Hacklore in State Government Guidance

How state agencies' public security advice compares with hacklore.org · November 14, 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 official state government websites in all 50 states for public guidance that still gives retired advice. We count clear hacklore: advice to the public or small businesses that repeats a retired practice. That includes hedged versions (“consider a VPN”) and narrower ones (“don't bank on public Wi-Fi”), because they still carry the core myth. Advice written for state staff, and advice that matches hacklore.org's own guidance, is listed in the appendix but not counted.

46	2	2
states with clear hacklore	states with only milder hacklore or guidance for state staff	states where we found none

- **Some states repeat far more retired advice than others.** New York repeats all six practices we track; New Jersey and South Carolina repeat five; Alabama, Delaware, Michigan, North Carolina, Ohio, Oklahoma and Virginia repeat four. 27 of the 46 states with clear hacklore repeat one or two. The scorecard ranks every state.
- **Password advice and public Wi-Fi warnings lead.** Complexity rules (33 states), public Wi-Fi and VPN warnings (30) and routine password changes (28) far outnumber warnings about USB charging (9) and Bluetooth (10).
- **Attorneys general and consumer protection offices are the largest single source,** ahead of state technology agencies. Their seasonal press releases (holiday shopping, Identity Theft Week, Cybersecurity Awareness Month) recycle older tip lists.
- **State technology agencies repeat it too.** Agencies in New Jersey, New York, Minnesota, Delaware, North Carolina, Oklahoma and Washington warn against public USB charging or tell people to turn off Bluetooth.
- **Shared templates carry the same advice from state to state.** Montana and Nevada repeat the wording of Ready.gov, the federal emergency preparedness site. Monthly newsletters from the Multi-State Information Sharing and Analysis Center (MS-ISAC), written for government staff, carry similar tips and are reposted on state sites in Mississippi, Hawaii and New Hampshire. Fixing one source would fix many pages at once.
- **Old pages stay live.** Pages from 2015 to 2019 in Connecticut, New Jersey, Tennessee and Utah are still online.

Our ask of state 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 state agencies.”

State scorecard

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

● Clear hacklore: at least one state page tells the public or small businesses to follow this advice.

○ Listed but not counted: milder hacklore, or advice written for state staff or tied to a one-time event such as foreign travel.

No mark: we found none.

State	Practices	Complexity	Public Wi-Fi	Password changes	USB charging	Bluetooth	Cookies
New York	6	●	●	●	●	●	●
New Jersey	5	●	●	●	●	●	
South Carolina	5	●	●	●	●	●	
Alabama	4	●	●	●	●		
Delaware	4	●	●	○	●	●	
Michigan	4	●	●	●	●		
North Carolina	4	●	●	●		●	
Ohio	4	●	●	●		●	
Oklahoma	4	●	●	●	●		
Virginia	4	●		●		●	●
Illinois	3	●	●	●			
Indiana	3	●	●	●			
Massachusetts	3	●	●	●			
Minnesota	3		●		●	●	
Missouri	3	●	●	●			
Nebraska	3	●	●	●		○	
Oregon	3	●	●	●			
Pennsylvania	3	●	●	●			
Washington	3		●		●	●	
California	2	●		●			
Colorado	2	●	●				
Georgia	2	●	●				
Iowa	2	●	●				
Maine	2	●		●			
Montana	2	●		●			
Nevada	2	●		●			
North Dakota	2	●		●			
Rhode Island	2	●	●				
Tennessee	2	●		●			
Texas	2	○	●		○		●
Utah	2	●	●				
West Virginia	2		●		○	●	
Wisconsin	2		●	●			
Wyoming	2	●	●				
Alaska	1			●			
Arizona	1		●				
Arkansas	1	●					
Connecticut	1			●			
Florida	1		●				
Hawaii	1		○	●			
Idaho	1		●				

State	Practices	Complexity	Public Wi-Fi	Password changes	USB charging	Bluetooth	Cookies
Kentucky	1			●			
Louisiana	1	●					
Maryland	1			●			
New Mexico	1	●					
Vermont	1	●					

Only milder hacklore or guidance for state staff: Mississippi and New Hampshire

None found: Kansas and South Dakota

Why this advice is retired

Advice	States	Why it doesn't help	What to say instead
Password complexity rules	33	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	30	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.
Change passwords regularly	28	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.
Turn off Bluetooth / NFC	10	Wireless attacks in the wild are extraordinarily rare and need special hardware, physical proximity and a device that hasn't been updated.	Leave Bluetooth on if you use it. Keep devices updated.
Avoid public USB charging	9	There are no verified cases of juice jacking (malware or data theft through a public charging port) affecting everyday users. Phones ask before allowing data transfer.	Charge wherever you need to.
Clear cookies regularly	3	Clearing cookies doesn't meaningfully improve security, and it doesn't stop modern tracking.	Drop the advice. Spend the time on updates and multi-factor authentication.

