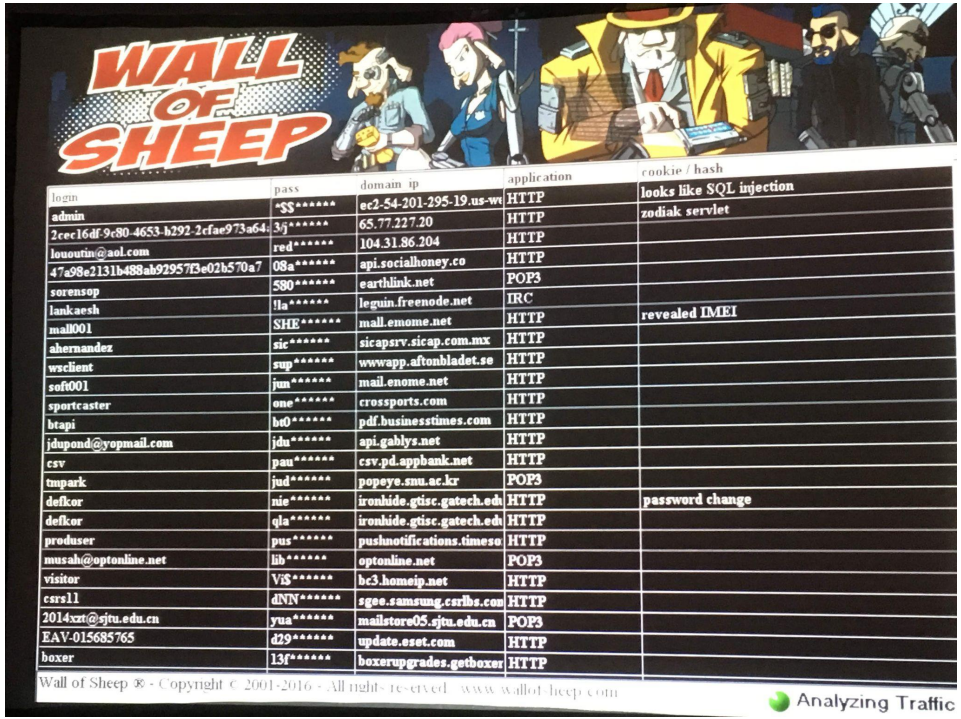
Cybersecurity for Nonprofits

Ming Chow
ming.chow@tufts.edu
October 7, 2025

About Me

- Teaching Professor at Tufts University
- Founder and Director of Tufts Cybersecurity Clinic
- Senior Member / Shepherd of the Wall of Sheep team



