Introduction

For a number of years, theft of subscribed content has been a major concern of publishers and libraries. Content theft is generally initiated by parties outside the authorized user base of an institute who have stolen credentials of authorized users, typically via a phishing scam. While it may seem that the primary victim of such activity is publishers, the members of the university community are at risk as well since IDs and passwords used for library access are often the same as those used by students and faculty to access Personal Identifiable Information (PII), such as grades, tuition bills and details of financial aid, research data, email accounts, and, in the case of employees of an institution, salary and other employment-related information. (see Rick Anderson's open letter to university faculty at https://scholarlykitchen.sspnet.org/2016/05/19/sci-hub-and-academic-identity-theft-an-open-letter-to-university-faculty-everywhere/

Elsevier terms & conditions related to content access

Elsevier's Subscription Agreements contain the following clauses (in **bold face)** that are relevant to this discussion

"1.4 *Restrictions on Use of Subscribed Products*.
Except as expressly stated in this Agreement or otherwise permitted in writing by Elsevier, the Subscriber and its Authorized Users may not:

- abridge, modify, translate or create any derivative work based on the Subscribed Products, except to the extent necessary to make them perceptible on a computer screen to Authorized Users;

- remove, obscure or modify in any way any copyright notices, other notices or disclaimers as they appear in the Subscribed Products;

- **use any robots, spiders, crawlers or other automated downloading programs, algorithms or devices to continuously and automatically search, scrape, extract, deep link, index or disrupt the working of the Subscribed Products;**

- substantially or systematically reproduce, retain, store locally, redistribute or disseminate online the Subscribed Products; **[or]**

- post individual items from the Subscribed Products on social networking sites[; or|.]

3.2 *Protection from Unauthorized Access and Use.*
The Subscriber will use reasonable efforts to:

- limit access to and use of the Subscribed Products to Authorized Users and notify all Authorized Users of the usage restrictions set forth in this Agreement and that they must comply with such restrictions;

- issue any passwords or credentials used to access the Subscribed Products only to Authorized Users, not divulge any passwords or credentials to any third party, and notify all Authorized Users not to divulge any passwords or credentials to any third party;

- **provide true, complete and accurate IP addresses, as identified on Schedule 2, (if any) for the exclusive use by the Subscriber (including, if requested by Elsevier, written confirmation by the relevant third party**

internet service provider) and proactively inform Elsevier of any changes to the Subscriber IP addresses, including the addresses no longer being used exclusively by the Subscriber; and

- **promptly upon becoming aware of any unauthorized use of the Subscribed Products, inform Elsevier and take appropriate steps to end such activity and to prevent any recurrence.**

In the event of any unauthorized use of the Subscribed Products, Elsevier may suspend the access and/or require that the Subscriber suspend the access from where the unauthorized use occurred upon notice to the Subscriber. The Subscriber will be responsible for the adherence to the terms and conditions of this Agreement by Authorized Users and any third-party provider the Subscriber engages, in particular, if such third-party provider supplies and manages IP addresses."

While it is most probably the responsibility of university IT departments to ensure a robust and secure IT environment, there are many precautions that libraries can take to protect their resources. These include:

- Keeping library credentials up to date--align them with university credentials—require short-lived and hard to guess passwords and institute a requirement to regularly change passwords needed to access library resources.
- Implement multi-factor authentication.
- Institute strict limits on how many attempts to enter passwords on proxy servers and other library access points are allowed in order to quash password guessing bots.
- Institute phishing education (where can we get information about best practices/sources of information.
- Review hacking sites that sell user names and passwords to ensure there are no credentials from your institute. If there are, shut them off.
- On a regular basis ensure that publishers have your correct IP ranges in their A&E System
- •Commit resources for proxy server management
- Exercise detection process before publisher calls you by reviewing your logs regularly looking for:
  - Top consumers of content
  - Users with longest sessions
  - Activity from multiple geographies and countries you know your users aren't in
  - Keep your evidence (configure log / audit files with data you need) and back them up
- Keep your server OS upgraded
- Install the current version of your proxy software
- Keep your system time correct

The EZProxy support site contains a plethora of information for customers regarding proper set-up and security. (Other proxy providers should have similar resources.)

EZproxy Support Site:

https://www.oclc.org/support/services/ezproxy.en.html

•Managing your EZproxy:

https://www.oclc.org/support/services/ezproxy/documentation/manage.en.html

•Securing your server:

https://www.oclc.org/support/services/ezproxy/documentation/example/securing.en.html

EZ Proxy Usage Limit

UsageLimits allow you to set limits on EZproxy usage to comply with content provider requests, minimize the potential for the illicit download of large amounts of content, and limit reductions in access speed.