Sources: the hacklore.org letter (https://hacklore.org/letter) and FAQ (https://hacklore.org/faq). No state page we found tells the public never to scan QR codes, so that advice is left out. An Indiana IT tip sheet says never to scan codes “placed in random locations”; it is listed in the appendix as milder hacklore.

What we ask of state 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 states 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. **Update seasonal material before it goes out again.** Cybersecurity Awareness Month proclamations and releases for holiday shopping and Identity Theft Week are where the old tip lists come back each year.
4. **Check templates before reusing them.** Tip lists copied from Ready.gov and MS-ISAC newsletters carry the same retired advice from state to state.
5. **Retire old pages that nobody maintains.** Pages from 2015 to 2019 are still online in several states.
6. **Review guidance for state staff too.** We did not count it, but much of it repeats the same advice.
7. **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 Jersey: Cybersecurity and Communications Integration Cell (NJCCIC), the state's cyber agency

Says to change passwords “every three to six months” and to “Disable all Bluetooth functions when not in use.” Also warns against public charging stations and says to connect to a VPN instead of public Wi-Fi.

https://www.cyber.nj.gov/guidance-and-best-practices

New York: Department of State and Office of Information Technology Services

Says to “Periodically delete your web browser’s ‘cookies’” and to “Use complex passwords and change them regularly.” Also has a 2023 alert about juice jacking and 2024 advice to turn off Bluetooth in public.

https://dos.ny.gov/protecting-yourself-when-online

Pennsylvania: Attorney General

“Never use the same password for all of your accounts and change your passwords every month.”

https://attorneygeneral.gov/protect-yourself/identity-theft/identity-theft-preventative-measures-checklist

Missouri: Attorney General

“Change them every 60 days and choose combinations of letters, numbers, and symbols.” A 2025 release also says to avoid online purchases on public Wi-Fi.

https://ago.mo.gov/identity-theft-prevention/

South Carolina: Department of Consumer Affairs

“Change your passwords every three months to keep your accounts safe.” Also says “Disable Bluetooth When Not in Use.” A December 2025 release says “Avoid public USB charging stations.”

https://consumer.sc.gov/sites/consumer/files/Documents/Identity%20Theft/Cybersecurity_Basics.pdf

Ohio: Attorney General, consumer brochure

Says to “Turn off Bluetooth and Wi-Fi features when not in use” and to change passwords regularly.

https://www.ohioattorneygeneral.gov/Files/Publications-Files/Publications-for-Consumers/General/CHIPP-Stay-Safe-in-Cyberspace

Minnesota: Minnesota IT Services, April 2025

Says to avoid public charging stations and, if you must use public Wi-Fi, to use a VPN.

https://mn.gov/mnit/media/blog/?id=38-486805

Delaware: Department of Technology and Information, DigiKnow site

Its tips for travel abroad say to always use a VPN, turn off Bluetooth, and avoid public USB charging stations. Another page has a “Don’t Get Juice Jacked” video.

https://digiknow.delaware.gov/traveling-abroad/

Michigan: Attorney General

Has a consumer alert about juice jacking. A 2025 release says to avoid public Wi-Fi networks.

https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/id-theft-telemarketing/beware-of-juice-jacking

Nebraska: Attorney General

Says to avoid logging into email or financial accounts on public Wi-Fi and to change passwords regularly. Also recommends complexity rules.

https://protectthegoodlife.nebraska.gov/online-safety

Bright spots

- We found no public guidance repeating retired advice in Kansas or South Dakota.
- No state page we found tells the public never to scan QR codes. Most QR advice warns about tampered codes and payment pages, which matches hacklore.org's own guidance.

Method and caveats

- We searched official state government websites in October and November 2026: state technology and cyber agencies, attorneys general, consumer protection, emergency management, state police and governors' offices. County, city and university pages were excluded.
- Each quote has one of three tiers. Clear hacklore: advice to the public or small businesses that repeats a retired practice, including hedged versions (“consider,” “limit,” “be cautious”), narrower ones (only for banking, travel or home routers), warnings that point people toward the practice, complexity rules even alongside a long minimum length, and prompts to change every password for no reason. Milder hacklore: turning off Wi-Fi or Bluetooth for privacy or battery life rather than security, or QR advice limited to codes in random places or from unknown sources. Not counted: advice that matches the hacklore.org FAQ, advice written for state staff or for workers connecting to an employer's network, and password changes triggered by an event such as foreign travel. Only clear hacklore is counted.
- Advice for state staff is listed but not counted, because the hacklore.org letter addresses everyday people and small businesses. This includes MS-ISAC newsletters, which say they are written for an organization's end users at work.
- The scorecard counts how many retired practices a state repeats, not how many pages repeat them. A state that publishes more isn't marked down for volume.
- Every quote in the appendix was checked on November 14, 2026 on the live page, by script or, for sites that block automated tools, in a browser. The one exception is a New Hampshire courts PDF that blocks automated tools; it was checked against an archived copy, and it is written for court staff and not counted.
- Three pages found during the research (a Florida Department of Law Enforcement release, a Montana Small Business Development Center tip sheet and a North Dakota Information Technology article on juice jacking) had been removed before our first check on October 24, 2026. They are not counted and not listed.
- Quotes that come down after our first check on October 24, 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

