Подготовка к потенциальным опасностям в Информационной сфере.

1. Как можно установить вредоносное ПО, даже не заметив. В современных реалиях Интернет-мошенничество имеет крайне много вариаций. Одна из них – это установка на ваш ПК вредоносное программное обеспечение. Нужно понимать, что такие ПО заносят нескольким путями – вы устанавливаете какую-то программу, при чем совершенно рабочую, но вместе с ней загружаются лишние программы, засоряя ваше место на ПК. Зачастую, это просто реклама сторонних сервисов, проникающая на ваш ПК, не неся какой-то вред вашей системе. Но также может и загрузиться вирус, который может нести огромный потенциальный вред вам и вашей системе. Здесь возможности разнятся вплоть до того, что мошенник может полноценно видеть все ваши данные, пароли через эту программу, даже если вы меняете их, то у мошенника они все равно видны. Это очень опасно и заметить это крайне тяжело, так как для этого нужно пользоваться качественным Антивирусом. Важно также скачивать файлы только с проверенных источников, так как не всегда Антивирус найдет очень сложный и скрытый вирус. О том, как его установить, вы узнаете в следующей записи.
2. Выбор антивируса на ваш ПК. В плане установки антивируса на ваш ПК также есть несколько вариантов. Вы в целом можете не устанавливать антивирус, а довериться встроенному и автоматическому антивирусу в операционной системе Windows. Этот антивирус сможет защитить Вас от базового стороннего ПО, но более современное и сложное он может спокойно пропустить и не заметить. Поэтому я все же бы рекомендовал остановиться на выборе какого-то одного из популярных антивирусов. По своему опыту я могу порекомендовать: Avast Free AntiVirus, Kaspersky Internet Security, Malwarebytes Premium, AVG Internet Security. Эти антивирусы показывают довольно надежную степень защиты, производительности удобности пользования. Но они все равно имеют свои отличия, и тут сложно выбрать, какой лучше конкретно. Также нужно учитывать, что некоторые Антивирусы платные, как Malwarebytes Premium. Но необязательно платное лучше бесплатного, так как Avast Free AntiVirus показывает тоже хорошую работу. Поэтому здесь я советую ознакомиться поподробнее с каждым антивирусом, узнать на что чаще вам нужна оперативная и правильная реакция антивируса и сделать свой выбор.
3. Установка антивируса. Разберём установку антивируса на примере Kaspersky Internet Security. Скачайте установочный файл Kaspersky Anti-Virus с сайта <https://www.kaspersky.ru/downloads/antivirus> или по ссылке из письма от интернет-магазина. Запустите установочный файл. Дождитесь окончания поиска новой версии программы или нажмите Пропустить. Внимательно прочитайте Лицензионное соглашение «Лаборатории Касперского». Если вы согласны со всеми пунктами, нажмите Принять. Если вы не примете условия Лицензионного соглашения, программа не будет установлена. Внимательно прочитайте Положение о Kaspersky Security Network. Если вы согласны со всеми его пунктами, нажмите Принять. Если вы не хотите принимать участие в Kaspersky Security Network, нажмите Отказаться. Нажмите Установить. Нажмите Да в окне Контроля учетных записей Windows. Дождитесь окончания установки. Убедитесь, что рекомендуемые параметры включены, и нажмите Применить. Нажмите Готово
4. Телефонные мошенники. Телефонное мошенничество продолжает существовать как один самых актуальных способов информационного мошенничества. При чём, много звонков происходят по довольно старым и банальным схемам. Но также способы в телефонном мошенничестве тоже стараются развиваться, чтобы попытаться вас обмануть. Так, в этих звонках вам говорят, чтобы вы восстановили свою кредитку; воспользоваться последним шансом перед судом; предлагают бесплатные подарки; звонок якобы из налоговой службы. Для того, чтобы не попасться в их ловушку, лучше незнакомый телефон сразу пробить в Интернете, чтобы увидеть возможные варианты. Но если вы ответили, ни за что не отвечайте на вопросы «да» или что-то в этом духе. Мошенники обязательно будут использовать это против вас, так что не забывайте записывать звонок, чтобы доказать, что вы говорили «да» в другом контексте.
