Chapter 3

Overview of Common Issues and Symptoms

Library science has tackled identifying trends in e-resource access disruptions from a number of vantage points. Many articles have focused on assessing errors resulting from specific technology components, including OpenURL linking, knowledge base metadata, authentication systems, gaps in web-scale discovery coverage, or the usability of discovery services. Others have approached access disruptions through the broader lens of e-resource troubleshooting. Less has been written on attempts to understand access disruption trends holistically, such as through help ticket analyses. Lowry, for instance, notes that only five of the thirty-five articles included in her content analysis of troubleshooting articles "utilized a method of analysis wherein troubleshooting tickets or reports were analyzed in some way" (Lowry 2021a, 165). Similarly, a recent survey of academic libraries showed that while 51 percent of the 143 respondents were tracking e-resource access issues reported at their institutions, only 15 percent had conducted a formal analysis of that data (Lowry 2021b). While strides have been made in recent years to standardize the language around access disruptions, the field is just beginning to develop a shared framework around which the rates and categories of access problems can be compared across institutions.

Without such comparative analyses, it can be difficult to state with certainty which e-resource access disruptions are the most prevalent. Here, discovery and content vendors could help fill in the gaps, contributing to the field with their own analyses of access issues reported and resolved via their support centers. These analyses do not seem to be forthcoming. Instead, librarians must rely upon personal experience, anecdotal stories, and individual case studies to spot larger trends in access disruptions. Fortunately, as Brett states, "Any practitioner who regularly addresses e-resource access problems knows there are common 'types' of problems" (Brett 2018, 198)—and that is what we will discuss in this chapter.

Literature Summary

The earliest studies to attempt to holistically assess the frequency and types of e-resource access disruptions throughout a library's system were availability studies. Availability studies utilize a method of systematic analysis to evaluate how well a library fulfills user item requests. Initially developed to evaluate the availability of physical items in library collections, these studies were subsequently adapted to incorporate e-resource access by Nisonger (2009), Crum (2011), and Mann (2015). In each study, the researchers searched for the full text of a predetermined sample of e-resource citations using either the library catalog or A&I databases equipped with the library's OpenURL link resolver. The results were then analyzed to determine the rate of success finding the full text and to identify trends that contributed to the failures. Mann (2015) is particularly noteworthy for being one of the first to develop a conceptual model to categorize e-resource access failures, as well as the first to attempt to quantify the effectiveness of troubleshooting by comparing availability results before and after error remediation. Mann and Sutton (2015) followed up this study with another incorporating aspects of usability testing, resulting in an expansion of Mann's original concept model to include both system and human errors.

During the same year, studies analyzing access disruptions reported via help tickets, chat transcripts, and ILL requests began to emerge. Browning (2015) analyzed problem-report e-mails received from March

through December 2013 by Auroria Library; Wright (2015) reported on findings from a study of University of Michigan's new problem ticket tracking system at ALA midwinter; Ashmore, Allee, and Wood (2015) used canceled ILL requests during the 2012–2013 school year at Samford University Library to identify link resolver errors; Ashmore and Macaulay (2016) expounded upon the results of the 2015 study to identify three core types of link resolver problems; Goldfinger and Hemhauser (2016) studied a random sampling of problem tickets submitted between March 2010 and October 2013 at the University of Maryland, College Park; Enoch (2018) analyzed error reports submitted for e-resource access issues within the University of North Texas Libraries' discovery service; Kimbrough (2018) analyzed chat transcripts to identify e-resource problems frequently encountered by patrons at Georgetown University Library; Baskaran (2019) examined chat transcripts at North Carolina State University Libraries to identify e-resource access problems for further investigation; Lounsberry, Wood, and Thornton (2021) used ILL data at LSU to identify access issues in a proactive manner; and, finally, Foster (2021) categorized problem alert tickets in JIRA using a locally developed controlled vocabulary at Ohio State University. The metrics and disruption trends gathered during these studies were used to inform many local practices, including decisions on cleanup projects, staff time allocations, troubleshooting workflows, and acquisitions.

