CYBERSECURITY ALERT:

TIPS FOR STUDENTS DURING THE #STAYATHOME SEMESTER

ISSUED BY THE
TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE
OF THE
NEW YORK STATE BAR ASSOCIATION

March 31, 2020

Opinions expressed are those of the Committee preparing this Cybersecurity Alert and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Mark A. Berman
Ganfer Shore Leeds & Zauderer LLP

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

COMMITTEE MEMBERS

Seth Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

AUTHORS OF THIS ALERT

Nicole Cardascia
Aishwarya Minocha

CONTRIBUTORS

Gail L. Gottehrer
Ronald J. Hedges
Mary Kavaney

INTRODUCTION FROM THE CO-CHAIRS

The COVID-19 outbreak has disrupted all our lives, including the lives of law students. A significant number of students will spend most of the Spring 2020 semester attending online classes from home, rather than in-person classes on campus, and participating in virtual study groups rather than face to face study sessions. While most of these students are likely comfortable with technology, they may not be familiar with the Internet setups in their homes or with some of the technologies they need to use to complete their coursework and communicate with their teachers. Despite their digital skills, understandably, cybersecurity may not be top of mind for students at this time.

Given our focus on providing practical, understandable, and timely cybersecurity resources to our community, the Committee on Technology and the Legal Profession has put together this Alert, which is geared towards students. It is designed to provide students with tips to help them study online, securely, during this "#stayathome semester." Like the *Key Takeaways* report we issued in February, and the first Alert we issued in March, it is concise and easy to read.

As part of its commitment to diversity, inclusion, and mentoring, the Committee is happy to announce that this Alert was drafted by Nicole Cardascia and Aishwarya Minocha, the two student members of our Cybersecurity Subcommittee. The Committee thanks them for volunteering their time and perspectives about the information that might be helpful for students. In addition, the Committee thanks Mary Kavaney, Chief Legal and Administrative Officer of the Global Cyber Alliance (GCA) and a member of our Cybersecurity Subcommittee, for her assistance and for the materials from the GCA's Work From Home campaign, some of which are cited in the Alert. The GCA's Work From Home materials and its Cybersecurity Toolkit, are available at no charge on the GCA's website, at: https://workfromhome.globalcyberalliance.org/.

Maximizing Your WiFi Speed

- Keep your router updated
- Remove all unwanted devices that are linked on the WiFi
  - Through the WiFi provider's app on your mobile device
- Switch to a different WiFi Channel
  - Create multiple channels so that one channel is not loaded with devices
- Offload the applications that are not being used frequently
- Reboot often - it regenerates the WiFi connections and could provide increased speeds
- Limit devices and optimize settings

Multi-Factor Authentication

(https://workfromhome.globalcyberalliance.org/sign-in-securely/)

- Easy to implement
- Knowing who is on the network and accessing your information is crucial
- Important way to help is use of multi-factor authentication (a/k/a two-factor authentication, or 2FA).
- 2FA requires multiple credentials, making it much harder for an attacker to gain access to your accounts
- Examples:
- **Authy** (https://authy.com)
- **Duo Mobile** (https://duo.com)
- **Google Authenticator** (https://www.google.com/landing/2step/

Creating Strong Passwords

Good passwords have *at least* 8 characters, use combinations of letters, numbers, and symbols, and mean something only to the person using the password. Here are some tips:

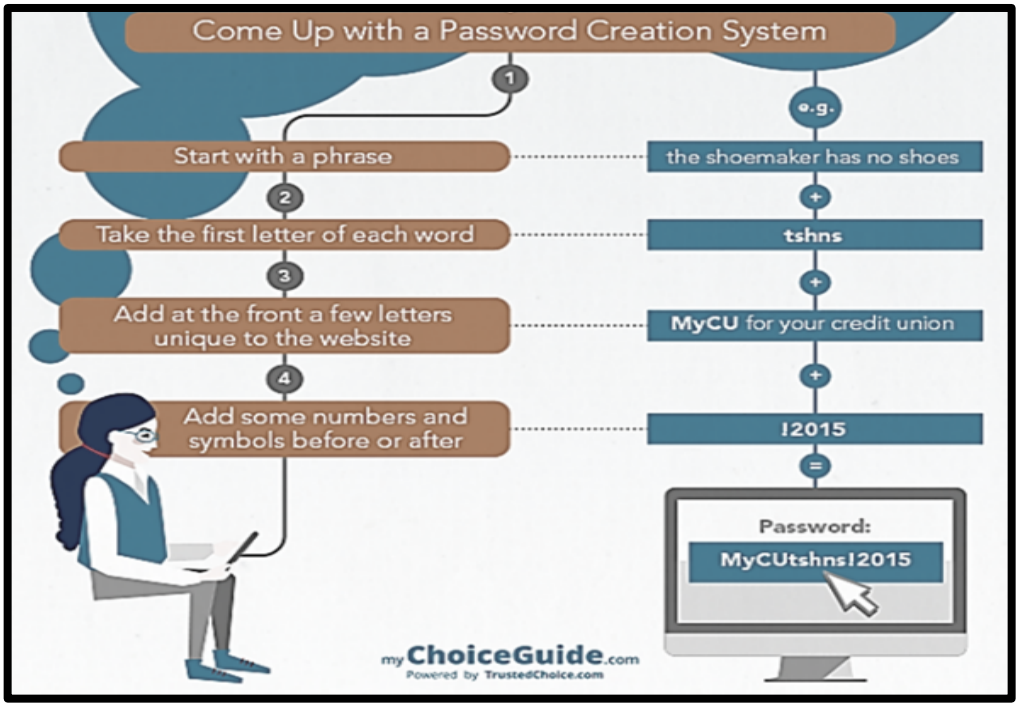
- Think of a nickname, favorite place, etc., etc., and then change a to &, s to $, o to 0, e to 8, L to 1, and random letter(s) to uppercase
- Example:

  Baruch College → B&ruchC0ll8ge → b$ruchC0ll8ge2
- Don't use the same password for all logins
- Change passwords periodically
- Keep passwords in a safe place

Email Encryption

for Office 365

- The new **Encrypt** button contains both S/MIME and IRM encryption options.
- **For detailed instructions** on adding encryption check Encrypting with S/MIME or Encrypt with Office 365 Message Encryption.



Securing Your Computer

- Make sure your computer has up-to-date antivirus software installed on it
- Be sure to install updates and patches promptly (once you verify they're from a legitimate source and not spam or malware that was sent to you or that popped up on your screen)
- CUNY schools offer free antivirus protection for students; ask them about free or discounted software that may be available

Storing Confidential Information and Sensitive Documents

- Store confidential documents separately to protect them from a virus and store them in a **Zip Folder**, an encrypted folder that prevents a virus from picking up any information inside it
- Avoid utilizing unapproved personal cloud service accounts for document storage if you're doing work for a law firm or other employer
- Back up important documents (your resume, job applications, transcripts, study outlines) on secure, password protected USBs

Public WiFi and Public Hotspots

- Public Hotspots are public WiFi services
- **Avoid** using public WiFi if you're working with sensitive or valuable information
- If you must use public WiFi, use a virtual private network (**VPN**)
- Ensure your protection software, operating system, and browsers are up to date and verify the name of the WiFi service you plan to use

Click Cautiously!!

- Phishing emails using COVID-19 information to lure people are increasingly common
- Keep an eye out for suspicious or unfamiliar emails (ones purporting to be from CDC or to provide news updates or maps showing the spread of COVID-19)
- Conduct your own research before opening or responding to a suspicious email (do an Internet search for correct CDC website address and access it directly, rather than through an email or link that was sent to you)

Securing Your Webcam with a Firewall

- A firewall is "a part of a computer system or network that is designed to block unauthorized access while permitting outward communication."
  - https://csrc.nist.gov/glossary/term/firewall

For Mac OS X v10.6 and Later:

- Choose **System Preferences** from the Apple menu
- Click **Security** or **Security & Privacy**
- Click the **Firewall** Tab
- Unlock the pane by **clicking the lock in the lower-left corner** and enter the administrator username and password
- Click **Turn On Firewall** or **Start** to enable the firewall
- Click Advanced to customize the firewall configuration

For PCs – Windows Defender Firewall:

- Select the **Start** button
- Select **Settings**, then **Update & Security**
- Select **Windows Security**, then **Firewall and Network Protection**
- Choose a Network Profile
- Under **Windows Defender Firewall**, switch the setting to **On**