Hacklore in City Government Guidance

How the largest cities' public security advice compares with hacklore.org · November 23, 2026

Summary

Hacklore is security advice that sounds sensible but no longer protects people. The word, a blend of hacking and folklore, comes from hacklore.org (https://hacklore.org). In November 2025, a group of current and former chief information security officers and other security leaders published an open letter there (https://hacklore.org/letter) asking the public, employers, journalists and policymakers to retire six pieces of advice: avoid public Wi-Fi, never scan QR codes, avoid public USB charging, turn off Bluetooth and NFC, clear cookies regularly, and change passwords on a schedule. The site's FAQ (https://hacklore.org/faq) adds password complexity rules. Advice like this uses up the limited time people have for security and crowds out the steps that work: keeping devices updated, turning on multi-factor authentication, and using long, unique passwords stored in a password manager.

We reviewed the official websites of the three largest US cities, New York City, Los Angeles and Chicago, for public guidance that still gives retired advice. This report is a companion to our report on state government guidance (https://hacklore.org/states). We count clear hacklore: advice to the public or small businesses that repeats a retired practice. That includes hedged versions (“limit what you do on public Wi-Fi”) and narrower ones (“only make transactions on HTTPS sites” when on public Wi-Fi), because they still carry the core myth. Advice written for city staff, and advice that matches hacklore.org's own guidance, is listed in the appendix but not counted.

3	22	6
cities with clear hacklore	city pages with clear hacklore	more pages listed but not counted

- **New York City and Los Angeles each repeat three retired practices; New York has the most pages.** Fifteen New York pages from seven city bodies and a council member's office give clear hacklore: consumer protection, emergency management, the public schools, NYC Cyber Command, the housing authority, the housing department and the employees' retirement system.
- **New York's own security app warns people off public Wi-Fi.** NYC Cyber Command's free NYC Secure app alerts people to unsecured Wi-Fi networks and tells them to disconnect.
- **New York's public schools teach it to children and parents.** The schools' security page, poster and guide for parents give complexity rules, and two of them say to limit what you do on public Wi-Fi.
- **Los Angeles sends mixed messages.** A 2015 police release and a 2015 pension system page are still live. The Emergency Management Department repeated CISA's complexity rule in 2024 and 2025, then dropped it in October 2026. The city's own sign-in for residents gives the basics.
- **Chicago's city departments say almost nothing, good or bad.** The one clear case is a 2019 library blog post. The city's technology office publishes no security advice for the public.

Our ask of city agencies. Fix the sentences quoted in the appendix, replace them with the basics, and tell us when you have. The full list is under “What we ask of city agencies.”

City scorecard

Each row is a city where we found clear hacklore. Each column is one of three retired practices. The Practices column counts how many of them a city repeats as clear hacklore, and the cities with the most are at the top. Every quote behind a mark is in the appendix, under the city's name.

- ● Clear hacklore: at least one city page tells the public to follow this advice.
- ○ Listed but not counted: milder hacklore, or advice written for city staff.
- No mark: we found none.

City	Practices	Complexity	Public Wi-Fi	Password changes
Los Angeles	3	●	●	●
New York City	3	●	●	●
Chicago	1		○	●

Why this advice is retired

Advice	Cities	Why it doesn't help	What to say instead
Change passwords regularly	3	There is no evidence that scheduled changes reduce crime. They lead people to pick weaker passwords and reuse them.	Change a password when there is reason to think it was exposed. Turn on multi-factor authentication.
Password complexity rules	2	Length matters more than symbols. NIST, the federal standards agency, dropped composition rules in 2017. Long passwords and passphrases are harder to crack than short ones full of symbols.	Use a long (16+ characters), unique, randomly generated password or passphrase, stored in a password manager.
Avoid public Wi-Fi / use a VPN	2	Almost every website and app now encrypts its traffic, even on open networks. Large-scale attacks through public Wi-Fi are exceedingly rare. Personal VPNs add little for most people.	Public Wi-Fi is fine for everyday use. Keep devices and apps updated.

Sources: the hacklore.org letter (https://hacklore.org/letter) and FAQ (https://hacklore.org/faq). No city page we found tells the public never to scan QR codes, to turn off Bluetooth or to clear cookies. New York City's NYC Secure app site calls public charging stations a theoretical risk while advising only a change to a developer setting; it is listed in the appendix as milder hacklore.