Like Foster (2021), many of these studies developed local schemata to classify their access issues within their analyses. However, as Browning (2015) points out, the classification process was often time-consuming and "allowed for personalization and creativity" (32), resulting in subjective, institution-specific categories. Goldfinger and Hemhauser expressed the limitations of these localized schemata, stating the "lack of controlled vocabulary for problem types among librarians impedes the ability to compare e-resource access problem experiences with other institutions," specifically describing their efforts to compare the University of Maryland's results to similar analyses at other institutions as "comparisons of 'apples to pears' rather than apples to apples" (Goldfinger and Hemhauser 2016, 92). In response, they offered up their own classification schema as a standardized way to describe and categorize e-resource access issues.

Brett (2018) subsequently used their categorizations to classify 305 help tickets at the University of Houston Libraries and compare the results to that of the University of Maryland, College Park. Brett concluded that the results "demonstrate that libraries experience similar types of access problems across institutions" and that "a standardized vocabulary for categorizing e-resource access problems would benefit the profession by improving troubleshooting practices and problem reporting to vendors" (Brett 2018, 203). Similarly, Lowry (2020) utilized Goldfinger and Hemhauser's classification schema to code troubleshooting tickets at the University of Alabama Libraries in order to compare findings among the three research institutions (University of Houston, University of Maryland, College Park, and the University of Alabama). The study confirmed that "certain types of access problems do occur at similar rates among research institutions, despite the likely differences in workflows, tools, management styles, and varying collections among them" and that the "two most common problems at all three libraries fell into the categories of KB/Link Resolver or Platform" (Lowry 2020, 29, 31). Finally, Gould and Brett (2020) performed a similar analysis for help tickets at Texas A&M University (TAMU) and the University of Tennessee, Knoxville (UTK) and discussed the results in comparison to previous studies. They discovered that "KB/Link Resolver, platform-related, and user-error access problems each accounted for large percentages of total problems at both institutions" (Gould and Brett 2020, 195), a result consistent with the findings of Goldfinger and Hemhauser (2016) and Brett (2018). Proxy- and IP-related problems were also flagged as constituting a large percentage of the reported issues.

Common E-resource Access Issues

Device and Network

The search and discovery process always begins with a user's individual technology components—that is, user- or patron-controlled components. This includes items like the user's device, internet or network connection, browser, and browser settings. E-resource access issues originating within these components can present symptoms anywhere throughout a user's discovery journey but are typically experienced at either the very beginning or the very end of the process. The symptoms also frequently cannot be reproduced by the troubleshooter, which can make diagnosing them quite difficult. Since access issues originating from user-controlled components are particular to the user's device and network setup, they require action by the user in order to be resolved. Thus, they are considered to be within the user's sphere of control.

Common causes and symptoms originating from each component include the following:

- Device
  - Causes
    - The user's device is running an old or unsupported operating system.
    - The user's device does not have the appropriate software for viewing or interacting with the library resource (e.g., does not have

a PDF viewer or reader with DRM software, such as Adobe Digital Editions, installed).
    - Symptoms
        - Slow upload and download times.
        - Inability to open or view downloaded file types.
- Network and internet connectivity
    - Causes
        - The user's network connection is slow, spotty, or experiences high latency (delays in transmitting and processing network data; this is common with satellite internet).
        - The user's satellite internet service providers' proxy or VPN (used to mitigate latency issues) interacts negatively with the library's authentication system, such as EZproxy.
        - The user's network utilizes firewalls or other network security features that interact negatively with the library's authentication system.
    - Symptoms
        - Timeout errors.
        - Lag.
        - Slow upload and download times.
        - Dropped proxy or authentication.
- Browser and browser settings
    - Causes
        - The user is using an older browser or a browser unsupported by the vendor platform.
        - The data stored in the browser's cache or cookies is interacting negatively with the vendor platform or library resource.
        - The browser's pop-up blocker is preventing content from loading, or the browser's security settings are blocking safe sites from being accessed.
    - Symptoms
        - Slow loading times.
        - Content or web pages not loading on the vendor platform.
        - Error messages or security warnings.

