هنگام گشت و گزار در اینترنت، در طی فرآیند DNS Lookup و پرسش از DNS Server از آدرس سایت به آی پی سرور آن می رسیم و برای تبادل ارتباط با سایت در شبکه اینترنت از پروتکل TCP/IP استفاده می شود. در صورت استفاده سایت از HTTPS محتوای تبادل رمزنگاری شده است و اتکر نمی تواند از محتوای آن باخبر شود. ولی با DNS سنتی، برای اتکری که در شبکه ما نفوذ دارد، این امکان وجود دارد تا از سایت هایی که ما معمولا ویزیت می کنیم باخبر شود و حتی DNS Lookup مارا به سمت سایت جعلی خود هدایت کند و فیشینگ را اجرا کند.

DNS over HTTPS (DoH) برای جلوگیری از موارد یاد شده بوجود آمده است. جستجوهای DNS در این روش با قدرت HTTPS تلفیق می شود و دیگر به صورت Clear Text نیست.

## فعالسازی در رجیستری ویندوز 10

1. باز کردن Registry Editor
2. رفتن به کلید HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters
3. اضافه کردن DWORD جدید با نام EnableAutoDoh و مقدار 2
4. ری استارت سیستم
5. تغییر DNS پیشفرض به یکی از سرورهایی که DoH در ویندوز 10 را پشتیبانی می کنند. در حال حاضر سرویس های جدول زیر قابل استفاده هستند:

|  |  |  |
| --- | --- | --- |
| Service | Primary DNS Server | Alternate DNS Server |
| **Cloudflare** | 1.1.1.1 | 1.0.0.1 |
| **Google** | 8.8.8.8 | 8.8.4.4 |
| **Quad9** | 9.9.9.9 | 149.112.112.112 |

## فعالسازی از طریق تنظیمات ویندوز 10

1. انتخاب Settings در Start Menu
2. انتخاب Network Settings
3. انتخاب Properties زیر قسمت Network Status برای اتصال اینترنت مورد نظر
4. انتخاب Manual Option و استفاده از یکی از سرویس های شرح داده شده در بالا
5. انتخاب گزینه Encrypted only (DNS over HTTPS)

## فعالسازی از طریق Group Policies

