**Beyond traditional literacy instruction: toward an account-based literacy training curriculum in libraries**

by David Cirella
*Computers in Libraries Dec. 2012*

As mainstream technology and popular online services have evolved beyond traditional business applications and basic internet browsing, so have the educational needs of our patrons. While information literacy training has successfully ensured that patrons are equipped to evaluate resources and satisfy their information needs, recent shifts in patron habits and the increased popularity of online services require enhanced training. Specifically, a new account-based literacy training curriculum, one that incorporates existing best practices and procedures, is needed to provide patrons with the training that they have come to expect from library computer and technology classes. Account-based literacy seeks to ensure that patrons are equipped to protect their privacy, preserve their data, and have a sense of efficacy in the face of the digital migration of their personal information, communications, and data.

## Account-Based Literacy

Account-based services are those that require some level of user contribution in the form of creating an ac count, entering personal information, or contributing content. A diverse group, account-based services include a wide variety of sites commonly used by patrons, including online shopping sites, social networks, photo- and video-sharing sites, banking and financial sites, government services, and cloud-based storage. While the requirement to create an account is by no means a recent trend, there does exist a convergence of issues at this time that necessitates an enhanced training with a focus on practices that protect privacy and data.

The specific dangers that patrons face when using account-based services are the loss of privacy, remote account breaches, and loss of personal data. While these dangers are not in and of themselves new, the extension of account-based services into many parts of everyday life makes it essential to address them.

Account-based literacy is based on a nexus of ideas including information literacy, media literacy, digital literacy, and computer security practices. There exists a need to provide patrons with training that speaks to the dangers inherent in the use of online services. Account-based literacy training seeks to ensure that patrons are able to successfully navigate and use these ubiquitous web services while protecting themselves, their personal information, and their data.

## Needs

Recent trends have resulted in patrons of all skill levels accessing account-based online services. As a librarian providing technology and computer instruction to public library patrons, I have witnessed an evolution in the needs of patrons who are new to computers in general and online-based services in particular. With the mass appeal of social networking, it is not uncommon for a person's first online act

to be the creation of a public profile rich in personal information and data such as photos. In the past, the uninitiated would gradually branch out from less public acts, such as web browsing, before delving into activities that require the disclosure of personal information. There now exists a danger in new users lacking the knowledge needed to assess the implications and risks involved with transferring personal information and data to online services. Compounding the lack of knowledge is the trend to embrace the full gamut of services, whether comfortable or not, in order to interact with friends and family or to gain the convenience of enhanced online services.

In contrast with the past, many of the gateway online activities commonly sought out by patrons require the creation of an account and disclosure of personal information. Current trends and advances in user-friendly services and consumer electronics contribute to their increasingly deep reach into the lives of all users.

The wide adoption of smartphone and tablet devices, coupled with the categorical reliance on account-based cloud storage services, puts an entirely new facet of user data at risk. The ease of use and pre-eminence of account-based services on mobile devices, including popular e-reader hardware, open users' privacy and data up to an unprecedented risk from external forces. These dangers are heightened in the case of the expanding group of users whose computing experience is largely confined to a single tablet device, risking loss of data and privacy with a single exploit.

The increasing amount of private, valued information moving online, coupled with the vulnerability of major account-based services illustrated by recent high-profile hacks, has made it clear that users must be proactive in protecting themselves.

**Account-Based Literacy Training**

The three chief goals of account-based literacy training include protecting accounts, protecting privacy, and preserving data.

Protecting accounts--The most important practice for patrons to observe is the strict avoidance of password reuse for different services. The linkage of online accounts, through email addresses or common logins, coupled with large-scale security breaches at major service providers, can turn a break-in at a single service into an exploit that has far-reaching consequences for an online life. Unique passwords must be used with each account from the start to avoid cascading account breaches in the event of a compromise.

When creating passwords for each service, good password practices must be employed to increase security, making individual accounts less vulnerable to attack. Simple passwords such as words found in the dictionary must be avoided. Passwords can be made stronger through the use of lowercase and uppercase characters, numbers, and symbols. Passwords that are longer in length are also less vulnerable to attack. A tactic for creating long passwords that are somewhat easy to remember is the use of a pass-phrase sentence that has some relevance in the user's life. For example, puppy@Grandmas4vacation constitutes a strong, 23-character password, using uppercase and

lowercase letters, a number, and a symbol. This pass-phrase would be easier to remember than a random password of equal length and complexity but just as difficult to guess.

