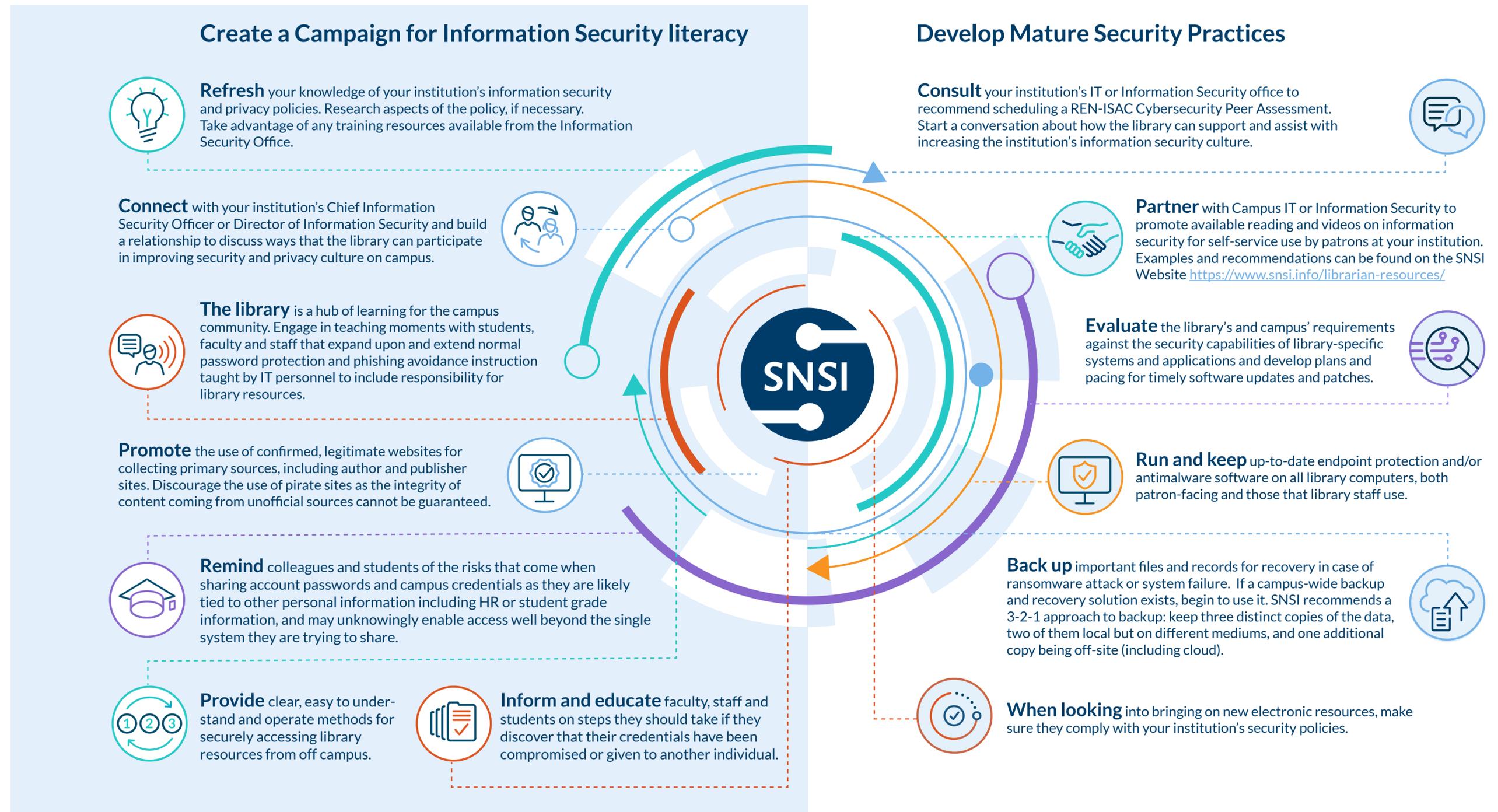# SNSI tips for academic librarians on building strong information security defenses at your institution

The Scholarly Networks Security Initiative recommends these rules of thumb when considering how libraries can contribute and support information security practices in higher education. These same recommendations can also be applied to nearly any other organization too. The investment of time, focus, and technology in prevention efforts is far more useful than the significant costs that result after a security intrusion or data breach.

Security is the responsibility of everyone within an organization, to protect institutional data, that of faculty, staff and students, and to ensure the integrity of the work and research the institution performs. However, this investment in protecting information must be visibly supported from leaders across the organization to establish and reinforce a strong security culture on campus.

Create a Campaign for Information Security literacy

Refresh your knowledge of your institution's information security and privacy policies. Research aspects of the policy, if necessary. Take advantage of any training resources available from the Information Security Office.

Connect with your institution's Chief Information Security Officer or Director of Information Security and build a relationship to discuss ways that the library can participate in improving security and privacy culture on campus.

The library is a hub of learning for the campus community. Engage in teaching moments with students, faculty and staff that expand upon and extend normal password protection and phishing avoidance instruction taught by IT personnel to include responsibility for library resources.

Promote the use of confirmed, legitimate websites for collecting primary sources, including author and publisher sites. Discourage the use of pirate sites as the integrity of content coming from unofficial sources cannot be guaranteed.

Remind colleagues and students of the risks that come when sharing account passwords and campus credentials as they are likely tied to other personal information including HR or student grade information, and may unknowingly enable access well beyond the single system they are trying to share.

Provide clear, easy to understand and operate methods for securely accessing library resources from off campus.

Inform and educate faculty, staff and students on steps they should take if they discover that their credentials have been compromised or given to another individual.

Develop Mature Security Practices

Consult your institution's IT or Information Security office to recommend scheduling a REN-ISAC Cybersecurity Peer Assessment. Start a conversation about how the library can support and assist with increasing the institution's information security culture.

Partner with Campus IT or Information Security to promote available reading and videos on information security for self-service use by patrons at your institution. Examples and recommendations can be found on the SNSI Website https://www.snsi.info/librarian-resources/

Evaluate the library's and campus' requirements against the security capabilities of library-specific systems and applications and develop plans and pacing for timely software updates and patches.

Run and keep up-to-date endpoint protection and/or antimalware software on all library computers, both patron-facing and those that library staff use.

Back up important files and records for recovery in case of ransomware attack or system failure. If a campus-wide backup and recovery solution exists, begin to use it. SNSI recommends a 3-2-1 approach to backup: keep three distinct copies of the data, two of them local but on different mediums, and one additional copy being off-site (including cloud).

When looking into bringing on new electronic resources, make sure they comply with your institution's security policies.

Librarians and libraries have long been champions of good security to uphold the values core to the library. The campus-wide efforts to protect data are increasing as threats against institutions' data rise. Libraries, in partnership with other administrative units across campus including IT and Information Security, can educate patrons on how to protect institutional and personal information, access genuine resources to support their research, and build strong relationships between the Library and campus Information Security colleagues.

Scholarly Networks Security Initiative (SNSI) brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of personal data. www.snsi.info