What we ask of city agencies

We ask every agency named in the appendix to take these steps. We recheck every page and record each fix, so we can report which cities have acted.

1. **Fix the quoted sentences.** Find your agency's quotes in the appendix. Each one links straight to the sentence on your page.
2. **Replace them with the basics.** Keep devices and apps updated, turn on multi-factor authentication, use long, unique passwords or passphrases, and use a password manager. In practice: recommend length instead of complexity rules, drop warnings about public Wi-Fi, and say to change a password only when there is reason to think it was exposed.
3. **Start with what reaches the most people.** In New York, that is the NYC Secure app, the public schools' material for students and parents, and the consumer protection tip sheets.
4. **Update seasonal material before it goes out again.** Cybersecurity Awareness Month newsletters and holiday shopping tips are where the old tip lists come back each year.
5. **Check templates before reusing them.** The Los Angeles complexity rule came from CISA's Cybersecurity Awareness Month text.

6. **Retire old pages that nobody maintains.** Pages from 2015 to 2019 are still online in all three cities.
7. **Review guidance for city staff too.** We did not count it, but much of it repeats the same advice.
8. **Tell us when you have made a change.** Message us on Bluesky at https://bsky.app/profile/hacklore.bsky.social so the next check can credit the fix.

Most notable examples

Selected for how much authority the source carries and how many retired practices it repeats.

New York City: NYC Cyber Command, NYC Secure app

The city's free security app “Alerts you to potentially unsecure Wi-Fi networks” and recommends that you “disconnect and switch to a secure network.”

https://secure.nyc/

New York City: Public Schools

Tells students to “Mix it up with letters, numbers, and symbols” and to “Limit what you do on public Wi-Fi.” A guide for parents repeats the complexity rule.

https://www.schools.nyc.gov/school-life/school-environment/digital-citizenship/cybersecurity-awareness-month

New York City: Department of Consumer and Worker Protection

Its identity theft and holiday shopping tips say “Avoid typing your personal information when using unsecured Wi-Fi.” An older scam guide says to use letters, numbers and symbols and to “change it frequently.”

https://www.nyc.gov/site/dca/consumers/identity-theft-prevention-tips.page

New York City: Emergency Management, Ready NY

Tells the public to “Use a Virtual Private Network (VPN)” and to change home router and Wi-Fi passwords “regularly.”

https://www.nyc.gov/site/em/ready/cybersecurity.page

Los Angeles: Police Department, 2015

“Do not enter passwords while on an open Wi-Fi.” Also recommends upper and lower case letters, numbers and special characters.

https://www.lapdonline.org/newsroom/lapd-issues-cyber-attack-prevention-information-after-anthem-cyber-hacking-nr15041jr/

Los Angeles: Emergency Management Department

Its October 2024 and 2025 newsletters repeat CISA's rule that strong passwords “include all four character types.” The October 2026 issue dropped it.

https://emergency.lacity.gov/sites/g/files/wph1791/files/2024-09/EMD_10.2024%20Newsletter.Final_.pdf

Bright spots

- Los Angeles promotes free public Wi-Fi without a warning. The mayor's office announced free community Wi-Fi in South Los Angeles in May 2026 (https://mayor.lacity.gov/news/mayor-bass-promotes-free-public-wi-fi-access-south-la), and the city's Get Connected LA site lists free Wi-Fi locations (https://getconnected.lacity.gov/digital-resources/wifi).
- Los Angeles' sign-in for residents, the Angeleno Account, asks for 12 or more characters, suggests several words with spaces and a password manager, and sets no complexity rule (https://account.lacity.gov/help/change-your-password).
- No city page we found tells the public never to scan QR codes. New York's Department of Transportation warns about stickers placed over the codes on parking meters, which matches hacklore.org's own guidance.