Discovery Service

A library's discovery service is usually powered by three main reservoirs of metadata: the ILS or catalog, knowledge base, and central indexes.

CATALOG

Access disruptions originating from a library's catalog or ILS generally concern locally controlled MARC records containing incorrect or incomplete bibliographic information, coverage dates, or URLs. MARC records may have also been erroneously loaded or unsuppressed for content the library does not currently own or subscribe to. When library users encounter faulty metadata from these MARC records within their OPAC or discovery service, they may experience

- broken links
- proxy error messages
- missing or unnecessary prompts for authentication
- paywalls on the vendor platform

Fortunately, once the problem is isolated to the appropriate MARC record, a troubleshooter is able to take swift action to resolve the issue because these records are typically managed by the library itself. This is often not true when it comes to knowledge bases and central indexes.

KNOWLEDGE BASE

Unlike a catalog, a knowledge base contains more than just bibliographic metadata; it also contains data that describes specific instances of e-resources, including the resource's platform, vendor, coverage dates, and access model, such as which packages or collections it appears in. Since the knowledge base receives this data directly from publishers or content providers, each of which has its own internal standards for representing e-resource information, the quality of the metadata can vary from provider to provider. Some knowledge base vendors attempt to augment or normalize this data in order to keep it consistent across providers, but this process can also introduce additional errors. Furthermore, providers frequently make changes to their platforms, the content of those platforms, and the way that content is packaged and sold to libraries, making it difficult for knowledge base vendors to keep up with the changes. As a result, there is often a lag time between when a collection or resource is modified on the provider's platform and when its metadata is modified within the knowledge base. This can result in scenarios such as the following:

- broken links caused by outdated URLs or incorrect linking information
- broken links caused by incorrect bibliographic or citation information (e.g., wrong ISSN/ISBN)
- links defaulting to a provider's home page instead of the individual article or title
- packages missing titles that have been added
- packages including inaccessible titles or titles that have been removed

Because a knowledge base is often utilized in a number of components, including ERMSs, discovery services, link resolvers, and e-journal A–Z lists, these symptoms can display in several places. This means testing access via different access tools may result

in the same error message or broken link. Not only does this limit the alternative routes troubleshooters can provide to problem reporters for accessing their desired content, but it also prevents troubleshooters from cross-checking the metadata within the library's access infrastructure. Instead, troubleshooters will need to do that through an outside source, such as OCLC or Ulrich's Periodicals Directory, or by going directly to the vendor or resource itself.

ELECTRONIC RESOURCE MANAGEMENT SYSTEM

An electronic resource management system, or ERMS, is powered by a knowledge base and is used to capture both electronic holdings and other e-resource-relevant acquisitions data. While librarians do not have the ability to directly modify the metadata contained within a knowledge base, they can use the ERMS to indicate which collections, packages, or individual resources their library subscribes to and the appropriate coverage dates for each one. For instance, a knowledge base may contain a collection of front file e-journals available for subscription from a publisher. A library may subscribe to only one of these journals, and only from the year 2015, which is when it first began its subscription. Through the ERMS, a librarian can select (or "track" or "activate") the single journal title from the collection and change its coverage dates to 2015–present in order to accurately represent the available access. The ERMS can also control other aspects of access and display, such as whether or not to include a proxy prefix for titles or collections, and the ability to include descriptions of access restrictions, such as seat or usage limitations. In other words, the knowledge base provides a reservoir of metadata from which a library can draw, but it is through an ERMS that the library indicates which metadata is relevant and adds additional information specific to their situation. Since edits cannot be made to the knowledge base itself but can be made to library selections, such as holdings and coverage dates, this knowledge management system has blended control.

Access disruptions originating from an ERMS, therefore, can be caused either by faulty metadata in the knowledge base, the symptoms of which we covered earlier, or from erroneously chosen holdings populated by a librarian. These could include

- incorrectly selected titles
- incorrect coverage dates
- missing proxy prefix
- erroneously added proxy prefix

These issues can result in library users encountering paywalls and proxy error messages or being unable to find accessible content within the library's discovery service.

