Лис будет печатать в полу-деловом стиле больше по причине для восприятия этой работы.

**Запомните – это для тех, кто не знает тонкости, для понимания и внешний обзор для поколения Z и А.**

О чём пойдёт это скромная работа – которая нацелена на азы а не углубление и подробное изучение:

Во первых - Об ответственности тех, кто имеет псевдореальный/внешний/белый адрес, и о заблуждениях связанные с этим фактом.

Во вторых – об средствах которые помогают защитить себя (хотя и поверхностно).

В третьих – Работа обзорная связанная с возможность иначе посмотреть на ситуацию, но не рассматривать её как истину а скорее как сторону правды, которая может быть у каждого своя.

***Вместо Введения***

Каждый кто имеет доступ к интернету рассматривает его как средство развлечения (игры, стафф, и даже творчество), возможность удовлетворить свои прихоти. Остальная часть приходит на работу и зарабатывает там. Будь это ф**рила́нсер**ство или же серьёзная разработка связанная с программы или иным обеспечением даже аппаратным.

Теперь давайте рассмотрит это более детально, здесь не будет идти речь о начале всех начал и о том откуда пошло понятие локальность (локальные сети тому не исключения). Локальная сеть изначально это местная сеть и та сеть которая объединяет хотя бы одно устройство с другим, не важно будет ли это компьютер или отдельное устройство главное в локальной сети это «Основной шлюз» к которому идёт подключение, обычно оно может быть и ДНС адресом устройства к которому идёт подключением связь Сервер – Клиент. Таким образом Сервер даёт возможность подключиться к себе а клиент принять сигнал, так это работает сейчас. Раньше было проще и сложнее одновременно можно было присвоить разные адреса но соблюдать условие с одинаковым адресом маски и всё, два компьютера работают без проблем с друг другом.

До введения DHCP это было скажем так проблемой где каждый клиент доступен для другого клиента главное среди них похожесть хотя бы в чём-то ну и один провод, для знающих сеть можно объединить сетевой картой PCI с двумя отверстиями (вход и выход – rj-45 мама и мама) и создать свой уголок на столько компьютеров, насколько позволяет адресация.

Проблема начиналась с устройства который был выходом во внешнюю сеть (интернет), да для безопасности можно установить Мост который позволит напрямую соединяться с другой организацией но увы без доступа во внешний интернет даже это сложно добиться.

На это устройство устанавливают защиту и фильтры, отключают порты (если нужно), и тогда офисный планктон пытаются найти возможность обойти эти ограничения. А теперь усложним – представьте что вы за компьютером в офисе с отключёнными usb устройствами которые контролирует касперский , нет доступа к биосу и сам системный блок опечатан а реестр контролируется тем же Касперским который возвращает изначальный параметр как только вы закрываете этот реестр. Учётная запись конечно же – не Администратор. Не забывайте, что вас ещё и снимают на запись. Наказание будет незамедлительное, т.к. при приёме на работу вы подписывали бумаги о неразглашении.

Вот такие сложности познаются в работе на тех, кто обеспечивает безопасность не говоря уже об отсутствии утечек данных со стороны, если кто-то выше вас по праву не захочет.

Представили, а теперь ситуацию перевернём и приземлим.

***Основная часть***

На основе офиса и продолжим, тот кто имеет пароль от вашей безопасности является ваш провайдер он контролирует и записывает все данные какие только может, для обеспечения защиты ещё лучше, как они считают (пользователи) были разработаны разные стандарты и сертификации которая в какой то мере работают. Беда в том, все эти стандартны и нормы иногда меняются, а об изменениях и прогрессе вы можете не узнать пока в одночасье зайдя на любимый вами сайт, вы не обнаружите, что он небезопасен. Кто вам это скажет, да всё та же безопасность даже в виде вашего браузера. Как эти стандарты могут, не работать потому что разработками занимаются не вы и даже не маркетологи а лица в области инженерии (да даже социальная инженерия это инженерия), а в данном случае Инженеры-Программисты ( на самом деле их по разному называют, ну помните их ещё обязывают изучать цифровую экономику и менеджмент). Сертификация как и стандарты, действительно облегчает жизнь как ещё мы узнаем без этих норм, что зайдя на сайт который не имеет приставки http(s), мы зашли на безопасный сайт который подписан, кто ещё скажет, что неподписанный это ложный сайт, как не эти стандарты. Вы думаете, что это ирония – и будете правы.

Приближаясь к ситуации, подведём под реальный пример.

Вы купили компьютер всё настроили и у вас даже есть тот, кто может обеспечить вам выход в интернет. Вы просите компанию дать вам интернет, они вам дают и о чудо вы видите возможность подключить услугу под названием «псевдореальный/внешний/белый адрес» (название может быть и иное), и с желанием поднять свой собственный сервис соглашаетесь. Вы платите деньги за то, что бы компания дала вам адрес который виден во внешнем интернете и с этого момента, вся безопасность (если ваш компьютер действительно виден из интернета) ложится на вас. Вы обеспечиваете сохранность своих данных, вы стараетесь чтобы ваш компьютер не стал этаким прокси через который будут устраивать нападки на других (да да такое тоже возможно благодаря [Socks5Systemz](https://www.bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey) ( с 2016 года), и вы замешаны во взломах и проблемах других. Осталось доказать, что вы это сделали как? Да очень просто, есть IP адрес и вы по логам компании владеете этим компьютером. Вы будете говорить, что не знали, что вас подставили и всего лишь из за того, что вы забыли обеспечить сохранность своих данных и прошли по неизвестной ссылке на неизвестный сайт.

Если без запугивания, то обеспечение безопасности вашего рабочего (и не только) места , это ваша прямая обязанность просто потому, что в договоре прописан пунктик цитирую:

«Ни одна из Сторон ни при каких обстоятельствах не несет никакой ответственности перед другой Стороной за остановку производства, утраченный бизнес, потерю данных, упущенную выгоду или любые другие косвенные потери или их последствия, в том числе возникшие в результате перерывов в оказании Услуг, вне зависимости от того, могла или нет Сторона предвидеть возможность таких потерь в конкретной ситуации» (формулировка может быть и иной), и это входят в обязанность вас, а их лишь предоставить (и то не всегда) услугу в оплаченный срок.

Тот кто думает иначе прав, до подключения услуги. Вы потенциальное место, для возможностей других в том числе и попытаться добраться до информации которая другим кажется малодоступной и ненужной. Поэтому на безопасность платят деньги соблюдая при этом осторожность и внимательность не только к себе, но и окружающим.

Вы думаете, что это развлечение, а другие получают за это деньги. Вы думаете, что в безопасности, но на деле всего лишь мишень думающая, что повезёт с оборудованием не дороже стоимости тарифа. С большими возможностями и большая ответственность, за которую иногда не то, что можно но и нужно платить иногда не малые деньги. Вы хотите бизнес который приносит вам по 100000 р в месяц, просто как пассивный доход, а сколько вы готовы отдать за этот доход если на кону будет, что – то более весомое или всё лишь будете заблуждаться, что он никому не нужен при внешнем доступе.

***Послесловие***

Работа получилась вольной, пожалуй без эмоций не обошлось, но может быть и к лучшему, ибо она не претендует на популярность или на открытие истинны.

А касательно защиты:

Если у вас есть хороший не дешевле 10к роутер, с актуальной прошивкой и прочим всегда в зоне риска будет информация не извне а снаружи, сайты письма и прочее, за это стоит беспокоиться особенно учитывая данные которые вы храните извне (на облаке), чем больше стоит ваша работа, тем больше к ней интерес. Чем выше популярность, тем больше конкурентов которые захотят унизить вас или дискредитировать. Может быть это вас не коснётся, а может не стоит думать, что вы никому не нужны ведь количество тех кто хочет вас, говорит о том что ваши данные им известны, а их интерес иногда может быть просто заказом за которые заплатили иногда даже образно баночкой энергетика и интересом.

Всем спасибо.