



# Technically Speaking

## PINS and Needles:

### The Password Roadblock

#### Elected Officers

##### President

Xibe Solis

##### Vice President/President Elect

##### Elect

Nick Tanzi

##### Secretary

Lisa Bitran

##### Treasurer

Eileen DeSimone

##### Past President

James Matias

##### Board Members-at-Large

Debbie Antolini

Chris DeCristofaro

James Hansen

Dominic Iadicicco

Bob Johnson

Min Liu

Mary O'Grady

##### SCLS Liaison

Eileen Keller

##### Newsletter Editor

Paul Zukowski

*By Chris DeCristofaro*

It happens to all of us. You are about to begin a One on One, Tech30, or Book a Librarian session with a patron. No matter what the device, the inevitable question rears its ugly head: "Do you know your password?" And that is when everything grinds to a halt. The session becomes either temporarily or permanently derailed and degenerates into the unending quest to determine how to remember or recover a forgotten password.

Passwords are a reality in the web-centric world in which we live; they are necessary to protect our digitized way of life. It keeps the dark corners of the Internet from creeping into our personal life. According to The Center for Strategic and International Studies, a DC-based think tank, more than 40 million people in the United States had personal information stolen in 2013. Because the public relies heavily on electronics that are increasingly embedded into our daily lives, passwords and PINS are a necessary evil.

#### **Being Creative with Passwords**

One of the most common problem for patrons (from teens to senior citizens) is remembering passwords. Many devices store passwords so the user has a difficult time recalling it when they do need it. As minimum requirements for passwords increases, the password conundrum is exacerbated. Capital letters, symbols and numbers are just more things to remember. Because requirements are becoming very sophisticated, people tend to simplify their passwords, which may make their accounts vulnerable. Using a family member's name (sometimes in conjunction with an age or birthday), a hobby, favorite sports team, or any personal information is a big mistake. Patterns (abc123), password, forgot my password or other references to

*-continued on p. 2*



2015 Long Island Library  
Conference  
Thursday, May 7

*The Digital Services  
Conundrum*

Libraries are fighting an uphill battle to compete with services being streamed directly to the home. Join us as we discuss the tools that librarians need, and the staff that libraries will need, to provide meaningful and relevant digital services to our patrons.

Stephen Ingram will be outlining broad technology trends, such as the prevalence of mobile devices and the growth of cloud based services. He'll go over the threats and opportunities these technologies pose to the library.

Nick Tanzi will engage in a case study, showing how the Mastics-Moriches-Shirley Community Library developed their digital services model. As the founding member of the Digital Services Department, he'll go over how they handle staff and patron instruction, and the types of programs and services they offer.

"password" are also easy for hackers to discover. And it is recommended to never use the same password for different accounts. Avoiding these practices will lessen chances of hackers gaining access to personal information. When talking password protection with patrons, there are many tips that can be utilized to invent ingenious and complex passwords only that person will understand and remember. The length of the password, in combination with unique characters, will make it more difficult for hackers to gain entry. Now a requirement in many new passwords, capital letters, numbers and symbols are a great way to make passwords more complex. The website [howsecureismypassword.net](http://howsecureismypassword.net) can be useful to demonstrate to patrons, in a humorous way, how easy it could be to hack their passwords.

Using simple pieces of information linked together may solve the problem most people have with remembering passwords. The "three tiered password" approach can yield results that are complex, but easy for patrons to remember. Using a combination of three words and/or numbers that have no value to hackers (such as the name of your favorite teacher, the year of the first car you owned and the address of an old job) may be diverse enough to outsmart hackers. Using 3 pieces of information along with a unique character, can create a formula for an effective password that is easy to remember. Switching the order of those 3 pieces of information allows the patron to have different passwords without changing the content of the password. The patron may forget the order of the password, but recalling the password only requires switching the order of the information used. Another effective strategy for reorganizing the information is spelling words backwards or interlacing numbers in between letters (ie taking the word "buster" and the number 4475179 becomes b4u4s7t5e1r79).

A popular strategy is substituting letters with characters that resemble letters (ie "sad to look at the sun" transcribes to "5ad2l00k@7h3su^"). Although this may seem like a strong strategy, hacker algorithms can detect these types of passwords so advise patrons not to rely solely on this technique.

## Write Them Down!

In the event that remembering passwords becomes a burden, having the information recorded in paper form stored in a secure place is a smart backup. There are many creative ways of recording passwords, but never record passwords on an electronic device that accesses the Internet (it should be assumed that anything that can be hacked will get hacked). Create a list of websites with user names and passwords that is kept in a locked desk drawer. Even better- purchase a small pocket sized notebook, assign a single page to each website or account with usernames and passwords. In the event a password needs to be changed, there is sufficient space to make that change and keep a reference of what was used in the past. There are many places online that have easily printable password sheets with fields for the name of the account and password. This is helpful as long as the sheet is available when you need it.

## Password Generators and Managers

If a patron cannot create a unique password, a password generator (such as <http://strongpasswordgenerator.com>) can create a password of random characters. These generators can be handy so long as the patron can remember the random characters.

As an alternative to writing the user name and password on a sheet of paper or a small notebook, there are many password managers that will record the information for you online.

(<https://lastpass.com/>, <http://keepass.info/>, <https://support.mozilla.org/en-US/kb/password-manager-remember-delete-change-passwords>, <https://support.google.com/chrome/answer/95606?hl=en>). These sites are encrypted for the users' protection but may require a degree of technical knowledge in order to work properly. As in any online storage, be mindful in recommending these services because no site is immune from cyber attacks. Although the site may be encrypted, no system is fool proof.

Helping patrons not only gain access to their online accounts, but to also remember and retain their passwords, is a constant challenge. Giving them the control to make password retention simple will only help to enhance their online and technology experiences.



At the April 2015 TIF meeting, Stephen Ingram was presented with a plaque for his years of service on the CATS board. Congratulations Stephen!



Visit [scla.net/cats](http://scla.net/cats) for details.

Computer and Technical Services Division  
Suffolk County Library Association  
c/o SCLS  
627 N. Sunrise Highway  
Bellport, NY 11713  
E-mail: cats@scla.net

---

### Upcoming Events:

#### Technology Information Forum (TIF) Meetings:

5/14/15 TIF Meeting– 10 AM Quogue Library

6/4/15 TIF Meeting– 10 AM Northport– East Northport Library

If your library is interested in hosting a TIF meeting, let us know!

#### CATS Board Meetings:

10 AM @ SCLS

5/13/15

6/10/15

7/8/15

9/9/15

We depend on members like you...

Please join today and help us write the next chapter:

<http://tinyurl.com/catsmembers>