5. Вирусы через точки доступа. Вирус использует технику перехвата DNS: она позволяет перенаправлять пользователя на вредоносный сайт при введении в браузере имени нормального ресурса. Злоумышленники осуществляют атаку за счёт встраивания в настройки заражённых роутеров своих адресов DNS-серверов. В случае с мобильными гаджетами на базе Android, после попадания пользователя на вредоносный сайт выводится предупреждение о том, что следует обновить браузер. Дальше начинается загрузка вредоносного приложения с именем chrome.apk. В момент установки зловред запрашивает различные разрешения. Целью мошенников является кража аккаунтов Google. В случае с устройствами под управлением iOS вирус пытается похитить логин и пароль от Apple ID, а также данные банковской карты жертвы. На персональных компьютерах вирус запускает майнинговый скрипт CoinHive, который добывает криптовалюту в пользу хакеров. Чтобы защитить сеть от зараженных компьютеров и мобильных устройств, необходимо использовать антивирусы со встроенным фаерволом и регулярно обновлять антивирусное программное обеспечение. Защищенные компьютеры могут блокировать навязчивые попытки вирусных атак в сети и будут препятствовать дальнейшему распространению вредоносного ПО через систему. Кроме того, если вы регулярно предоставляете сетевые пароли другим пользователям, рассмотрите возможность смены ваших паролей каждые несколько недель, чтобы уменьшить количество пользователей, которые могут свободно получать доступ к вашей сети WiFi.
6. Как выбрать антивирусы на телефоне. Телефон, безусловно, неотъемлемая часть нашей жизни. И, конечно, мошенники не могли пройти мимо такого шанса, как загрузить вирус на ваш телефон. Для этого также существует множество антивирусов. При чём, на телефонах как такового автоматического антивируса нет, поэтому советую выбрать антивирус из следующих мной рекомендованных: Avast Mobile Security, который имеет следующие достоинства: Чёрный список и блокировка входящих звонков с неизвестных номеров, Защита от опасных сайтов и фишинга, Брандмауэр, Проверка безопасности сети Wi‑Fi; AVG AntiVirus Free с достоинствами: Антивор: удалённая блокировка, очистка и поиск мобильного устройства, Чёрный список и блокировка входящих звонков с неизвестных номеров, Защита от опасных сайтов и фишинга, Проверка безопасности сети Wi Fi; Bitdefender Mobile Security с достоинствами: Антивор: удалённая блокировка, очистка и поиск мобильного устройства, Защита от опасных сайтов и фишинга, Защита приложений с помощью сканера отпечатков пальцев, Модуль для поиска потерянных умных часов.
7. Ваша информация в Интернете. Мы все вольно или невольно храним определенную информацию о себе в Интернете. При чём, зачастую это может быть очень важная информация, как данные банковской карточки. Также вы можете регистрироваться на какие-то Интернет-ресурсы через паспорт, данные которого хранятся на сервере компании, которой вы отослали их. Также в Интернете могут, например, найти вашу историю покупок, ваши интересы, после чего вашу учетную запись мошенники могут попытаться «скомпрометировать» для своих целей – например, писать вашим друзьям, прося деньги. Данные вашего браузера – cookie-файлы, журналы провайдера, плагины с данными являются ценными для рекламодателей. Именно от этого и зависит, какая вам будет высвечиваться реклама.

**ЧТО ДЕЛАТЬ В СЛУЧАЕ ПОПАДАНИЯ В УЛОВКУ ИНТЕРНЕТ-МОШЕННИЧЕСТВА.**

1. Что делать, если вас взломали? Часто пользователь понимает, что его взломали, по тому, что аккаунт вдруг перестает принимать его пароль. Во многих случаях угонщики первым делом его меняют, чтобы лишить жертву доступа к учетке и спокойно орудовать в ней. Но даже в такой ситуации вы можете многое сделать. Так что не паникуйте, а глубоко вдохните, выдохните — и действуйте. Важно сделать все быстро и правильно расставить приоритеты. Первым делом попробуйте сбросить пароль: есть шансы, что взломщики не успели отвязать от аккаунта вашу почту. Предупредите о взломе как можно больше знакомых: позвоните близким или напишите им в другом сервисе, опубликуйте сообщение о взломе в соцсетях, где вас читают. Зная о взломе, ваши друзья и родные, скорее всего, не поведутся на уловки мошенников, если те начнут рассылать им от вашего имени просьбы срочно перевести денег или что-то еще. Если мошенники добрались до аккаунта в платежной системе или к учетке была привязана кредитка, позвоните в банк или платежный сервис, чтобы тот заблокировал ваш аккаунт или карту. Просканируйте компьютер антивирусом, чтобы убедиться, что на нем нет зловредов, ворующих пароли от аккаунтов.
