Интернет-безопасность: определение и описание

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети. Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам.
Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз.
Кража личных данных, например, личной и финансовой информации злоумышленниками.
Частные лица и организации могут защититься от подобных угроз, используя приемы интернет-безопасности.

Распространенные угрозы интернет-безопасности

Чтобы сохранить конфиденциальность и безопасность в интернете, важно знать о различных типах интернет-атак. Ниже описаны распространенные угрозы интернет-безопасности.

Фишинг

Фишинг – это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от коллег, чтобы пользователи переходили по ссылкам или открывали вложения. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы.

Фишинг – одна из старейших угроз интернет-безопасности, возникшая еще в 1990-х годах. Он остается популярным и сегодня, поскольку является одним из самых дешевых и простых способов кражи информации. В последние годы фишинговые сообщения и используемые методы становятся все более изощренными.

Взлом и удаленный доступ

Злоумышленники всегда стремятся использовать уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет

пользователям получать доступ к компьютеру и управлять им удаленно. Его использование значительно выросло в период пандемии, когда все больше людей работают удаленно.

Протокол, позволяющий пользователям удаленно управлять компьютером, подключенным к интернету, называется RDP – протокол удаленного рабочего стола. Многие компании, независимо от размера, широко используют RDP, поэтому высоки шансы недостаточно надежной защиты сети. Злоумышленники используют различные методы выявления и эксплуатации уязвимостей RDP, чтобы получить полный доступ к сети и ее устройствам. Они могут как самостоятельно осуществлять кражу данных, так и продавать учетные данные в даркнете.

Вредоносные программы и вредоносная реклама

Термин вредоносные программы охватывает все программы: вирусы, черви, трояны и прочие, которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное.

Термин «вредоносная реклама» описывает онлайн-рекламу, распространяющую вредоносные программы. Интернет-реклама – это сложная экосистема, включающая веб-сайты рекламодателей, рекламные биржи, рекламные серверы, сети ретаргетинга и сети доставки контента. Злоумышленники используют эту сложность для размещения вредоносного кода там, где рекламодатели и рекламные сети не всегда могут его обнаружить. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты.

Программы-вымогатели

Программы-вымогатели – это вредоносные программы, блокирующие использование компьютера или доступ к определенным файлам на компьютере, пока не будет уплачен выкуп. Они часто распространяются как троянские программы – вредоносные программы, замаскированные под легальные. После установки программа-вымогатель блокирует экран системы или определенные файлы до тех пор, пока злоумышленники не получат выкуп.

Для сохранения анонимности злоумышленники обычно требуют платежи в криптовалютах, например, биткойнах. Стоимость выкупа варьируется в зависимости от программы-вымогателя и курса обмена цифровых валют. Однако злоумышленники не всегда разблокируют зашифрованные файлы после получения выкупа.

Количество атак программ-вымогателей растет, продолжают появляться новые варианты программ-вымогателей. Наиболее обсуждаемые программы-вымогатели включают Maze, Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky и WannaCry.

Ботнеты

Термин ботнет означает сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в интернете без разрешения и ведома владельцев этих компьютеров.

Когда компьютер управляется ботнетом, он может использоваться для выполнения злонамеренных действий. К ним относятся:

Создание фальшивого интернет-трафика на сторонних веб-сайтах с целью получения прибыли.
Использование компьютера для участия в распределенных атаках типа «отказ в обслуживании» (DDoS), вызывающих сбои в работе веб-сайтов.
Рассылка спама миллионам пользователей интернета.
Совершение мошеннических действий и кража личных данных.
Атаки на компьютеры и серверы.
Компьютеры становятся частью ботнета так же, как и заражаются любой другой вредоносной программой: например, при открытии вложений электронной почты, загрузке вредоносных программ, посещении веб-сайтов, зараженных вредоносными программами. Ботнеты также могут передаваться с одного компьютера на другой по сети. Количество ботов (зараженных компьютеров) в ботнете зависит от способности заражать незащищенные устройства.