LINK RESOLVER

Many ERMSs are sold with link resolver functionality, but link resolvers can also be sold as stand-alone products or in conjunction with other access tools, such as e-journal A–Z lists. Like ERMSs, link resolvers consist of a knowledge base containing e-resource and linking data and an administrative interface through which a library may select its holdings. These holdings are then used to populate access tools, such as e-journal A–Z lists and discovery services. As a result, access issues are caused either by faulty metadata within the knowledge base or by incorrect holdings chosen via the administrative interface. Symptoms would also be identical to those experienced by both a knowledge base and an ERMS, including broken or misdirecting links, paywalls, proxy error messages, and missing or erroneously included content.

CENTRAL INDEX

Missing, erroneous, and outdated metadata is also the primary cause of access issues originating from a central index. Like a knowledge base, a central index ingests metadata from hundreds of publishers and content providers, each of which has its own standards for representing e-resource metadata. This means the metadata quality often varies according to who is providing it and suffers from issues similar to those of a knowledge base regarding normalization, missing content, and lag time between when a resource is modified on a platform and when it is updated within the index. However, unlike a knowledge base, a central index is primarily used to provide discoverability for the contents comprising a larger work, such as articles, abstracts, book chapters, images, video segments, and so on. This distinction is important to remember because a knowledge base and a central index express similar symptoms—most typically, broken or misdirecting links—when their metadata is faulty, but the issue may need to be reported to a different vendor or support portal, depending on which company the library has contracted with for each. It is often easiest to identify whom to contact based on what type of discovery record is experiencing the problem.

Authentication

IP AND VPN AUTHENTICATION

IP address recognition has been the primary method of authentication to online library resources since the mid-1990s. For on-site users, the process is virtually invisible. They navigate to the e-resource while connecting to the internet via their institution's network (and thus IP address), and as long as the correct IP ranges have been registered with the vendor platform,

the user is granted access without needing to log in or otherwise further identify themselves. However, off-site access using IP authentication has been more fraught. VPNs, for example, require users to download and utilize specialized software to make it appear as though their computer is on site. Even then, having navigated the installation process, users may still be denied access to content if the VPN is configured to utilize split tunneling, where only certain traffic is routed through the institution's IP ranges.

IP authentication is also susceptible to large-scale access disruptions. Any issues with an IP address will affect everyone utilizing that address, be it an individual user or an entire campus department building. An increasingly common example is unauthorized text and data mining. If a user engages in behavior that goes against a resource's licensing agreement, the vendor may choose to disable access to that resource to stop the behavior. Since authentication happens with the IP address, the vendor cannot block the individual user and is instead forced to disable access to the entire IP address. If that IP address is for the VPN or proxy, this block can adversely affect the access for everyone off site.

Errors also happen on the administration side. IP ranges may not be submitted to the vendor or entered into the platform to enable access. Also, IP ranges may change unexpectedly. As Dowling explains,

> Many of our institutions have, over the years, added additional campuses and additional networks, or have changed networks, requiring a continual need to revise the IP ranges we report to every one of our publishers. At the same time, the publishers have had to manage these continual changes from a growing number of institutions. The process has become time-consuming for everyone involved and increasingly prone to error. (Dowling 2020, 43)

PROXY AUTHENTICATION

Proxy servers can be either locally hosted by the library or remotely hosted by a vendor or other third-party entity, such as a consortium. Depending on where the proxy server is hosted, an institution may not be able to make direct edits to the server or its configuration files. Like all servers, proxy servers can experience downtime or lapses in access as a result of technical issues. They are also prone to the same IP authentication issues outlined earlier. However, proxies can also run into issues that revolve around the configuration files.

Library proxies require the maintenance of several configuration files in order to function, including one that contains the URLs, hosts, and domains of the e-resources licensed for IP authentication and access. These URLs, hosts, and domains are grouped by platform into entries called stanzas and need to be frequently updated in order to keep pace with changes to the platform. Access issues originating within this configuration file are generally the result of missing, erroneous, or incomplete stanzas and will result in users being confronted with a proxy error message or being forced to authenticate for open or free resources.