186

quotes on live pages

183 quotes from 118 links in 48 states, checked on November 14, 2026, plus 1 removed since October 24, 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: turning off Wi-Fi or Bluetooth for privacy or battery life rather than security, or QR advice limited to codes in random places or from unknown sources. Listed but not counted.
- **Not counted:** Advice written for state staff, advice for workers connecting to an employer's network, advice that matches the hacklore.org FAQ, or a password change after an event such as foreign travel. Listed but not counted.

Alabama

Alabama Securities Commission, Back-to-School Cyber Tips (PDF), 2023-08-21
https://asc.alabama.gov/wp-content/uploads/2023/11/8-21-2023_Back-to-School_Cyber_Tips.pdf

Complexity, Password changes: “Update passwords frequently and use a mixture of letters, numbers, and characters, especially for passwords used to access financial accounts.” (page 1) Open at quote

Public Wi-Fi: “Avoid connecting to free public Wi-Fi.” (page 1) Open at quote

Office of Information Technology (OIT), "Mobile Device Security While Traveling," 2019-03-08
https://oit.alabama.gov/6058/mobile-device-security-while-traveling/

Public Wi-Fi: “If you must use public Wi-Fi, consider purchasing a mobile Virtual Private Network (VPN) application from a trustworthy company.” Open at quote

USB charging: “Another security pitfall to be aware of is public UBS charging stations.” Open at quote "UBS" is the page's typo for USB.

Alaska

Governor's Cybersecurity Awareness Month proclamation, 2022
https://gov.alaska.gov/cybersecurity-awareness-month-3

Password changes: “creating unique passwords and changing them regularly” Open at quote Governor's proclamation.

Governor's Cybersecurity Awareness Month proclamation, 2023
https://gov.alaska.gov/cybersecurity-awareness-month-4/

Password changes: “creating unique passwords and changing them regularly” Open at quote Governor's proclamation.

Governor's Cybersecurity Awareness Month proclamation, 2026
https://gov.alaska.gov/cybersecurity-awareness-month-2026/

Password changes: “creating unique passwords and changing them regularly” Open at quote

Arizona

Attorney General, Identity Theft press release, 2024-01-29
https://www.azag.gov/press-release/attorney-general-mayes-encourages-arizonans-beware-risks-identity-theft

Public Wi-Fi: “avoiding accessing sensitive information on public networks” Open at quote

Arkansas

Attorney General, Public Protection, "Passwords/WiFi" (undated)
https://arkansasag.gov/divisions/public-protection/technology/passwords-wifi/

Complexity: “Passwords should be complex and contain uppercase letters, lowercase letters, numbers and punctuation marks or special characters.” Open at quote

California

Attorney General, Cybersecurity Awareness Month release, 2024-10-17
https://oag.ca.gov/node/593491

Complexity: “include all four character types (uppercase, lowercase, numbers, and symbols)” Open at quote

Office of Emergency Services (Cal OES), "Cyber Safety: How to Avoid Cyber Risk," 2021-07-23
https://www.news.caloes.ca.gov/cyber-safety-how-to-avoid-cyber-risk

Complexity: “Create a password with eight characters or more along with a combination of upper and lowercase letters, numbers, and symbols.” Open at quote

Password changes: “Change passwords regularly.” Open at quote

Cal OES, Cybersecurity Awareness Month 2025
https://www.news.caloes.ca.gov/cybersecurity-awareness-month-2025-building-a-cyber-secure-california/

Complexity: “Create strong, complex passwords for your online accounts” Open at quote

Office of Emergency Services (Cal OES), Cybersecurity Awareness Month 2026, 2026-10-06
https://www.news.caloes.ca.gov/cybersecurity-awareness-month-2026/

Complexity: “Create strong, complex passwords for your online accounts” Open at quote

Colorado

Office of Information Technology (OIT), "5 Easy Habits to be Cyber Safe," 2023-10-12
https://oit.colorado.gov/blog-post/5-easy-habits-to-be-cyber-safe

Complexity: “Passwords should be at least 14 characters long and include a combination of uppercase letters, lowercase letters, numbers and symbols.” Open at quote

Public Wi-Fi: “Use a virtual private network (VPN) or a personal/mobile hotspot when you need a more secure connection.” Open at quote

Connecticut

Attorney General Jepsen, 2015-10-09
https://portal.ct.gov/ag/press-releases-archived/2015-press-releases/attorney-general-jepsen-october-is-national-cyber-security-awareness-month

Password changes: “Regularly change and update passwords and web keys” Open at quote 2015 release, still live.

