, которые будут полезны именно для вас.

Вы узнали, что безопасность в интернете – это далеко не последнее, о чём нужно задумываться. Особенно, если работаете с электронными деньгами. Предупреждён – НЕ значит защищён. Обязательно применяйте полученные рекомендации на практике, не откладывая в папку Downloads ;)

Спасибо Вам за то, что прочитали мою мини-книгу. Мне очень важно узнать Ваше мнение о книге. Будьте добры, и напишите коротенький отзыв по этому адресу.

В одной мини-книге невозможно рассказать всё что хотелось бы. Почаще заходите на мой сайт IT-LIKE.RU и вы узнаете намного больше интересного!

Всего доброго, удачи Вам и до новых встреч на страницах моего сайта http://**it-like.**ru и в письмах рассылки!