VisitNC.com now uses HTTPS

HTTPS is a good thing.

We've recently made changes so all visits to VisitNC.com are made over a secure connection (HTTPS).

Going full HTTPS is an additional layer of protection to guard the privacy and integrity of partners' and visitors' data. Using encrypted HTTPS (secure) connections on websites is a universal direction toward which the internet is continuing to evolve. In addition to added security, a major benefit of having a secure connection is ranking higher in Google search results. Google recently added HTTPS as a lightweight ranking signal, which prioritizes sites with HTTPS above HTTP (non-secure) sites. Sites that appear higher in search results typically receive more organic search traffic.

What does this mean for you?

Going secure has changed how our **non-HTTPS partner websites** see our referral traffic in Google Analytics. VisitNC.com referral traffic is reaching you the same as it always has, but Google Analytics now logs these visits as "direct traffic" and not "referral traffic." This is the nature of HTTPS sites sending traffic to HTTP websites. Referral information is off-limits per the security rule.

So, in summary, while you're still receiving traffic from VisitNC.com if your site is HTTP, you just won't see VisitNC.com referral traffic in the usual place in Google Analytics (*Acquisitions > All Traffic > Referrals).*

So what's the solution? How do I see VisitNC.com referral traffic?

We have already implemented a solution for our non-HTTPS partners to get around this limitation and have additional recommendations for your site moving into the future.

1. **Look for the VisitNC Referral Campaign (VisitNC solution, already in place)**
   VisitNC.com now tags all downstream clicks with a Google UTM query-string. When referral traffic from VisitNC.com comes to your site, this UTM is recorded by Google Analytics as a *"Campaign."* **You can see these referral numbers in Google Analytics by navigating to *Acquisitions > All Campaigns*. VisitNC.com will appear in this report as "*www.visitnc.com / website*."**

2. **Add a special meta tag. (Requires some developer support)**
   A change you can make is to add a special meta tag to all pages in your website.

   Meta tag: *<meta name="referrer" content="always" />*

   This meta tag informs the browser the referral source information should not be blocked, which then makes it available to Google Analytics for reporting as usual. That said, this meta tag is mainly supported by newer browsers such as Chrome and Safari, but not all browsers.

   Note: if this meta tag is implemented on your website, VisitNC.com referral traffic will be tracked in two locations:
   - *Acquisitions > All Campaigns* (as outlined in #1 above)
   - *Acquisitions > All Traffic > Referrals* (as it was before the VisitNC.com HTTPS transition)

3. **Go HTTPS! (Requires developer support)**
   The best thing you can do is join us and go HTTPS too. Everyone is headed in that direction. Adding HTTPS to your website eliminates the referral tracking issue and as a bonus, elevates your website in Google search results.

   Note: if your site is updated to use HTTPS, VisitNC.com referral traffic will be tracked in two locations:
   - *Acquisitions > All Campaigns* (as outlined in #1 above)
   - *Acquisitions > All Traffic > Referrals* (as it was before the VisitNC.com HTTPS transition)

We've included some additional questions and answers regarding HTTPS and the process for implementing it on your site below for reference. That said, please do not hesitate to reach out with any questions about transitioning your site to HTTPS or any of the options we've shared above.

HTTPS Q&A

Q: Where can I learn more about HTTPS?
A: Learn more about HTTPS (secure) websites at: https://en.wikipedia.org/wiki/HTTPS and get more details on how Google prioritizes secure sites at: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

Q: How do I know if my site uses HTTPS?
A: If you are unsure about HTTPS on your site you can easily test it. Here's how:

1. Using your browser, navigate to your website.
2. In the URL bar of your browser look to see if the URL begins with "http**s**://." If you see "http**s**://" and there is a small lock icon next to it, this means your website is using HTTPS and is secure.
3. If you don't see "https://" in the URL bar, simply change the URL from "http://" to "https://" and refresh the page. If your browser displays a warning message that your connection is not private, your site is NOT configured to use HTTPS and is not secure.

Q: How do I make my site secure?
A: Setting up your website to use HTTPS will need to be completed by your developer or web host. Contact your developer or hosting provider to get the process started. Please note, **HTTPS is not free.** Your organization will be required to purchase an "SSL certificate," which is then installed on your site's webserver to ensure the connections between your website and visitors are encrypted. SSL certificates can range in price from $100 to thousands of dollars depending on the level needed for your site.

Q: Once I have HTTPS on my website is there more I should know?
A: Yes! First, your SSL certificate will not last forever. You set the lifespan of the certificate in the initial purchase and it will expire after that amount of time. We recommend purchasing the SSL certificates for three years. In this way, you are not renewing your SSL certificate every year, but often enough to keep it front of mind.

Q: What else do I need to know?
A: While this is not a complete HTTPS lesson, adding HTTPS to your website usually requires subtle changes to your HTML code. All images, CSS, Javascript, etc. that your sites uses also have to use HTTPS. This is another job for your developer. If you have links to HTTP resources but your page is HTTPS, the browser will alert you and visitors that the page is using "mixed content" and the page is not fully secure.

Sometimes this is minor and other times it can make your page look broken if these resources cannot be loaded properly. These are good questions to talk through with your web developer prior to the installation of the SSL certificate.