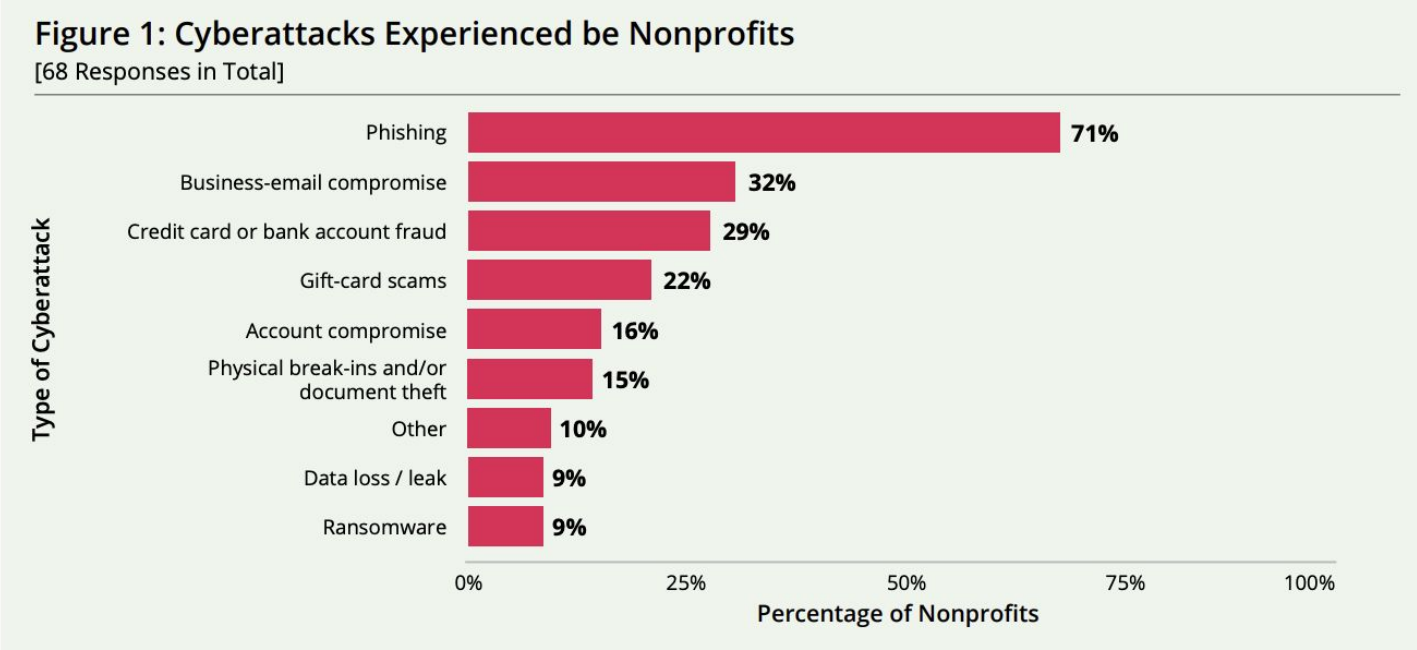
About the Tufts Cybersecurity Clinic

- Student teams work with underserved, under-resourced nonprofit organizations on cybersecurity matters
- *Pro bono*
- For students: real work experience
- For nonprofit organizations: receive cybersecurity services
- For Commonwealth of Massachusetts: workforce development
- For Tufts University: public good service

Why Nonprofit Organizations Need to Care About Cybersecurity?

- Cybersecurity is often the last thing organizations think about…
- …until an incident happens (i.e., reactive)...
- …and it's now a matter of *when* an incident happens, not *if*…
- …and then it gets very expensive
  - Bad publicity
  - Data breach => need to report to Commonwealth of Massachusetts, donors, clients, public
  - Potential loss of operations
  - Remediation and cleanup
  - 👋 $100K+ bill
- Doesn't matter how big or small organization is, there are no boundaries

Threats to Nonprofits



Source: Center for Long Term Security (CLTC) at University of California, Berkeley [1]

Constraints for Nonprofit Organizations

- Money
- Staffing and high turnover
- Knowledge
- Time / convenience
- (Outdated) infrastructure

Key Findings from CLTC [1]

Key findings include:

1. **Nonprofits are frequent targets of cybercrime,** with 85% of nonprofits surveyed reporting that they have experienced at least one cyber attack. **Nonprofits remain attractive for cyber criminals because they collect and store sensitive information;** 75% of surveyed nonprofits reported that they collect social security numbers.

2. **Nonprofits lack the staff they need to protect themselves against cyber attacks:** 53% of surveyed nonprofits have no full-time IT staff, and those that do have an average of just one full-time IT staff member for every 96 employees.

3. **Nonprofits have moderate adoption rates of basic cybersecurity controls.** While 61% of surveyed nonprofits employ multi-factor authentication (MFA) for email and collaboration tools, 16% do not use MFA at all, and 53% do not offer any type of cybersecurity awareness training for employees.

4. **Nonprofits struggle most with funding and prioritizing cybersecurity:** 46% of surveyed nonprofits ranked funding as their greatest obstacle to improving their organization's cybersecurity, followed closely by a lack of knowledge on what to improve and difficulty prioritizing cybersecurity over competing objectives.

5. **Nonprofits want hands-on, human assistance to improve their cybersecurity.** Nonprofits ranked a city help line and proactive cybersecurity consulting as the highest priority needs for improving their cybersecurity. These items ranked above other cybersecurity resources, such as tools and software, educational websites, and awareness training, emphasizing the necessity of human interaction in cybersecurity resilience.