Method and caveats

- We searched the official websites of the three largest US cities by population in November 2026: New York City, Los Angeles and Chicago, per the Census Bureau's estimates for July 1, 2025 (https://www.census.gov/newsroom/press-releases/2026/vintage-2025-city-town-pop-estimates.html). We covered the same kinds of agencies as our state report (technology and cyber offices, consumer protection, police, emergency management and mayors' offices), plus fire departments, aging and small business offices, comptrollers, councils, public schools and city-run libraries.
- City government here includes city departments, New York's housing authority (NYCHA) and the city pension systems (NYCERS in New York and Fire and Police Pensions in Los Angeles), whose tips are written for members' personal accounts. County, state and nonprofit pages were excluded. So were national courses that the Chicago Public Library hosts on its DigitalLearn site: they repeat public Wi-Fi and complexity advice, but the Public Library Association and its partners wrote them.
- Each quote has one of three tiers. Clear hacklore: advice to the public or small businesses that repeats a retired practice, including hedged versions (“limit,” “avoid,” “try not to”), narrower ones (only for shopping, banking or home routers), warnings that point people toward the practice, complexity rules even alongside a long minimum length, and prompts to change passwords for no reason. Milder hacklore: spoken remarks in podcast transcripts, a page that describes advice without giving it, or a risk raised only to recommend an unrelated setting. Not counted: advice that matches the hacklore.org FAQ, advice written for city staff, and terms of use for an agency's own network. Only clear hacklore is counted.
- The scorecard counts how many retired practices a city repeats, not how many pages repeat them. A city that publishes more isn't marked down for volume.
- Every quote in the appendix was checked on November 23, 2026 on the live page, by script or, for pages that build their text in the browser or are scanned images, by reading the page in a browser.
- Quotes that come down after our first check on November 23, 2026 stay in the appendix, marked removed with the date of the check that found them gone, so the agency gets credit. They are not counted.
- The search was not exhaustive, so “none found” means we didn't find any, not that none exist.

About this report

Prepared by Robert Lord for hacklore.org (https://hacklore.org).

If you think we quoted something unfairly or out of context, tell us on Bluesky at https://bsky.app/profile/hacklore.bsky.social.

Appendix: Quotes and quote links

36

quotes on live pages

35 quotes from 28 links in 3 cities, checked on November 23, 2026. This appendix lists the exact sentences that repeat retired advice, so each agency can find and change them. Every quote has its own link. On a web page, the link scrolls to the quote and highlights it in Chrome, Edge, Safari and Firefox. Links to PDF files open at the page that holds the quote; search that page for the quoted words. Some pages hide text in collapsed sections; the note says which section to open.

Quotes are copied exactly, including the page's own spelling and punctuation. Each starts with the advice it repeats. Quotes marked Removed came down after our first check; they stay listed so the agency gets credit. Quotes that are not clear hacklore carry a label and the reason. The three labels mean:

- **Clear hacklore:** Advice to the public or small businesses that repeats a retired practice, including hedged or narrower versions, complexity rules even alongside a long minimum length, and prompts to change every password for no reason. Only clear hacklore is counted.
- **Milder hacklore:** Weaker versions: spoken remarks in a podcast transcript, a page that describes advice without giving it, or a risk raised only to recommend an unrelated setting. Listed but not counted.
- **Not counted:** Advice written for city staff, advice that matches the hacklore.org FAQ, or terms of use for an agency's own network. Listed but not counted.

Chicago

Chicago Public Library (CPL) blog, Cybersecurity Month: Books and Websites to Protect Yourself Online, 2019-10-16
https://www.chipublib.org/blogs/post/resources-for-cyber-security-month/

Password changes: “October is National Cybersecurity Awareness Month, so use this as an excuse to make some really quick moves, like updating your passwords or privacy settings.” Open at quote

CPL, WiFi Use Policy
https://www.chipublib.org/wifi-use-policy/

Public Wi-Fi: “Information sent to or from your device can be captured by anyone else with a wireless device and appropriate software.” Open at quote Not counted. Terms of use for the library's own network, not a safety tip.

Los Angeles

Police Department (LAPD), Cyber-Attack Prevention Information After Anthem Cyber Hacking, 2015-02-05
https://www.lapdonline.org/newsroom/lapd-issues-cyber-attack-prevention-information-after-anthem-cyber-hacking-nr15041jr/

Complexity: “Think of phrases using spaces, upper and lower case letters, numbers, acronyms, and special characters.” Open at quote

Public Wi-Fi: “Do not access critical data on public or open Wi-Fi networks. Do not enter passwords while on an open Wi-Fi. Only use public Wi-Fi networks which request a passcode to enter, even if everyone knows that code.” Open at quote

Emergency Management Department (EMD), newsletter, October 2024 (PDF)
https://emergency.lacity.gov/sites/g/files/wph1791/files/2024-09/EMD_10.2024%20Newsletter.Final_.pdf

Complexity: “Strong passwords are long, random, unique and include all four character types (uppercase, lowercase, numbers and symbols).” (page 1) Open at quote Tip credited to CISA.