FEDERATED IDENTITY MANAGEMENT

Federated identity management is a more reliable and secure way to authenticate users compared to methods relying on institutional IPs. However, FIM authentication still has its challenges. Commonly identified access issues related to FIM authentication have to do with users finding and navigating the Where Are You From (WAYF) menu. While FIM-enabled platforms allow users to arrive at the content through any means, even through links from the wider web, users still need to identify which institution they are affiliated with when logging in. This is generally done using a WAYF menu, a drop-down menu that lists every available option. This list is potentially very long, and understandably users can encounter difficulty finding their correct institution if it is missing, confusingly labeled, or hard to find. Although improvements have been made to simplify the WAYF menu, including search features, a persistence service, and institutional naming standards, institutions still prefer to have users avoid the WAYF menu whenever possible. As a result, many institutions are using WAYFless URLs to bypass the menu entirely.

WAYFless URLs are specially formatted URLs that communicate the users' institutional affiliation to the service provider, thus redirecting the user to the appropriate log-in screen without having to select it from a list. WAYFless URLs are used primarily within institutional portals or discovery systems. Users navigating to the platform from the web would still need to use the WAYF menu. Also, depending on how the WAYFless URLs are constructed, they can be prone to breaking as a resource's web location information changes. This means a user may still be confronted with a WAYF menu even when using a WAYFless URL.

Finally, it is worth noting that not all vendor platforms support FIM, particularly smaller society publishers that may not have the staff bandwidth for implementation. Therefore, FIM is often utilized alongside other authentication methods in order to provide robust coverage. This can lead to additional confusion for users, who must maneuver through multiple authentication methods depending on the resource.

Vendor Platform

Access issues originating from a vendor platform fall into two categories: technology issues with the

Table 3.1. Common access issues and their solutions

Issue	Reason	Solution
User Error	The patron navigated to the resource from outside the library's access tools.	Educate the patron on how to access and use library e-resources.
	The patron incorrectly interpreted a library's holdings.	
	The patron is unfamiliar with using features of library e-resources.	
	The patron is attempting to access a resource from the wrong browser or without the necessary software.	
	The patron is no longer an authorized user.	
Vendor Cut Access	Your library does not have access to an e-resource due to a payment issue.	Work with the vendor and the library's acquisitions staff to process payment.
	The vendor incorrectly thought your library does not have access rights.	Contact the vendor to reestablish access on the platform.
Incorrect E-resource Implementation	Your library does not own or subscribe to the e-resource. You verify, via acquisitions or other records, that it should not have been made discoverable.	Remove the e-resource from discovery.
	Access was never established on the vendor platform when the e-resource was acquired.	Supply the vendor with the necessary information, such as IP addresses, to complete registration.
Broken or Misdirecting Link	Incorrect metadata in a link from research guide, ILS, or database A–Z list leads to an error message or being directed to the wrong content.	Navigate to the vendor platform to attempt to find the desired content elsewhere on its platform. Inform the patron of the alternate route. Change local records to reflect updates.
	Incorrect metadata in a link from knowledge base or central index leads to an error message or being directed to the wrong content.	Navigate to the vendor platform to attempt to find the desired content elsewhere on its platform. Inform the patron of the alternate route. Whether or not you find the content via an alternate route, contact the e-resource or access tool vendor to update its metadata.
	The e-resource URL is outdated due to a vendor website architecture change or content being removed.	Contact the vendor of either the access tool or e-resource to alert it of the outdated link with incorrect metadata.
	The e-resource record is used only for internal purposes and the access mechanism is not actively updated.	Suppress or otherwise hide the e-resource record from patron view.
Incorrect Holdings	Holdings do not accurately represent the library's access entitlements: • Incorrect coverage dates • Missing titles the library has subscribed to or purchased • Including titles not subscribed to or purchased by the library	Use acquisitions records, vendor title lists, or licenses, etc., to update your library's holdings within your access tools.
Authentication: EZproxy	An EZproxy prefix was not added to an e-resource's URL; patrons are therefore hitting a paywall.	Add the EZproxy prefix to the e-resource's URL.
	An EZproxy prefix was erroneously added to an e-resource's URL; patrons are receiving an EZproxy error.	Remove the EZproxy prefix to the e-resource's URL.
	The e-resource's stanza is not included in the EZproxy configuration file.	Add the EZproxy stanza to the EZproxy configuration file.
	The stanza for the e-resource in the configuration file is incorrect, e.g., missing host or domain name.	Correct the EZproxy stanza in the EZproxy configuration file.