Опасности в публичных и домашних сетях Wi-Fi

Использование публичных сетей Wi-Fi – в кафе, торговых центрах, аэропортах, отелях и ресторанах – сопряжено с определенными рисками, поскольку уровень безопасности в этих сетях часто низкий или защита полностью отсутствует. Это означает, что киберпреступники могут отслеживать действия пользователей в интернете и красть пароли и личную информацию. Другие опасности использования публичных сетей Wi-Fi включают:

Прослушивание сети – злоумышленники отслеживают и перехватывают незашифрованные данные при передаче по незащищенной сети.
Атаки типа «человек посередине» – злоумышленники взламывают точку доступа Wi-Fi и подключаются к процессу передачи данных между пользователем и точкой доступа с целью перехвата и изменения данных в процессе передачи.

Мошеннические сети Wi-Fi – злоумышленники создают приманку в виде бесплатной сети Wi-Fi для сбора личных данных. Точка доступа злоумышленника служит каналом для всех данных, передаваемых по сети.
Слежка за домашней сетью Wi-Fi не должна вызывать столько беспокойства, поскольку сетевое оборудование принадлежит вам. Но опасность, тем не менее, существует: в США провайдерам интернет-услуг разрешено продавать данные о пользователях. Хотя эти данные являются анонимными, сам факт сбора данных может вызывать беспокойство у тех, кто ценит конфиденциальность и безопасность в интернете. Использование VPN в домашней сети значительно усложняет отслеживание вашей онлайн-активности.

Как защитить личные данные в сети
Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Используйте многофакторную аутентификацию везде, где возможно
Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация:

Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты.
Ответы на личные вопросы безопасности.
Отпечаток пальца или другая биометрическая информация, например голосовые данные или лицо.
Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также можете применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

Используйте сетевой экран
Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

Внимательно относитесь к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных. Фонд свободы прессы составил подробное руководство, описывающее плюсы и минусы безопасности основных веб-браузеров.

Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами:

Длинный: минимум 12 символов, в идеале, даже больше.

Содержит заглавные и строчные буквы, а также специальные символы и цифры.

Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.

Не содержит запоминающихся сочетаний клавиш.

Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.

Используйте на устройствах последнюю версию программы безопасности

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.

Как обезопасить свою семью в интернете

Защита детей от опасного и неприемлемого контента и контактов в интернете, а также от вредоносных программ и атак очень важна. Обучение детей основам безопасности в интернете позволит их обезопасить.

Рекомендации по обеспечению безопасности детей в интернете

Дети проводят все больше и больше времени в интернете, и важно объяснить им, как оставаться в безопасности. Важно, чтобы они знали, какую

информацию следует хранить в секрете. Например, следует объяснить, почему никому нельзя сообщать пароли и раскрывать личную информацию. Установка компьютера там, где вы можете наблюдать и контролировать его использование, также поможет обеспечить безопасность ребенка в интернете.

Многим детям нравится смотреть видео на YouTube. Чтобы сделать этот процесс более безопасным, можно использовать родительский контроль для YouTube. Также можно использовать специальное приложение для детей – YouTube Kids. Оно имеет удобный для детей интерфейс, а видео в приложении отбираются модераторами-людьми и автоматическими фильтрами, и подходят даже для детей младшего возраста.

Безопасность и конфиденциальность в интернете

Как защитить электронную почту
Электронная почта разработана так, чтобы быть максимально открытой и доступной и позволить людям общаться друг с другом. Недостатком такой доступности является уязвимость некоторых аспектов электронной почты. Это позволяет злоумышленникам использовать электронную почту для нарушения безопасности в интернете.

Что такое безопасность электронной почты?
Безопасность электронной почты – это набор методов, используемых для защиты учетных записей электронной почты и переписки от несанкционированного доступа, потери и компрометации. Учитывая, что электронная почта часто используется для распространения вредоносных программ, спама и фишинговых атак, ее безопасность является важным аспектом безопасности в интернете.