Best Cybersecurity Investments to Make

- Password Manager
- Two-Factor Authentication, Multi-Factor Authentication
- Offline Backups
- Phishing Training
- Patching

Passwords

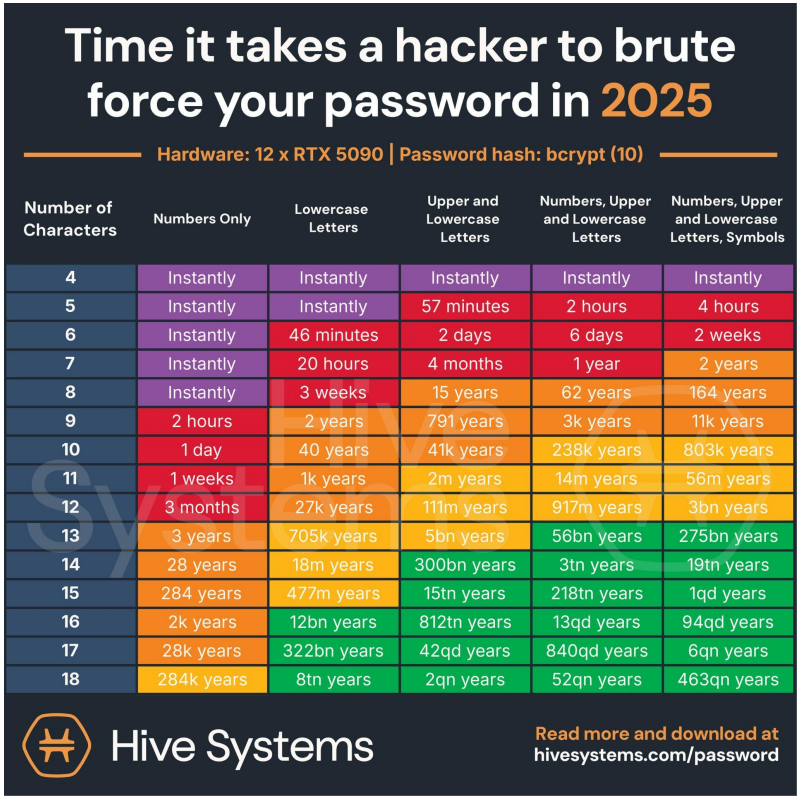
- Weak passwords still one, if not the most effective way, to breach systems and institutions
- Generally speaking, people and institutions have well over 50+ accounts
- All the weak passwords are now well known, cracked
    - Credential stuffing makes things even worse
- A strong password policy doesn't go far enough…
- How One Bad Password Ended a 158-Year-Old Business (September 2025)

```
1   123456
2   123456789
3   12345678
4   password
5   qwerty123
6   qwerty1
7   111111
8   12345
9   secret
10  123123
11  1234567890
12  1234567
13  000000
14  qwerty
15  abc123
16  password1
17  iloveyou
18  11111111
19  dragon
20  monkey
21  123123123
22  123321
23  qwertyuiop
24  00000000
25  Password
26  654321
```

Source: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/2023-200_most_used_passwords.txt

Two-Factor Authentication

- It is not a matter of *if* your password will be cracked, but *when*
- Two-Factor Authentication (2FA) is a type of Multi-Factor Authentication
- Enabling 2FA: even if your password is cracked, still needs additional proof to enter
- Many institutions now require 2FA



Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

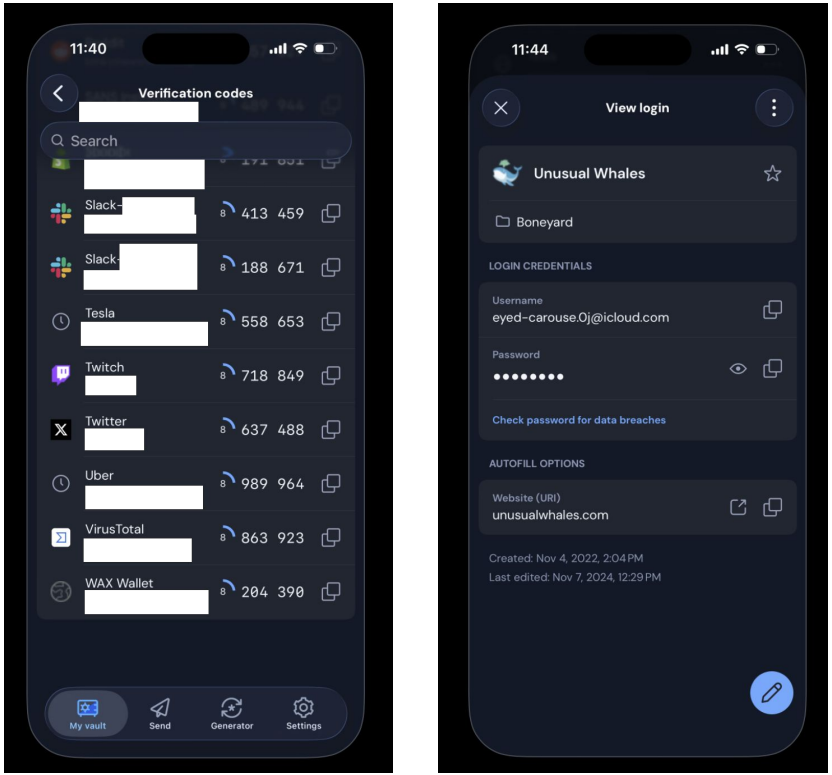
Read more and download at hivesystems.com/password

Password Managers

- Arguably the best investment you can make in cybersecurity
- Stores credentials, 2FA codes, IDs, payment cards
- You remember one master password
- Randomize passwords for all accounts

Choosing a Password Manager

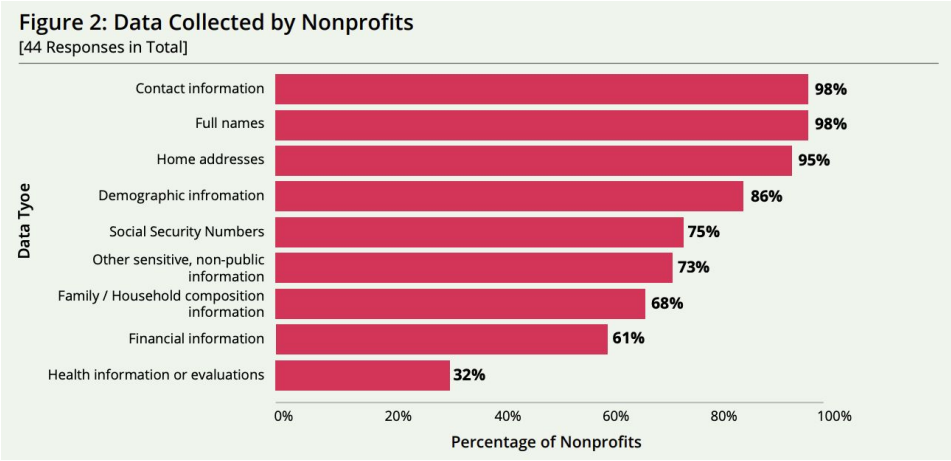
- An official password manager is now installed on Apple and Google ecosystems (iOS and Android)
- Bitwarden and 1Password have a small fee –both ideal options
  - https://1password.com/for-non-profits/
  - https://bitwarden.com/help/getting-started-organizations/
- Best to use password manager app and not storing passwords on web browser for portability
- Can detect whether account was in a data breach



