Library Tech Security

Contacts

* [John Kronenburg](mailto:jkronenb@mail.nfls.lib.wi.us?subject=Library%20Tech%20Security): Nicolet Federated Library System *IT Coordinator* (920)448-4412
* [Dave Bacon](mailto:dbacon@mail.owls.lib.wi.us?subject=Library%20Tech%20Security): OWLSnet *Network Administrator* (920)832-6193

Passwords

* Do not share with anyone.
* Never say out-loud (i.e. talking with Dave/John or new staff) unless you do it quietly when you are sure no one is around.
* Never have a written password out in view of others.
  + Do not let anyone see where you keep it.
  + Do not set paper down where others can see it.
  + Do not leave anywhere (it is easy to get distracted and walk off without the paper).
* Do not enter password on computer if anyone can see what you are typing.
* Never set computer or program to “Remember password” (do not check that box!), especially in Sierra.
* Never give password to any “tech support” or “company representative” (except maybe Dave or John) because an official technician will never ask. It is a tell-tale sign of a fraud/scam when your username/password is requested. Same with sending in an email – a reputable individual will never ask. When a program or person helps you reset a password, they will never ask for your original one. They will always give you a new generic one and then recommend that you change it.

Public computers

* Follow all above password policies when working on public computers (closing SAM, thawing Deep Freeze, logging into Staff account, etc.).
* Do not let anyone see the key combinations or written procedures for accessing secure parts of computer (closing SAM, opening Deep Freeze login, logging off accounts, etc.).
* Though rebooting the computer will allow Deep Freeze to totally wipe the computer clean, it may also cause issues with Sam managing the timing of the computers for any patrons in the queue, in addition to the delay of waiting for the PC to restart. At the least, encourage patrons to delete any saved files/data and empty the Recycle Bin to avoid leaving behind any personal data/information. Though SAM will close any open programs and delete your Internet Explorer browsing history, it does not delete files or remove every trace of your work.
* Library-owned public laptops (and other mobile devices) run a much greater risk of theft. It is each individual library’s responsibility to create and enforce policies that lessen the chances of these devices being stolen or damaged (age limit, account in good standing, holding a patron’s ID, limiting where they can use device, etc.). If interested, contact John for assistance purchasing cable locks or theft-deterrent software (i.e. LoJack).

Staff computers

* Never let patrons use a staff computer. It is especially vital that Sierra access is prevented to protect patron records.
* Lock computer when you leave your desk (*Start->Lock* or keyboard shortcut: *Windows key+L*).
* Use a screen saver. Set it to a short duration and require login password upon resuming.
* Try to configure the layout/placement of staff computers so that there is some kind of barrier between them and the public/patron space.
* Try to maintain a staff presence near staff computers.
* Keep Windows, Java, and Adobe products updated. Setting these programs to update automatically may still require input from the user so maintain an active role in the process. Remember to uncheck any boxes touting additional software (like Ask Toolbar, McAfee Security Scan, Yahoo Toolbar, etc.).
* Staff-designated laptops are not configured for public use so never let patrons use them. Besides the usual risks associated with patrons using any library computer, the staff laptops are setup to connect to a specially designed staff wireless network which may provide access to other staff resources on the network.
* Email
  + Set email to require password (John can help configure this).
  + The more people that share the same staff computer/email, the more chance of people looking at each other’s emails. When possible, limit/reduce the number of users and/or email accounts on each computer.
  + Roundcube webmail, though less user-friendly, offers much higher security since a password is mandatory before having any account access at all.
  + Ultimately, no email program is totally secure so try not to send valuable/sensitive information in an email. Additionally, the Open Records law potentially allows anyone the right to read your emails, so take that into consideration when you write.

Miscellaneous

* **USB storage devices**: Thumb/flash drives, along with external/portable hard drives, carry with them the possibility of a virus. This is less of a concern with the public computers as it is the staff ones, which have no Deep Freeze. Scanning the drive (preferably on a public computer) before accessing any files is recommended. Upon inserting the USB cable into the computer, ESET presents a yellowish window in the lower right corner of the desktop that has a link to “Scan now”.
* **Printers**: Do not allow patrons (or staff) to change settings on the actual printer; instead, make changes in the “Printer Properties” box on the computer itself during each individual print job.
* **Printer waste**: Paper and toner wasted by patrons who hide (or refuse to pay for) unwanted copies is a financial burden. Libraries can help limit this through these suggestions:
  + Educate patrons on proper printing techniques
  + Place printers near staff
  + Keep paper drawer empty and hand out paper to patrons as they pay
  + Invest in a printing software solution
* **Network jacks**: Any open/unused network jacks must be disabled (by John/Dave) so no one can walk up and plug into our network.
* **Network cables**: Never allow patrons to unplug a network cable from a library computer (or the wall) to use in their own device (i.e. laptop).
* **Network closet/equipment:** No one but John or Dave should touch the network equipment (switch, router, wireless access points, etc.) unless authorized by Dave/John. The ideal situation would be to have the equipment locked in a room only accessible by the library staff. Since that is not always an available option, at least have it in a staff area as secure as possible from the public.
* **Guest wireless access**: Though the Guest Network WiFi signal often travels outside the library building, we do not intentionally provide, and thus guarantee, that service. By default, the access points remain on and active 24/7. As long as this exterior access is not abused, we have no problem with the public using it around the clock. However, if it becomes problematic in any way the OWLSnet Network Administrator and/or the library director maintain the right to limit the hours of operation and/or block certain devices from being able to connect. Examples of previous issues resulting in corrective action:
  + Groups of kids starting gathering behind a library building at night to use WiFi which resulted in risky/unruly behavior
  + Nearby resident adopted the signal as their primary internet connection at home
* **Security**: Ultimately, security depends on effort, dedication, and vigilance. When an individual gets lazy and takes shortcuts security breaks down. To avoid jeopardizing patron records, as well our entire system of libraries, please be thorough and follow all of the above security policies at all times. Please feel free to call the NFLS IT Coordinator or OWLSnet Network Administrator with any questions.