What Does “Bad” Behaviour Look Like?

Suspicious EZproxy Logs and Audit Events

No Breaks: It’s not really possible for a single person to be accessing resources for hours without a break. Certainly not unaided. Since automated access is almost universally prohibited in library license agreements, activity over many hours is considered a red flag. The longer the lack of a break, the more major the red flag is.

Regular Pattern: Typical information searching and access is quite random. One person’s regular activity isn’t going to create a pattern of EZproxy “transfers” or Audit Events that is perfectly consistent over time, such as the same number of seconds or minutes between each event or having close to the same number of transfers for every hour of activity. There will usually be peaks and valleys. A very consistent pattern of activity suggests that access has been automated, which is against almost all license agreements. Another common pattern is activity only or almost entirely during business hours on weekdays: this strongly suggests use in a business setting such as a student’s co-op position or an instructor’s consulting firm. Commercial use of library resources is also pretty much universally disallowed in license agreements so such a pattern of activity is considered a major red flag.

Many IP Address Changes: The typical library patron’s activities shouldn’t require any IP address changes let alone many. Any IP address changes is considered at least a minor red flag. The more changes in a day, the faster they are, and the more extreme they are (such as changing countries), the more major it is.

Valuable Resources: One reason that people unaffiliated with your institution may try to access library resources is they can be extremely valuable. Financial data products (such as Thomson One) or science literature (such as “American Chemical Society” journal articles) are common targets for inappropriate activity, and so accessing only or mostly these kinds of resources is considered a red flag.

How these “red flags” are used: They are already aspects of activity that suggest looking into the activity more to determine appropriateness. There are cases where a pattern will engage in perfectly appropriate activity that raises some red flags. Any general rule is that the more red flags there are (and the “redder” they are), the more likely it is that the activity is inappropriate. There’s no “x strikes and you’re out” rule. Each case is judged by its own details on whether the number and kinds of signs of inappropriate activity actually mean that the activity has been inappropriate, and then what should be done about it. Give the patron the benefit of the doubt.

Simultaneous Sessions: Regular EZproxy users don’t usually have more than one simultaneous session. Having two or three is considered a minor red flag – the more simultaneous sessions they have, the more major the red flag is.

Exceeding “UsageLimits”: EZproxy is a function to set usage limits, by number of transfers and/or number of bytes transferred, and note or block users if these are exceeded within a 24 hour period. If set high enough, it should be uncommon that a single regular patron’s activity will exceed them. For example, Laurier Library’s are set at 5000 transfers or 3500 megabytes. Exceeding these limits is considered a red flag. Exceeding them by a lot, or often, is a major red flag.

Activity Outside Your Domain: Although we certainly have patrons that legitimately access our resources from outside our immediate region, those are in the minority so activity outside the province is a minor red flag, and outside the country is slightly more major. Activity from Russia or China is always a major red flag given that known inappropriate use has typically come from IP ranges in those countries.

Audit Events for Days: Many patrons will log in a few days in a row but most activity is limited to one day only. Seeing at least one Audit Event each day for multiple days in a row is considered a red flag. The more days in a row there are, the more major the red flag is.

Simple Log-In Info: Although most access is now through our institutional usernames and passwords, which tend to be very secure, many are still using 14 digit barcodes numbers and last names (or similar) to log in. Barcode numbers are long but they do have a pattern. And some last names are more common and short than others, such as “smith” or “Lee.” This makes it relatively easy for someone to simply guess at functional access info. This isn’t so much a “red flag” but more of a final confirmation that the legitimate patron wasn’t responsible for this activity.