THE CHRISTIAN LIBRARIAN®
JOURNAL OF THE ASSOCIATION OF CHRISTIAN LIBRARIANS

Volume 58 | Issue 2 Article 6

2015

The End of HTTP and the Library Website: The Growing Need for HTTPS in Library Services

Michael Wells
Northern Kentucky University

The End of HTTP and the Library Website: The Growing Need for HTTPS in Library Services

Michael Wells, Systems Librarian
Northern Kentucky University

Over the last few years, the frequency of information security breaches has continued to rise. Whether with corporate entities or nonprofits, the occurrence of cyber-based attacks against organizations like Sony Pictures, Anthem Health Insurance, Home Depot, and Target have littered the media landscape. Many of these attacks are fiscally motivated, but more recently, there has been a sharp rise in larger disruptive attacks from state-sponsored organizations.

Libraries are not immune to these attacks, as we often hold the key to paywall-protected, copyrighted content that researchers in other nations would love to have access to. Many times in the past year, my institution has had to shut down access to unauthorized, internationally-based attackers through our proxy server. The successful access attempts that got through the proxy were gained after the attacker had used phishing or "spear-phishing" e-mails to obtain authentication credentials from students or faculty.

These library-oriented computer security breaches are not unique to my institution as Steven Bell explained in his November 2014 *Library Journal* article. Bell mentions the presence and growth of an underground market for research and the use of "research assistance from librarians" to obtain access to it (Bell, 2014). As librarians, we now need to balance the perspective of computer security with patron access to materials and personal privacy. These sometimes divergent elements create for a very interesting and unique information environment these days.

One important tool that librarians and IT professionals have in their arsenal for security when dealing with digital information is encryption. Specifically, when examining library sites and proxy servers, the use of encryption is growing more and more important. To the uninitiated, SSL/TLS certificates provide a website the

capability to deliver an encrypted and secure connection to your browser using the HTTPS protocol. This is the connection protocol we establish as consumers using commercial sites like Amazon to make purchases or completing online banking transactions.

In late 2014, Google announced that in an effort to better secure the internet they would deprecate websites in their search results that did not use SSL/TLS certificates (Santamaria, 2015). This means that sites that only use the HTTP protocol for web content delivery would rank lower on a Google search and receive some sort of negative indicator when viewed in the Chrome browser. To follow Google's lead in this area, on April 30, 2015, the Mozilla Foundation that develops the Firefox web browser announced that their browser would also begin a deprecation of sites that only use HTTP as well (Barnes, 2015). Though at this time it is unclear how this will look in Firefox, the idea is that websites that do not use SSL/TLS certificates over an HTTPS connection would either not load or show a scary warning message instructing the user to proceed with caution.

These announcements should be applauded for promoting a shift to secure connections on the internet. However, one has to understand that historically, setting up SSL/TLS and HTTPS has not been a trivial effort. For this article, I will save you all the technical detail; however, the process of registering a secure certificate involves several steps. Typically, these certificates are minted with a certificate authority (CA) outside your organization and can sometimes be a challenge to install, and typically, the good certificates are not free.

It would be a worthwhile undertaking to survey academic, public, and special libraries to see what percentage actually use secure HTTPS connections at this time. Realistically, it is likely that most do not. So, what impact will lower Google search results and browser warnings have on traffic to these library sites? My guess is, if you use a cloud-hosted solution like LibGuides for your site, you won't have much to worry about. However, if you host your own website, or if your institution provides hosting, now is a good time to start some conversations about the future use of an HTTPS connection.

One potentially viable solution on the horizon is the "Let's Encrypt" project that is being spearheaded by the Electronic Frontier Foundation (EFF) and partners like the University of Michigan (https://letsencrypt.org/). The Let's Encrypt website is said to offer an easy and seamless process of registering secure web server certificates. These certificates are not the top level, expensive certificates that many online businesses use and need. However, they should be a good basic certificate that can allow you to overcome the HTTP bias that is growing online.

That HTTP bias is valid for many reasons. Historically, the internet was not designed and built for privacy and HTTP is evidence of that. Anyone with certain software can read and manipulate HTTP traffic if it is captured in transit. This can be a problem, especially in the age of cloud-hosted systems. Most cloud ILSs make a point to use SSL/TLS encryption; however, sometimes libraries can overlook the need for encryption for devices like self-check units and other peripheral systems that use HTTP to connect to those cloud-based ILS platforms. Your library website may need this encryption ability just to stay accessible and relevant, but it might also be worthwhile to investigate encryption at a broader level if you offer these additional services over HTTP.

In the end, library websites are already fighting to maintain an institutional foothold against sites like Google and Wikipedia. With changes coming to the broader internet, now would be the best time to start to scope and plan a means for getting your website and other resources using encrypted communications. Realistically, libraries are not top level targets of cyber-attacks; however, we do profess to value patron privacy and encryption is a way for us to deliver on that promise. ✞

ABOUT THE AUTHOR

Michael Wells is Systems Librarian at Northern Kentucky University in Highland Heights, KY. He can be contacted at wellsm6@nku.edu.

REFERENCES

Barnes, R. (2015, April 30). Deprecating non-secure HTTP [blog post]. Retrieved from https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/

Bell, S. (2014). Keeping library content secure. *Library Journal*, 18, 14.

Santamaria, M. (2015, June 19). HTTP deprecation [DigiCert blog post]. Retrieved from https://blog.digicert.com/http-deprecation/