Patrons should be advised to consider how easily the answers to password-recovery questions can be found. Whether or not a piece of information is obtainable online must be considered when creating password-recovery answers for each account. If a patron discloses a seemingly benign piece of information such as a pet's name on a social networking site and then uses the pet's name as an answer for a password-recovery question, it creates vulnerability that they may not have considered otherwise.

The linking of accounts through common usernames multiplies the risk of any breaches and reinforces the need for good practices across services. More advanced users can explore the use of password keepers and two-factor authentication where available.

Protecting privacy--The evaluation of services and the information that the services request when creating an account is an important consideration. For each account, the patron must consider what the service is, what personal information would be reasonably needed by that service, and how the entered information is likely to be used.

A hierarchy of privilege regarding personal information should be observed dependent on the needs of the service. While it is reasonable for a bank or an online tax-filing service to ask for billing information and a Social Security number, it is not reasonable for a hobby website to require those things. In a less drastic scenario, a social networking site may ask for occupation, high school, and place of birth when creating a profile. If patrons don't want to be associated with their places of birth, they must consider that the service is asking for this information in order to facilitate public searching and finding. This consideration of why a service is requesting information, how it will reasonably use the information, and if it is necessary to gain access will go far toward protecting the user's privacy.

Additional considerations include service-specific privacy settings that limit or publicly expose information such as location, email address, phone number, shopping history, or viewing preferences. Each service has different processes that must be followed in order to limit public access to contributed data. The concept is complicated further by the tendency of these services to default toward sharing more and enacting frequent changes to privacy agreements, often with little or no explanation.

The linking of disparate accounts by third-party data miners through common usernames and public information, with the ability to tie online accounts together into a coherent, single profile, needs to be discussed with patrons. While the user might feel secure in disclosing small bits of personal information within different services, automated data miners or a determined individual can often make connections between seemingly unconnected accounts. The end result may be a much fuller view of users' personal lives than they consciously disclosed in each separate setting. By being aware of this eventuality, patrons can actively consider how and what they are comfortable sharing around the web.

Preserving data--While data preservation is a concern in all settings, the danger of data loss when the user no longer has physical control over the storage medium is increased. Patrons must be vigilant in keeping personal backup copies of any data held in online services. While many online services currently provide space for user data sharing, the protection and access to user data may not always be

a priority for the operators of such services. As history has shown, former internet heavyweights such as GeoCities and Friendster can disappear overnight, taking user data with them. Numerous photos that are uploaded directly to and shared exclusively within Facebook are in danger of being lost if the service were to suffer from outages or to change its business model. If users are not keeping backup copies of the data created in and held in account-based services, they are in danger of losing their data.

This issue is made worse when using mobile devices that exclusively rely on account-based services hut have no simple backup option. Data created in mobile apps is often held online and accessed by user accounts. Patrons must be aware of and use data export tools to keep local backup copies of all valuable data.

**Outcomes**

The need for account-based literacy training grew out of a series of computer and technology classes at the West Haven Public Library, a midsize library in Connecticut serving a population of 56,000. Through the development of a curriculum covering a diverse range of technology topics and an ongoing dialog with patrons of diverse skills, training that focused on account-based issues emerged as a consistent need. Questions from patrons regarding a wide range of specific services accompanied by reluctance, fear, and feelings of helplessness in the face of recent publicized exploits solidified the need for such training.

While specific classes on computer and internet security have been well-received, the principles of account-based literacy lend themselves to integration with other related topics. Classes that primarily focus on internet basics, social networking, and job searching provide ample teachable moments to discuss account-based literacy principles as they relate to specific services and applications. This integration allows for the discussion of pragmatic steps that can he taken by patrons as they are introduced to new services, providing them with the literacy they need when using online services.

~~~~~~~~

David Cirella is a librarian working in the technical services department of the West Haven Public Library in Connecticut. His professional interests include user instruction, information technology, web services, and outreach. He can be reached at decirella@gmail.com.

Cirella, D. (2012). Beyond Traditional Literacy Instruction. *Computers In Libraries*, *32*(10), 5-8.
~~~~~~~~