Malcolm Harris
LIS 258
Discussion 3

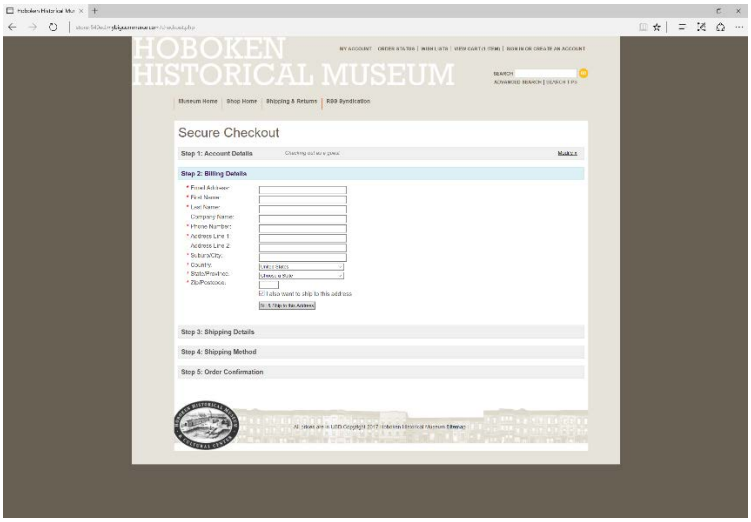
Museum - Partner Observation Assignment 3

Dealing with the security of data that a museum collects through a variety of sources, can be difficult if there is not an initiative taken to address that aspect of museum administration or if the operations of the museum are not extensive enough to provide proper security to digital information. For the Hoboken Historical Museum, they are in a 'bare-bones' position of not having many aspects to their public relations, simply involving the collection of data such as names, addresses, numbers, emails, etc. There is nothing of note from their website that shows the organization's commitment to security when it comes to data collection for some of their general sections.

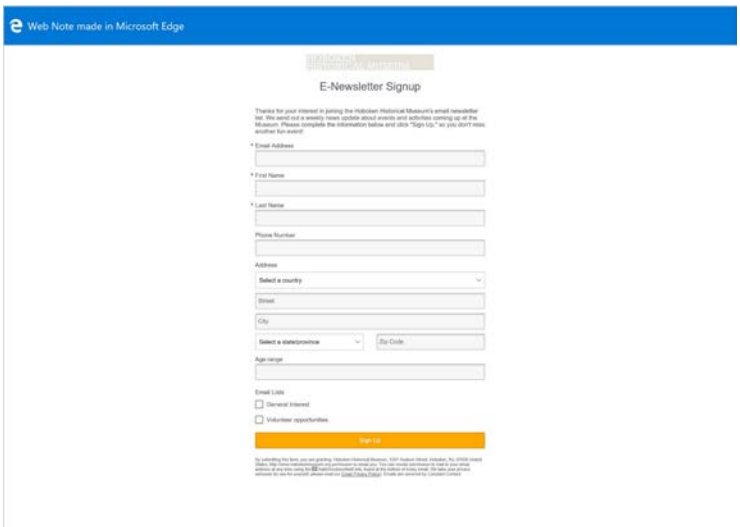
Two things that could be implemented by the museum would be the development and displaying of private security policies on their website, and the use of an internal audit to assess the possible risks that the museum has with data security. For security policies, being able to have information that the public can see that shows what the website or institution has to protect individual information that they collect is just the basic way to prevent any possible liability for data breaches and stolen information. Having all of the areas within an organization covered as to how the data is collected, stored and used is the clearest way to prevent misuse by third-party entities or museum staff that interact with that information. Cherie L. Givens (2014) writes the following statement about crafting security policies in *Information Services Today: An Introduction*: "A well-written private policy explains what information is being collected, how the information is used, and with whom it may be shared" (p. 352). Whether the patron information being collected is in the hundreds of thousands per year or the hundreds, there has to be accountability towards where that information goes and who has access to that personal data.

For the use of an internal audit, understanding what areas of the organization are lacking when it comes to security and data management is necessary to prevent outside entities from covertly funneling information out of a well-intended organization into the hands of those who would look to misuse that data. Having this conducted on a reoccurring period of time also guards against accusations of mismanagement and carelessness with data collection if something such as a data breach or leak should happen, whether incidental or intentional.

For the Hoboken Historical Museum, the lack of data security that can be focused to two areas: the “E- Newsletter” sign up and the museum shop checkout pages. While the “E-Newsletter” provides a private policy link to the web program hosting the page, there is no data security policy shown from the museum directly. For the museum shop, neither the museum nor the web program hosting the shop items and subsequent checkout phase have any policies shown towards data collection or privacy. Either they both should show a museum data privacy policy on those specific pages, or it should be placed on the first pages of both the main museum page and shop page.




HHM shop page, no private policy listed, no secure URL checkout




HHM e-newspaper signup. Constant Contact private policy link, endorsed by the museum

Reference

Givens, C. L. (2014). “Information privacy and cybersecurity.” From *Introduction services today: An introduction*. Hirsch, S. ed. (p. 352-353). Rowman & Littlefield, 2015, Lanham, MD