EMD, newsletter, October 2025 (PDF)
https://emergency.lacity.gov/sites/g/files/wph1791/files/2025-09/EMD-October-2025-Newsletter.pdf

Complexity: “Strong passwords are long, random, unique and include: uppercase letters, lowercase letters, numbers, and symbols.” (page 1) Open at quote Tip credited to CISA.

EMD, newsletter, December 2023 (PDF)
https://emergency.lacity.gov/sites/g/files/wph1791/files/2023-11/December%202023%20EMD%20Newsletter.pdf

Public Wi-Fi: “Use your home or a trusted Wi-Fi source and make sure you are making purchases through trusted vendors.” (page 2) Open at quote Holiday shopping tip credited to CISA. The PDF is a scanned image, so searching it will not find the words.

LAPD, Read More Community Information
https://www.lapdonline.org/read-more-community-information/

Complexity: “Place a special security feature (password) on all your accounts. Make it something involving numbers, letters and symbols.” Open at quote Advice for identity theft victims.

Los Angeles Fire and Police Pensions (LAFPP), Protect Your Online Identity, 2015-12-02
https://lafpp.lacity.gov/protect-your-online-identity

Complexity: “Try to utilize upper and lower case letters, as well as symbols to keep identity thieves and scammers from figuring out your passwords.” Open at quote

Password changes: “Create strong passwords – and update them frequently!” Open at quote

New York City

Department of Consumer and Worker Protection (DCWP), Identity Theft Prevention Tips
https://www.nyc.gov/site/dca/consumers/identity-theft-prevention-tips.page

Public Wi-Fi: “Avoid typing your personal information when using unsecured Wi-Fi; create strong, personal passwords; and only download software and apps from trusted sources.” Open at quote

DCWP, Protect Your Identity tip sheet (PDF)
https://www.nyc.gov/assets/dca/downloads/pdf/consumers/protect-your-identity-tips-english.pdf

Public Wi-Fi: “Avoid typing your personal information when using unsecured Wi-Fi” (page 1) Open at quote

DCWP, Holiday Shopping Tips
https://www.nyc.gov/site/dca/consumers/holiday-shopping-tips.page

Public Wi-Fi: “Avoid typing your personal information when using unsecured Wi-Fi.” Open at quote

DCWP, Holiday Shopping Tips (PDF)
https://www.nyc.gov/assets/dca/downloads/pdf/consumers/DCWP-Holiday-Shopping-Tips-English.pdf

Public Wi-Fi: “Avoid typing your personal information when using unsecured Wi-Fi.” (page 2) Open at quote

DCWP, Internet Scam Guide (PDF)
https://www.nyc.gov/assets/dca/downloads/pdf/consumers/Consumers-Internet-Scam-Guide.pdf

Complexity, Password changes: “Use a combination of letters, numbers, and symbols for your password, change it frequently, and do not share it with anyone.” (page 3) Open at quote The guide still refers to dial-up access.

NYC Emergency Management (NYCEM), Ready NY, Plan for Hazards: Cybersecurity
https://www.nyc.gov/site/em/ready/cybersecurity.page

Public Wi-Fi: “Use a Virtual Private Network (VPN) that creates a secure connection.” Open at quote

Password changes: “Protect your home network by changing the administrative and Wi-Fi passwords regularly.” Open at quote

NYC Public Schools, Cybersecurity Awareness page
https://www.schools.nyc.gov/school-life/school-environment/digital-citizenship/cybersecurity-awareness-month

Complexity: “Mix it up with letters, numbers, and symbols.” Open at quote

Public Wi-Fi: “Limit what you do on public Wi-Fi and especially avoid logging in to key accounts like email and bank accounts.” Open at quote

NYC Public Schools, Cybersecurity Awareness Month poster (PDF), 2023
https://pwsblobprd.schools.nyc/prd-pws/docs/default-source/default-document-library/cybersecurity-awareness-poster.pdf?sfvrsn=b444c76b_4

Complexity: “Use letters, numbers, and symbols.” (page 1) Open at quote

Public Wi-Fi: “Public networks are unsecured.” (page 1) Open at quote

NYC Public Schools, Keeping Your Child Safe Online, guide for parents (PDF), 2026
https://pwsblobprd.schools.nyc/prd-pws/docs/default-source/default-document-library/38979-digital-age-parents-guide.pdf?sfvrsn=768faeef_2

