Кибersквоттинг

Кибersквоттинг (англ. cybersquatting) — это регистрация доменных имён, содержащих торговую марку, принадлежащую другому лицу с целью их дальнейшей перепродажи или недобросовестного использования. Многие кибersквоттеры просто регистрируют веб-домены с целью их последующей продажи существующим компаниям и владельцам брендов, такая практика часто называется «парковкой» доменов.

Однако некоторые кибersквоттеры преследуют иные цели. Регистрируя адрес веб-сайта таким образом, что он выглядит так, как будто он принадлежит хорошо известной компании или организации, киберпреступники могут заманивать на сайт ничего не подозревающих посетителей. Эти веб-сайты часто содержат вредоносные программы.

Как избежать попадания на веб-сайты кибersквоттеров

Ниже мы приводим несколько советов от экспертов «Лаборатории Касперского», которые помогут вам не стать жертвой киберпреступников, занимающихся кибersквоттингом.

- **Вводите URL-адрес вручную и убедитесь в том, что он набран без ошибок**

Если вы собираетесь посетить определенный веб-сайт, безопаснее всего вручную ввести его URL-адрес в адресную строку веб-браузера вместо использования ссылки. После ввода URL-адреса необходимо внимательно проверить его правильность, прежде чем нажать кнопку ввода на клавиатуре. Любые опечатки могут привести к переходу на веб-сайт кибersквоттера, а такой сайт может содержать вредоносное программное обеспечение.

- **Не открывайте подозрительные сообщения электронной почты и не проходите по ссылкам в них.**

При получении подозрительных электронных сообщений (особенно писем от социальных медиасайтов или связанных с ними ресурсов) лучше не открывайте их и не щелкайте ссылки внутри этих сообщений. Вместо этого откройте сайт, о котором говорится в письме, через браузер, чтобы напрямую просмотреть уведомления или сообщения, содержащиеся на сайте.

- **Устраните уязвимости в ОС и приложениях**

Убедитесь, что операционная система и все приложения, работающие на компьютере, включая браузеры и подключаемые модули, регулярно обновляются. Это поможет устранить уязвимости, которые могут быть использованы вредоносной программой, если вы окажетесь на веб-сайте кибersквоттера.

- **Установите антивирусное программное обеспечение для защиты от интернет-угроз и своевременно обновляйте его**

Эффективное антивирусное решение, которое включает сетевой экран, может помочь защитить компьютер посредством блокировки вредоносных поддоменов. Некоторые антивирусные решения предупреждают пользователя и о попытке входа на сайт, который может содержать вредоносную программу. Чтобы обеспечить максимальный уровень защиты, убедитесь в том, что программное обеспечение для защиты от интернет-угроз регулярно обновляется.