Screenshots of Bitwarden

Backups

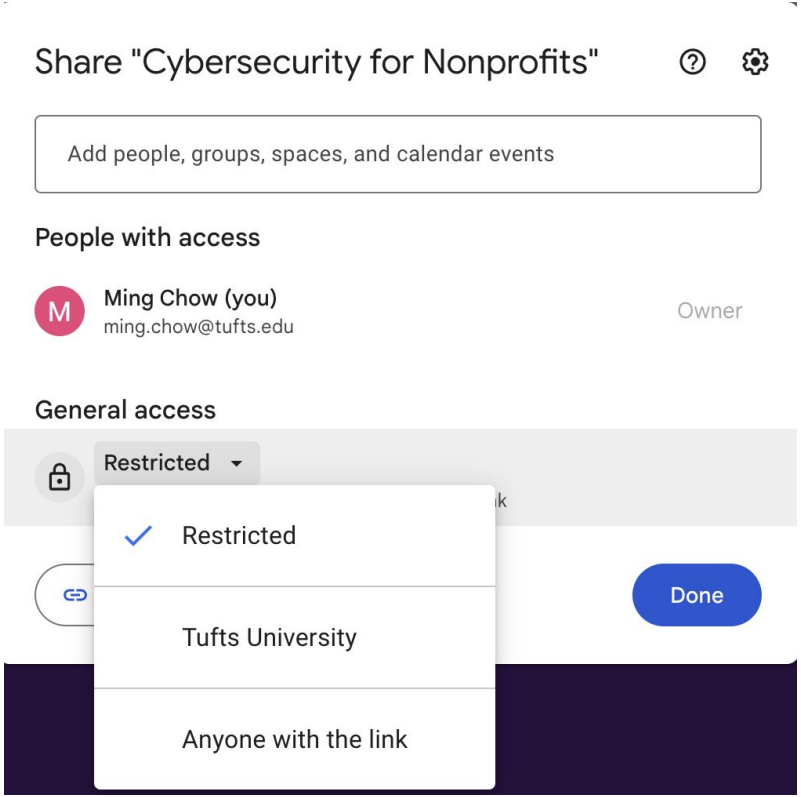
- Putting everything in Google Drive, Dropbox, Box, etc. isn't truly backup –single point of failure
- *Less is more*, easier to manage
- Move archival data to offline backup (e.g., external hard drive)
- [Fire destroys S. Korean government's cloud storage system, no backups available (October 1, 2025)]



Source: Center for Long Term Security (CLTC) at University of California, Berkeley [1]

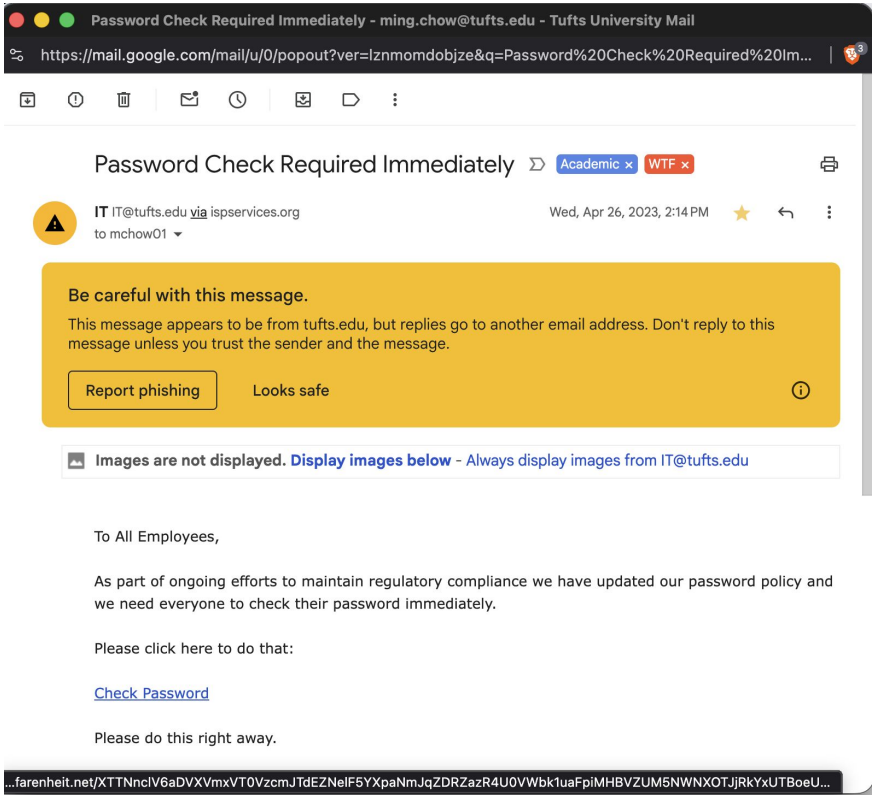
Access Control

- Who has access to what?
- Not everyone needs access to everything
- What is your policy for data access internally, externally?