Complexity: “Show your child how to make strong passwords using a mix of letters, numbers, and symbols.” (page 1) Open at quote

City Council Member Gale Brewer, Guide to Preventing Scams (PDF), 2025
https://council.nyc.gov/gale-brewer/wp-content/uploads/sites/90/2025/06/ScamsLetterSizeFInal-interactive.pdf

Password changes: “Change passwords and PINs often” (page 2) Open at quote

NYC Cyber Command, NYC Secure app site
https://secure.nyc/

Public Wi-Fi: “When an unsecured Wi-Fi network threat is detected, it is recommended that you disconnect and switch to a secure network with encryption capabilities that will prompt you for a password.” Open at quote The city's free app alerts people to unsecured Wi-Fi.

USB charging: “The device is put at risk when, for example, you need to plug your phone into an unfamiliar USB port—like a public charging station.” Open at quote Milder hacklore. Calls the charging station risk theoretical and advises only turning off USB debugging, a developer setting.

NYC Housing Authority (NYCHA) Journal, October Is Cybersecurity Awareness Month, 2023-10-11
https://nychajournal.nyc/october-is-cybersecurity-awareness-month-2/

Public Wi-Fi: “Don’t share personal info on public wi-fi.” Open at quote

New York City Employees' Retirement System (NYCERS), 7 Tips to Shop Online Safely this Holiday Season, 2025-11-24
https://www.nycers.org/member-resources/updates-alerts/7-tips-to-shop-online-safely-this-holiday-season

Public Wi-Fi: “When using public Wi-Fi, only make transactions on HTTPS sites.” Open at quote Under the heading “Use secure Wi-Fi for online transactions.”

Public Wi-Fi: “If it’s easy for you to join, it’s easy for cybercriminals to do so too!” Open at quote

NYCERS, Protect Yourself from Fraud
https://www.nycers.org/supplemental-post/protect-yourself-from-fraud

Complexity: “Create strong passwords by using a combination of letters, numbers, and special characters.” Open at quote

NYCEM, Prep Talk podcast, episode 39 transcript (PDF), 2019
https://www.nyc.gov/assets/em/downloads/pdf/podcast_transcripts/prep_talk_39_cybersecurity.pdf

Complexity: “Just make sure you have your special characters injected someplace in there.” (page 6) Open at quote Milder hacklore. Spoken remarks in a podcast transcript. The episode also recommends passphrases, password managers and multi-factor authentication.

NYCEM, Prep Talk podcast, episode 57 transcript (PDF), 2020-10-22
https://www.nyc.gov/assets/em/downloads/pdf/podcast_transcripts/prep_talk_57_cybersecurity_awareness_month.pdf

Complexity: “Should be a mix of letters, upper and lower case, numbers and symbols, and no ties to your personal information and no dictionary words.” (page 2) Open at quote Milder hacklore. Spoken remarks in a podcast transcript, right after “The longer, the better.”

NYCEM, release for the ¡Prepárate! podcast, 2021-10-14
https://www.nyc.gov/site/em/about/press-releases/20211014_pr_nycem_spanish-podcast-highlights-importance-of-cybersecurity.page

Public Wi-Fi: “why free Wi-Fi access is not always a good idea” Open at quote Milder hacklore. Describes a podcast episode rather than giving the advice directly.

Department of Housing Preservation and Development (HPD), NYC ID guide for the owner portal (PDF), 2019
https://a806-asap.nyc.gov/HPDPortal/files/NYC_ID_DTR_Owner_Portal.pdf

Password changes: “Do this from time to time to minimize the possibility of unauthorized logins.” (page 14) Open at quote On changing the account password.

Office of Technology and Innovation (OTI), Citywide Cybersecurity User Responsibility Policy (PDF)
https://www.nyc.gov/assets/newhire/downloads/Citywide-Cybersecurity-User-Responsibility-Policy_OTI.1.13.2026.P-02-PR-AT-Non-Restricted92.pdf

Public Wi-Fi: “Users are strongly encouraged to not connect to insecure network. (e.g., public Wi-Fi).” (page 7) Open at quote Not counted. Policy for city staff.

Office of Payroll Administration, Employee Self-Service FAQ (PDF), 2024
https://www.nyc.gov/assets/opa/downloads/pdf/ess-faq-2024.pdf

Password changes: “You should create passwords that cannot be linked to you and change your password regularly.” (page 2) Open at quote Not counted. For city employees using the payroll system.