Table 3.1 continued on page 20

Table 3.1. Common access issues and their solutions (cont.)

Issue	Reason	Solution
Authentication: VPN	Your institution's IT department has implemented split tunneling for your institution's VPN. The VPN is no longer routing e-resource traffic through the VPN.	Explain to patrons that the VPN no longer works as it used to and that they should not use it to access e-resources. In addition, work with your IT department and explain how the issue is confusing and an inconvenience to patrons and library staff. They may or may not choose to change how traffic is routed.
Authentication: FIM	Your institution's name is missing, confusingly labeled, or hard to find on the WAYF list on the e-resource's platform.	Contact the e-resource vendor to resolve this issue.
Authentication: Username/ Password	The patron has not created a necessary account with a particular e-resource and is attempting to log in with their library credentials.	Educate the patron on how to create the necessary account and to use it in the future to access the e-resource.
	A vendor has reset the username/password required for your library to access an e-resource without notifying your library.	Update the username/password for your patrons.
Unauthorized Text and Data Mining	A vendor has deliberately denied your library access to an e-resource due to unauthorized text and data mining.	Contact the patron to explain the situation and alert them of future requirements for compliance. Contact the vendor to tell them that you have notified the patron of their unauthorized use.

platform itself, such as the server being offline or the platform relying on old or obsolete technology, and deliberate denials of access by the vendor, usually due to a belief that the library no longer has rights to access the content. For technology issues, the symptoms are what you might expect to find with any website, such as slow loading times, error messages, and pages, scripts, or images not displaying correctly. These symptoms are reproducible and can be very widespread, affecting not just your library and users but also libraries and users from across the vendor's consumer base. They also require action on the part of the vendor in order to be resolved.

Fortunately, these platform issues are relatively rare and, issues with obsolete web technology aside, tend to be addressed quickly by the vendor. Instead, troubleshooters are much more likely to encounter deliberate denials of access. Acquisitions issues, such as missed invoices or incorrectly applied payments, are the most frequent reason a vendor would revoke access, but issues with content migration, excessive or suspicious usage and download activity (e.g., unauthorized scripting or text and data mining), and vendors updating their own websites or customer data sets can also cause deliberate access denials.

Common Access Issues and Their Solutions

In table 3.1, we have compiled some of the most commonly experienced access issues and their solutions. This list is not comprehensive but can act as a reference tool by briefly summarizing solutions to common problems encountered by troubleshooters.

References

Ashmore, Beth, Emily Allee, and Rebekah Wood. 2015. "Identifying and Troubleshooting Link-Resolution Issues with ILL Data." *Serials Review* 41, no. 1: 23–29. https://doi.org/10.1080/00987913.2014.1001506.

Ashmore, Beth, and David Macaulay. 2016. "Troubleshooting Electronic Resources with ILL Data." *Serials Librarian* 70, no. 1–4: 288–94. https://doi.org/10.1080/0361526X.2016.1153336.

Baskaran, Dharini. 2019. "Chat Ref Analysis—Exploring and Analyzing Chat Reference Transcripts Specifically Relating to Acquisitions and Discovery." *Serials Review* 45, no. 3: 132–36. https://doi.org/10.1080/00987913.2019.1647775.

Brett, Kelsey. 2018. "A Comparative Analysis of Electronic Resources Access Problems at Two University Libraries." *Journal of Electronic Resources Librarianship* 30, no. 4: 198–204. https://doi.org/10.1080/1941126X.2018.1521089.

