Final Report

BEST PRACTICES TO INFORM PATRONS ABOUT AUTHENTICATION FOR OFF-CAMPUS ACCESS TO LIBRARY SUBSCRIPTION RESOURCES TASK FORCE

To: The Reference Common Knowledge Group
Direction & Oversight Committee via Sarah Troy

From: Best Practices to inform patrons about Authentication for off-campus access to library subscription resources Task Force (Ken Furuta, UCR, Frank Gravier, UCSC, Cynthia Johnson, UCI, Elizabeth McMunn-Tetangco, UCM)

Date: July 29, 2016

Brief overview of the charge:
Students' understanding of the need to authenticate and their having an easy path to off-campus authentication is vital if we want them to make use of the materials we license. A subgroup of the Reference Common Knowledge Group investigated how the UC campuses might improve our students' understanding and ability to authenticate when off-campus. The outcome will be a set of Best Practices for the UC libraries.

Outcomes and proposed next steps:

In addition to widely sharing the proposed Best Practices (Appendix 1), we recommend the following next steps:

1. CDL (for Tier 1 and Tier 2 databases) work with database vendors about adding a phrase such as "Check if your library has off-campus access" to the web pages that request users to login.
    a. Vendors should be willing to work with libraries since patrons' use of the databases is an important element in determining renewals.
    b. Other libraries and library consortia will support plans to make it easier for patrons to learn about and use their libraries' authentication processes.
2. User testing to determine if "Connect from off-campus" is an effective phrase that helps lead patrons to necessary information about authentication.
3. Develop shareable graphics for posters that can be used by campuses to better advertise information about authentication either in print or digital form.

The Reference CKG will continue to spearhead promotional efforts to inform patrons about the need for authentication, and it will also continue to advocate making authentication more seamless for our users. Our proposed next steps will include:

1. Sharing the Best Practices with UC librarians and staff, particularly those involved with website redesigns.
2. Creating a team to develop graphics and poster ideas, and finding a space to share these ideas, as well as outreach and marketing ideas to ensure that our patrons are better informed about the need to authenticate.

Report on the specific tasks outlined in the charge:

We reviewed the language used to describe off-campus access on the UC libraries' websites and we also surveyed some non-UC libraries. We determined that defining the "VPN" and "Proxy" would not be beneficial for most patrons. To create a meaningful definition that helped explain the differences, we would have to define how each method works. We feel it is more important that patrons understand that these are methods used to help them access licensed resources, not how the two authentication methods work.

The survey of library websites also helped us identify language explaining why authentication is important. We developed the following phrasing:

> From off-campus, the Library's online subscription resources (databases, electronic journals, and e-books) can only be accessed by current <campus name> faculty, students, and staff. Authenticate <link to campus information> to access these resources from off campus. This will make your computer think you are on campus and will provide quick, seamless access to all of the Library's databases. Contact the library if you have questions about your eligibility.

The survey of websites also provided a variety of different names given to the process of authentication, to help patrons know where to click on the library website. The Reference Common Knowledge Group preferred the term **"Connect from off-campus"** but we did not do user testing. We recommend that libraries have this information on their home pages and that the information appears in a consistent location throughout the entire website.

If a library provides more than one type of authentication (Proxy and VPN, or VPN and WebVPN, for example), the individual library should provide information about which to use for the best results or in what circumstances a patron should choose one (e.g. VPN instead of Proxy). This Task Force can provide examples.

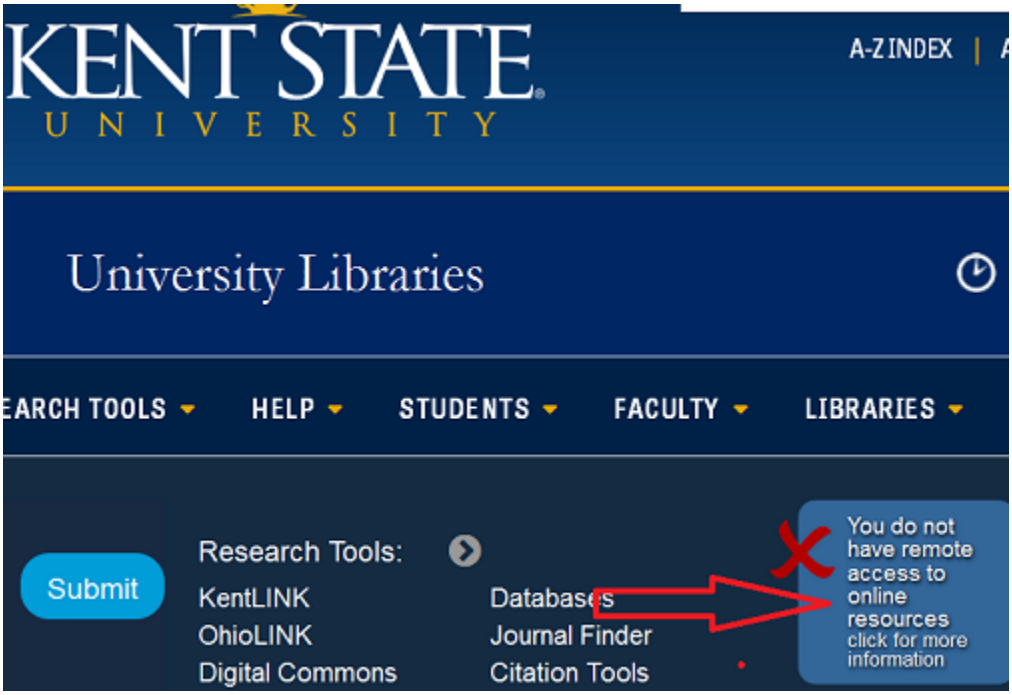
To direct patrons to help, we recommend that each library clearly state how patrons can receive further assistance, including technical assistance, and the days and hours that assistance is available. Examples include:

1. For further assistance, call OIT at (949) 824-2222 (available 24/7) or visit the OIT Help Desk page.
2. For further help, check out our troubleshooting guide.

The Task Force, with the Reference CKG, conceived a variety of methods to increase patrons' awareness of the need to authenticate. Below are our ideas:

1. Working with CDL to have database and journal vendors adjust the language on the open web login screens to include a message similar to "Check if your library has off-campus access"
2. Bring-your-device workshops to help set up the software VPN
3. Information sent to new students via library partnerships with IT and other campus units

4. Advertising to students (particularly commuters) with posters (physical and/or digital) in student areas, such as Commuter Lounges, as well as posting to social media. Examples:
    a. “Stay Connected to the Library”
    b. “Students. Are you moving off-campus? Take the library with you….”
5. Place a “troubleshooting” button on the website that informs patrons if they are not authenticated, or that allows them to test if they are authenticated.



Appendix 1

Authentication Best Practices

1. Use the term “Connect from off-campus” as the text for the link to connect patrons to information about authentication.
2. “Connect from off-campus” should appear on library home pages; it should also appear in *a consistent* location throughout the entire website.
3. Use the following language to inform patrons why authentication is important:
    a. From off-campus, the Library's online subscription resources (databases, electronic journals, and e-books) can only be accessed by current <campus name> faculty, students, and staff. Authenticate <link to campus information> to access these resources from off-campus. This will make your computer think you are on campus and will provide quick, seamless access to all of the Library's databases. Contact the library if you have questions about your eligibility.
4. Provide information about which method to use for the best results or in what circumstances a patron should choose to authenticate using the VPN or using the proxy server if your campus has more than one way for patrons to authenticate.
5. Clearly state how patrons can receive further assistance, including technical assistance, and the days and hours that assistance is available. For example:
    a. For further assistance, call OIT at (949) 824-2222 (available 24/7) or visit the OIT Help Desk page.
    b. For further help, check out our trouble shooting guide.
6. Find non-library venues to inform patrons about authentication. Examples:
    a. Working with CDL to get vendors to adjust the language on the open web from things like “log on”, to also include a message similar to “Check if your library has off-campus access”
    b. Bring-your-device workshops to help set up the software VPN
    c. Information sent to new students via library partnerships with IT and other campus units
    d. Advertising to students (particularly commuters) with posters (physical and/or digital) in student areas, such as Commuter Lounges, as well as posting to social media.
        i. Stay Connected to the Library
        ii. Students. Are you moving off-campus? Take the library with you….
    e. Place a “troubleshooting” button on the website that informs patrons if they are not authenticated, or that allows them to test if they are authenticated. An example is Kent State University Libraries’ website.