Анализ URL-адресов

Узнайте о способах анализа URL-адресов и о том, как избежать небезопасных или рискованных URL-адресов.

1. Из чего состоит URL-адрес?

Чтобы проанализировать универсальный указатель ресурса (Universal Resource Locator, URL), нужно знать, из каких частей состоит URL-адрес и что вы можете увидеть. Рассмотрим пример URL-адреса: https://www.microsoft.com/en-us/.

Пример	Часть URL-адреса	Пояснение и определение	Факторы риска
https	Протокол	В протоколе описывается то, как веб-браузер должен извлекать информацию из URL-адреса.	Главное в данном случае — определить наличие «https», или безопасного протокола. URL-адреса, начинающиеся с «http», не являются безопасными и считаются сопряженными с риском.
www.microsoft.com	Домен	Домен — это имя веб-сайта и тип веб-сайта. Домены состоят из домена второго уровня и домена верхнего уровня. В данном случае домен второго уровня — «www.microsoft», а домен верхнего уровня — «.com», который говорит о том, что сайт коммерческий.	Мошенники могут использовать домены для маскировки или для обмана людей. Например, они могут использовать сопряженный с риском домен верхнего уровня в сочетании с заслуживающим доверия доменом второго уровня с целью обмана людей. Пример — «www.microsoft.xyz».

/en-us/	Путь	Путь указывает на конкретную страницу или ресурс, на который вы перейдете на веб-сайте. В данном случае путь говорит о том, что мы посещаем англоязычную версию веб-сайта Microsoft для США.	Мошенники могут включать в путь файла трекеры или странные символы. Обратите внимание: мошенник может использовать укороченный URL-адрес, например bit.ly, чтобы скрыть подозрительность своих URL-путей.

2. Как проанализировать URL-адрес и удостовериться в его безопасности?

Анализируя URL-адрес, обращайте внимание на следующее.

Протокол

- **Обратите внимание на протокол.** Обязательно определите наличие «https», или безопасного протокола. Если вы не видите протокол «https», выясните, что именно вы видите, чтобы убедиться в безопасности, и не нажимайте на ссылку, пока не будете уверены, что она безопасна.

Домен и путь

- **Обратите внимание на информацию в домене и пути.** Ищите небольшие орфографические ошибки, странный домен верхнего уровня или необычные символы. Эти признаки зачастую могут указывать на сопряженный с риском или небезопасный URL-адрес.

- **Обратите внимание на весь домен.** Мошенники часто добавляют к домену дополнительные подозрительные элементы, без которых он выглядит заслуживающим

доверия. Даже если один из элементов домена выглядит надежным, не позволяйте себя обмануть: проанализируйте весь домен и убедитесь в его подлинности.

- **Помните: домен верхнего уровня находится на последнем месте.** Сначала идет домен второго уровня, затем — домен верхнего уровня. Иными словами, домен верхнего уровня — последний элемент перед путем. С целью обмана мошенники часто используют домены второго уровня, похожие на подлинные. Обращайте внимание на все, что находится между протоколом «https» и символом «/».

- **Проверяйте сокращенные или видоизмененные URL-адреса.** Сократить URL-адрес или создать видоизмененную ссылку для письма очень легко. Воспользуйтесь инструментом (см. ниже) для проверки таких URL-адресов, прежде чем на них нажимать. Сокращенные URL-адреса могут использовать мошенники, чтобы скрыть вредоносные ссылки!

Ниже приведено несколько примеров сопряженных с риском URL-адресов, в которых используется известное вымышленное учреждение — университет Хадсона:

Hudsonuniversity.edulogin.com

В данном примере фактическим доменом верхнего уровня является «.com»; с целью обмана мошенник объединил путь с доменом. Подлинная версия такого адреса должна выглядеть примерно так: hudsonuniversity.edu/login.

Hudsoununiversity.edu

В данном примере слово «Hudson» написано неправильно — «Hudsoun». Мошенники часто используют такой прием, чтобы вынудить людей нажимать на фальшивые ссылки, которые на первый взгляд выглядят надежными.

http://hudsonuniversity.edu.student_login%.ie

В данном примере сразу несколько проблем! Во-первых, в этой ссылке использован небезопасный протокол «http». Во-вторых, имя домена — «student_login%.ie», а не

«hudsonuniversity.edu». Помните, что домен верхнего уровня находится на последнем месте! Наконец, домен содержит нестандартные символы, что может указывать на небезопасный URL-адрес.

3. Как проверить URL-адреса?

Для проверки URL-адресов вы можете воспользоваться различными инструментами и ресурсами.

Инструменты проверки репутации. Эти сайты могут проверить репутацию URL- или IP-адреса и предупредить вас в случае его подозрительности или вредоносности.

https://www.urlvoid.com/
https://www.virustotal.com/gui/home/url

Инструменты расширения URL-адресов и поиска IP. Эти инструменты можно использовать для проверки сокращенных URL- или IP-адресов. Помните, что сокращенные URL-адреса часто используются, чтобы скрыть вредоносные URL-адреса.

https://checkshorturl.com/
https://www.expandurl.net/
https://www.ipvoid.com/

Песочницы. Эти сайты позволяют просканировать и проанализировать URL-адрес, прежде чем на него нажимать.

https://urlscan.io/

И наконец, в большинстве браузеров есть функции обеспечения безопасности, предупреждающие о вредоносных URL-адресах. Обращайте внимание на эти предупреждения, если случайно нажмете на что-то подозрительное!

В качестве дополнительной практики по анализу URL-адресов изучите приведенные выше ссылки и проверьте, можете ли вы определить, почему они подлинные!