Content providers will sometimes place limits on the amount of content that users can download during a given time period due to licensing agreements they have with content owners. These limits can be enforced with the UsageLimit directive, which allows you to apply limits to individual resources without altering the amount of content your users can access from other resources.

You can also proactively impose usage limits to keep intruders from downloading large quantities of information with compromised credentials. If content providers detect unusually large quantity downloads, they may block your access to their resources, causing interruptions for your legitimate users. To avoid this, you can set appropriate limits on users' ability to access all resources as a preventative measure. As described in the example tab, it is best to monitor usage before setting these limits so you do not inadvertently prevent legitimate users from having appropriate levels of access to resources.

Finally, if you put appropriate limits in place, high volume users who could potentially slow down access speeds for other users will be limited in how much they can download at one period of time, and thus free up bandwidth for other users to access resources.

https://www.oclc.org/support/services/ezproxy/documentation/cfg/usagelimit.en.html

Audit

Audit logs allow EZproxy administrators to gain insight into a range of user and security related issues. The data collected in these logs is highly customizable and, when used with other security directives in your config.txt, can provide you with a picture of what limits should be set to strike a balance between security and providing your users with the access to the resources they need.

Additionally, this information can be used to determine if users are regularly having difficulty accessing your EZproxy resources. If this is shown to be the case through the recording of numerous failed attempts and eventual denied access to EZproxy, you might consider providing more specific instructions in the form of documentation or tutorials to teach your users how to access resources remotely.

https://www.oclc.org/support/services/ezproxy/documentation/cfg/audit.en.html

We recommend the following security measures as best practices our customers should institute:

1. Information Security Program

a. The Customer should have in place documented policies and procedures, which should be reviewed, and if appropriate, tested and updated, at least annually, covering the administrative, physical and technical safeguards in place and relevant to the access, use, loss, alteration, disclosure, storage, destruction and control of information and which are measured against objective standards and controls ("Customer's Information Security Program").

b. Customer's Information Security Program should:

i. account for known and reasonably anticipated risks and threats, and Customer should, on an ongoing basis, monitor for new threats;

ii. meet or exceed industry best practices; and

iii. ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

c. Customer should promptly remediate any deficiencies identified in the operation, sufficiency or efficacy of Customer's Information Security Program.

d. Customer's Information Security Program should be in writing and, at a minimum, address the following areas:

i. Physical security inclusive of ensuring that physical access to facilities is restricted and controlled to allow access only to authorized personnel, and that such physical access is immediately terminated when no longer needed;

ii. Acceptable use of assets owned by Customer or Customer personnel, and used for the performance of the Services;

iii. Use of mobile and portable devices including ensuring that Publisher data is appropriately protected if stored on such devices;

iv. Access control and management including the identification, authentication and control of access to, and use of, information, facilities, networks, computers and software including prompt deactivation of any credentials when no longer needed or where access presents a security risk;

v. Appropriate logging, monitoring and retention of such logs for all information technology infrastructure, applications and physical security controls and retention of such logs for a minimum of ninety (90) days;

vi. Virus and malicious software detection, response and eradication performed on a timely basis;

vii. Security and system patching including processes for review, testing and implementation of all security related operating systems, devices and production software;

viii. Building, operating, managing and administering systems;

ix. Network controls to prevent and detect malicious activities and segregate physical and logical access;

x. Procedures for appropriate retention, handling and destruction of information including as may be applicable to Publisher information;

xi. Reviews of Customer personnel with access to Publisher data, systems or facilities or with access to Customer systems that allow access to Publisher systems or data (referred to as "Access Personnel");

xii. Reviews, including appropriate background screening, of all Access Personnel to ensure none present a security risk to Publisher or Publisher personnel, data, systems or facilities;

xiii. Change control including provisioning and de-provisioning of services and relevant modifications to access accounts including elevated privilege and service accounts;

xiv. Segregation of duties implemented at key operational points and reviewed and approved as appropriate;

xv. Media destruction using industry standard procedures and processes to certify destruction was performed in accordance with such standards;

xvi. Protection of data at rest and in transmission including requiring transfer via secure network connections, secure transport protocols and implementation of additional controls, including, but not limited to, as may be appropriate, encryption; and

xvii. Appropriate backup, disaster recovery and business continuity plans including, for example, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident