EDUCATE

- Read up on security topics in higher education and scholarly publishing at places like Ren-Isac and The Scholarly Kitchen blog archives.
- EZProxy users, talk to OCLC about their efforts to block/minimize illegal access to licensed content.

SUPPORT

- Respond quickly to publisher notices of unauthorized use of their platforms from your institution.
- Support the Coalition for Seamless Access and implement this NISO certified solution for your remote users.
- Seek to make the user experience of library resources as easy as possible – as many users claim to utilize Sci-Hub solely based on ease of use.
- Encrypt all library resources using https for security, including web sites, catalogs and other library tools.
- Make all reasonable efforts to comply with the commitments set out in online access agreements to ensure only those authorized to access content do so.
- Support publishers who make honest efforts to advance the open access movement through transformative deals and publishing models.

JOIN

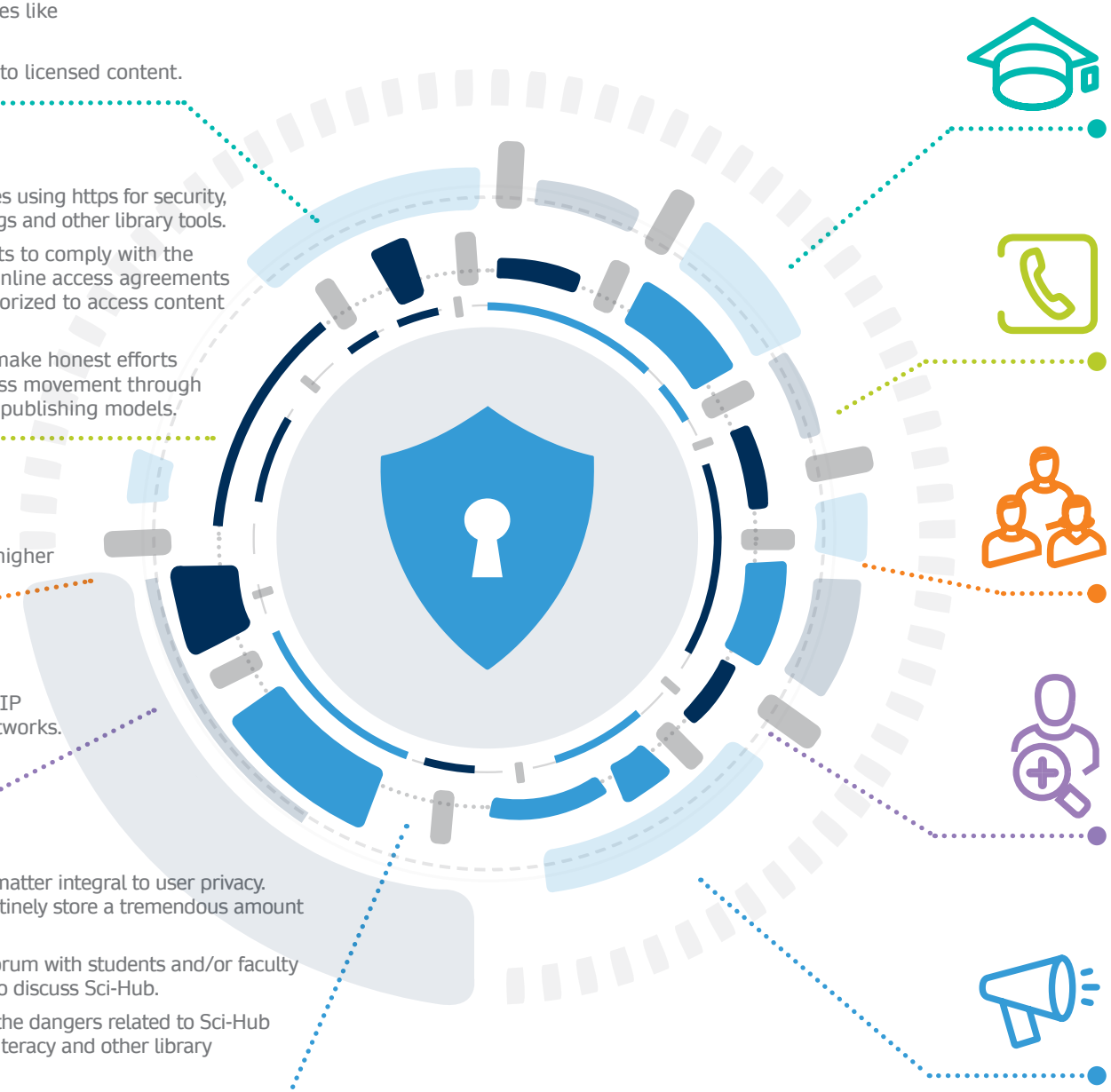
- Academic institutions should Join Ren-Isac if they have not already done so.
- Consider joining the EDUCAUSE Security listserv to monitor common issues in higher education security. Visit educause.edu/community/security-community-group

FOLLOW

- Sign-up to the free PSI Registry alerts (psiregistry.org/signup) to be notified of IP addresses known to be used by Sci-Hub to illegitimately access institutional networks.
- Treat Sci-Hub as a persistent threat to your institutional network security.

SPREAD THE WORD

- Don't think higher education is immune from cyber-attack. The education sector is the third largest target of cyber-attacks, ahead of retail.
- Schedule a talk with your head of network security to discuss any library-specific concerns. Share this checklist with your network security staff.
- Give all library staff a sense of responsibility for reporting and acting on security threats when they spot them.
- Treat security as a matter integral to user privacy. Library systems routinely store a tremendous amount of personal data.
- Consider an open forum with students and/or faculty and research staff to discuss Sci-Hub.
- Consider including the dangers related to Sci-Hub use in information literacy and other library outreach programs



Find out more: springernature.com/tools-services

Scholarly Network Security Initiative

SNSI is an initiative bringing together publishers and institutions to solve cyber challenges threatening the integrity of the scientific record, scholarly systems and the safety of personal data.

This list was created based on input from the participants at an Information Security Summit held in October 2019 at Worcester Polytechnic Institute, and sponsored by the Boston Library Consortium, Worcester Polytechnic Institute, and Springer Nature.

SNSI Scholarly Networks Security Initiative

Find out more about discovery and securely implementing content in your library at our dedicated tools & services webpage springernature.com/tools-services

A83514

SPRINGER NATURE

INFORMATION SECURITY CHECKLIST FOR ACADEMIC LIBRARIES

This checklist is a starting place for academic libraries to become involved in the process of providing better security for students, faculty and staff as they utilize the information resources of the campus. Get involved!