Phishing

- Still very effective for targeting people, institutions
- Training employees and volunteers is ideal
- Spotting phishing emails:
  - Check the sender's email address
  - Different people and addresses
  - Watch for urgent or threatening language – "Your account will be locked!" or "Click now!"
  - Hover over links – does the URL match where it says it's going?
  - Look for typos or weird formatting
  - Unexpected attachments or links
  - Signature doesn't look trustworthy
  - Sender doesn't exist at institution



More Phishing

---------- Forwarded message ---------
From: **Alexandra Deemys Kidd** <mrsvdw03@optonline.net>
Date: Mon, Apr 7, 2025 at 11:44 AM
Subject: [External] Claiming Gift Response is Needed
To:

Dear Staff and Faculty,

We are pleased to share that our school has recently upgraded its welding tools and equipment. As a result, we have several high-quality tools in excellent working condition that are now available to find a new home. Rather than letting these items go unused, we would like to offer them to anyone who may find them beneficial.

Available Items Include:

*Miller Dynasty 300 TIG Welder
*MIG Welder
*Stick Welder
*Welding Helmet
*Chipping Hammer & Wire Brush
*Regulators & Flowmeters
*Snap-On Mechanics Tool Set – Complete set of wrenches, sockets, and accessories

If you are interested or know someone who might benefit from these tools, please reach out to Mrs. Tracy Abrahamson for more details and to arrange delivery .

For inquiries, please contact Mrs. Tracy Abrahamson at tabrahat@outlook.com

Thank you for your continued support.

Best regards,

Alexandra Deemys Kidd
Human Resources Compensation Program Manager

Tufts University

---------- Forwarded message ---------
From: **Tufts University Server** <noreply@mailserver-outlook.com>
Date: Tue, Mar 11, 2025 at 11:49 AM
Subject: [External] Maintenance Notification
To: <jfoste07@tufts.edu>

Outlook Expiry Notice

Hi Jeffrey,

Your password for jfoste07@tufts.edu is set to expire on March 14, 2025.

You can keep your current password with the button below.

Keep My Password

Was this helpful?
Organization: Tufts University
Acct Summary: jfoste07@tufts.edu

Patching

- Software (e.g., operating systems, apps) is riddled with vulnerabilities…
- …vulnerabilities that can be exploited by attackers…
- Ransomware weaponize publicly known vulnerabilities. This also include weak passwords.
- “40 percent of the vulnerabilities exploited in 2024 were at least four years old, with some dating back to the 1990s”
- Patching systems is a necessity to defend against ransomware, attacks

Action Items

1. Migrate to use a password manager
2. Enable 2FA on accounts, store 2FA codes in your password manager
3. Install latest security updates on your system
    a. No need to go one full version up (e.g., Windows 10 to Windows 11)
4. Backup critical files to an external hard drive; move older files off of cloud drive to external hard drive

What About Cyber Insurance?

- Ideal if your organization is storing lots of personal and confidential information
- Can involve lots of work, and don’t lie!
- What cyber insurance is NOT:
  - An excuse to not care about cybersecurity
  - One size fits all
  - Covers everything
- What cyber insurance can cover:
  - Incident handling and response
  - Forensics
  - Legal counsel
  - Public relations
  - Data recovery

What About Testing Tools?

- Many organizations use WordPress for website…
- …and WordPress plugins are notorious for vulnerabilities…
- …routine audits using tools like `wpscan` can reveal weaknesses on website

Final Thoughts

- *Build good habits and good hygiene*
- *Be accountable for yourself, your institution, and stakeholders*
- None of this is new…
- …but yet we have been battling the same problems for decades to no end
- For organizations and individuals, it's overwhelming…
- …and becomes more overwhelming over time
- Hence, why we decided to do a Cybersecurity Clinic at Tufts. For more details or expressing interest in participation, send email to cyberclinic@tufts.edu

Thanks. Questions?

Acknowledgements

Special thanks to Sarah Powazek, the Consortium of Cybersecurity Clinics, and the Center for Long Term Cybersecurity (CLTC) for their works, and most importantly, leadership working with non-profit organizations, governments, and small businesses.

Usable References

1. https://cltc.berkeley.edu/wp-content/uploads/2024/11/CyberCAN_Cybersecurity-for-Cities-and-Nonprofits.pdf
2. https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf
3. https://www.reddit.com/r/sysadmin/comments/ln8u6g/affordable_or_free_password_manager_for_nonprofits/