Browning, Sommer. 2015. "Data, Data, Everywhere, nor Any Time to Think: DIY Analysis of E-resource Access Problems." *Journal of Electronic Resources Librarianship* 27, no. 1: 26–34. https://doi.org/10.1080/1941126X.2015.999521.

Crum, Janet A. 2011. "An Availability Study of Electronic Articles in an Academic Health Sciences Library." *Journal of the Medical Library Association* 99, no. 4 (October): 290–296. https://doi.org/10.3163/1536-5050.99.4.006.

Dowling, Thomas. 2020. "We Have Outgrown IP Authentication." *Journal of Electronic Resources*

Librarianship 32, no. 1: 39–46. https://doi.org/10.1080/1941126X.2019.1709738.

Enoch, Todd. 2018. "Tracking Down the Problem: The Development of a Web-Scale Discovery Troubleshooting Workflow." *Serials Librarian* 74, no. 1–4: 234–39. https://doi.org/10.1080/0361526X.2018.1427984.

Foster, Anita K. 2021. "A Controlled Vocabulary for an Electronic Resources Problem Reporting System: Creation, Implementation and Assessment." *Library Resources and Technical Services* 65, no. 1: 23–32. https://doi.org/10.5860/lrts.65n1.23-32.

Goldfinger, Rebecca Kemp, and Mark Hemhauser. 2016. "Looking for Trouble (Tickets): A Content Analysis of University of Maryland, College Park E-resource Access Problem Reports." *Serials Review* 42, no. 2: 84–97. https://doi.org/10.1080/00987913.2016.1179706.

Gould, Elyssa M., and Kelsey Brett. 2020. "A Tale of Two Universities: Electronic Resources Troubleshooting Comparisons." *Serials Librarian* 79, no. 1–2: 192–99. https://doi.org/10.1080/0361526X.2020.1760184.

Kimbrough, John. 2018. "Technical Services and the Virtual Reference Desk: Mining Chat Transcripts for Improved E-resource Management." *Serials Librarian* 74, no. 1–4: 212–16. https://doi.org/10.1080/0361526X.2018.1428482.

Lounsberry, Megan, Nicole Wood, and Bonnie Thornton. 2021. "The Power of Cross-Unit Data Sharing: Nontraditional Uses for ILLiad." *Serials Librarian* 80, no. 1–4: 131–34. https://doi.org/10.1080/0361526X.2021.1879759.

Lowry, Lindsey. 2020. "Where Do Our Problems Lie? Comparing Rates of E-access Problems across Three Research Institutions." *Serials Review* 46, no. 1: 26–36. https://doi.org/10.1080/00987913.2020.1733173.

———. 2021a. "Exploring the Evidence-Base for Electronic Access Troubleshooting: Where Research Meets Practice." *Journal of Electronic Resources Librarianship* 33, no. 3: 156–69. https://doi.org/10.1080/1941126X.2021.1949153.

———. 2021b. "Fighting an Uphill Battle: Troubleshooting Assessment Practices in Academic Libraries." *Library Resources and Technical Services* 65, no. 1: 4–13. https://doi.org/10.5860/lrts.65n1.4-13.

Mann, Sanjeet. 2015. "Electronic Resource Availability Studies: An Effective Way to Discover Access Errors." *Evidence Based Library and Information Practice* 10, no. 3: 30–49. https://doi.org/10.18438/B88C82.

Mann, Sanjeet, and Sarah Sutton. 2015. "Why Can't Students Get the Sources They Need? Results from a Real Electronic Resources Availability Study." *Serials Librarian* 68, no. 1–4: 180–90. https://doi.org/10.1080/0361526X.2015.1017419.

Nisonger, Thomas E. 2009. "A Simulated Electronic Availability Study of Serial Articles through a University Library Web Page." *College and Research Libraries* 70, no. 5 (September): 422–445. https://doi.org/10.5860/0700422.

Wright, Jennifer. 2015. "Electronic Outages: Who Broke It? How Long Was It Broken? We're . . . Tracking That, Right? Report from ALA Midwinter 2015." *NASIG Newsletter* 30, no. 2. https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1662&context=nasig.