2. Что делать, если на ваш телефон был установлен вирус? Самым первым делом попробуйте проверку антивирусной программой, при чем, можно попробовать сделать проверку несколькими антивирусами. Если это не сработало, то постарайтесь минимизировать вред, которые причиняет вирус вашему андроид устройству и вашему кошельку: включите режим «В самолете», чтобы программы не имели доступ к интернету. Затем проверьте список приложений. Если среди них есть те, что вам неизвестны, или недавно установлены — удалите их. Также можно посмотреть в «Диспетчере приложений» телефона, какие из них работают активнее других и расходуют максимум трафика. далить вирус с телефона на базе Андроид достаточно быстро можно, если найти вредную программу в списке «администраторов» и отобрать у нее права. Для этого зайдите в меню «Настройки», выберите вкладку «Безопасность» и найдите подпункт с правами приложений. Также это меню может находиться в папке «Приложения». Удалить вирус с телефона на базе Андроид достаточно быстро можно, если найти вредную программу в списке «администраторов» и отобрать у нее права. Для этого зайдите в меню «Настройки», выберите вкладку «Безопасность» и найдите подпункт с правами приложений. Также это меню может находиться в папке «Приложения». \
3. Как удалить вирус с ПК? Пора открыть ваш антивирус или решение класса Internet Security и запустить сканирование на вирусы. Если вы используете Kaspersky Internet Security, выберите и нажмите на кнопку ‘Запустить проверку’ (Scan). Если нашелся вирус, им может быть затронуто несколько файлов. Выберите «удалить» (Delete) или «поместить в карантин» (Quarantine), чтобы избавиться от вируса. Заново запустите проверку компьютера, чтобы убедиться, что других угроз не осталось. Если нашлись другие угрозы, поместите их в карантин или удалите. Теперь, после удаления вируса, вы можете перезагрузить компьютер. Просто включите его, как обычно. «Безопасный режим» больше не нужен. Чтобы защитить компьютер от дальнейших атак, поменяйте все пароли на тот случай, если они скомпрометированы. Это обязательно, только если у вас есть причина считать, что ваши пароли украдены вредоносной программой, но перестраховаться не мешает в любом случае. Функционал вируса вы всегда можете проверить на веб-сайте производителя вашего антивируса или связавшись с их группой технической поддержки. Обновление ПО, браузера и операционной системы снизит риск эксплуатации киберпреступниками брешей в старом коде для установки вредоносных программ на вашем компьютере.
4. Что делать, если у вас украли деньги с банковской карточки? Чтобы отрезать мошенникам доступ к оставшимся деньгам на карте, ее нужно немедленно заблокировать, например, через мобильное приложение банка. Если оно у вас установлено и там есть опция блокировки карты, найдите в приложении нужную карту и выберите команду «Заблокировать». По закону банк обязан вернуть деньги, если вы выполнили два условия: Сообщили банку о краже денег с карты не позднее следующего дня после того, как банк уведомил вас о подозрительной операции. Не успеете — банк имеет право вам отказать. Не нарушали правила безопасности при использовании карты. В частности, не сообщали мошенникам данные карты, не хранили ПИН-код вместе с картой, не писали код на самой карте, не позволяли никому делать ксерокопии или фотографировать вашу карту. Если банк докажет обратное, то не вернет вам украденные деньги. Поскольку кража денег — это уголовное преступление, напишите заявление в полицию. Возможно, ваша информация поможет быстрее вычислить и поймать преступников. По итогам расследования с вами свяжется сотрудник банка и сообщит о решении. Если банк убедится, что вы не нарушали правила использования карты и при этом опротестовали операцию вовремя, вам вернут деньги.
5. Зачастую в социальных сетях вам может написать подозрительный аккаунт. Понять это можно по нескольким причинам – видно, что он создан недавно, страничка почти не ведется (мало публикаций, мало подписок и т.д), а само содержание сообщение может сразу напрямую содержать предложение заработать денег «простым способом». Это обычно так называемые боты, которые могут вам отсылать ссылки, при переходе на которых вы невольно «дарите» какие-то свои данные, а также такие сообщения могут писать ненастоящие аккаунты с целью предложения заниматься незаконной деятельностью. В таких случаях, нельзя ничего отвечать подозрительным аккаунтам, но нужно пожаловаться на них по теме «мошенничество».