Delaware

Dept. of Technology & Information (DTI), DigiKnow "Traveling Abroad" (undated)
https://digiknow.delaware.gov/traveling-abroad/

- **Public Wi-Fi:** “Always use a secure VPN when accessing the internet” Open at quote
- **Password changes:** “Change all passwords and device passcodes” Open at quote Not counted. Triggered by international travel, not a schedule.
- **USB charging:** “Do not plug USB-powered devices into public charging stations.” Open at quote
- **Bluetooth:** “Turn off your Bluetooth” Open at quote

DTI DigiKnow, "Protect Your Identity"
https://digiknow.delaware.gov/protect-your-identity/

- **Complexity:** “They are a combination of letters, both upper and lower case, numbers and symbols.” Open at quote

DTI DigiKnow, "Mobile Devices"
https://digiknow.delaware.gov/mobile-devices/

- **USB charging:** “Don’t Get Juice Jacked at the Airport” Open at quote Video title.

Florida

Attorney General, 2022-04-15
https://www.myfloridalegal.com/node/6811

- **Public Wi-Fi:** “refrain from using public WiFi when accessing personal and financial files or apps online” Open at quote

Attorney General, Evil Twin alert, 2024-10-30
https://www.myfloridalegal.com/node/27823

- **Public Wi-Fi:** “Consider using a virtual private network to encrypt data and make it more difficult for cybercriminals to access personal information via public Wi-Fi” Open at quote
- **Public Wi-Fi:** “Avoid conducting financial transactions or logging in to personal accounts when connected to public Wi-Fi” Open at quote

Georgia

Consumer Protection Division, 2021-10-04
https://consumer.georgia.gov/node/4161

- **Complexity:** “Mix letters, numbers and special characters.” Open at quote
- **Public Wi-Fi:** “Limit the types of business you conduct in this environment, being certain to avoid those that involve your personal or financial information, such as banking, credit card transactions or doing your taxes.” Open at quote

Hawaii

Governor's proclamation (posted by ETS, the state IT office), Oct 2021
https://ets.hawaii.gov/wp-content/uploads/2021/10/Cybersecurity-Awareness-Month_RTP-PDF.pdf

- **Password changes:** “create unique passwords and change them regularly” (page 1) Open at quote Governor's proclamation, 2021.

State IT newsletter (DAGS/ICSD), July 2013, likely aimed at staff
https://ags.hawaii.gov/wp-content/uploads/2013/07/July13_Newsletter6.pdf

- **Public Wi-Fi:** “Do not log into accounts, especially financial accounts, when using public wireless networks.” (page 1) Open at quote 2013 staff newsletter. Not counted. State staff newsletter (MS-ISAC tips for an organization's end users).

Idaho

Office of Emergency Management, 2024-01-30
https://ioem.idaho.gov/?p=10187

Public Wi-Fi: “This added layer of security is especially crucial when connecting to public Wi-Fi networks.” Open at quote

Office of Emergency Management, 2025-01-16
https://ioem.idaho.gov/?p=12954

Public Wi-Fi: “Use a Virtual Private Network (VPN) when accessing sensitive accounts on public networks.” Open at quote

Illinois

Attorney General, 2023-01-30
https://illinoisattorneygeneral.gov/news/story/attorney-general-raoul-recognizes-identity-theft-awareness-week

Public Wi-Fi: “Don’t use public Wi-Fi to shop or bank online.” Open at quote

Password changes: “Keep your passwords in a secure place and change them regularly.” Open at quote

Ready Illinois / emergency management agency (IEMA), 2019-10-01
https://ready.illinois.gov/news-releases/100119.html

Complexity: “When creating a password, use at least 10 characters, with a combination of uppercase and lowercase letters, numbers and symbols.” Open at quote

Emergency management and homeland security agency (IEMA-OHS), 2023-10-23
https://iemaohs.illinois.gov/news/press-release.27173.html

Complexity: “includes four different kinds of keyboard characters (Aa1!)” Open at quote

Governor's office and Dept. of Innovation and Technology (DoIT), Cybersecurity Awareness Month release, 2026-10-05
https://gov.illinois.gov/news/press-release.32995.html

Complexity: “consider making them complex (upper, lowercase, numbers, symbols)” Open at quote

Indiana

Dept. of Homeland Security, Get Prepared: Cybersecurity
https://www.in.gov/dhs/get-prepared/general-safety/cybersecurity

Complexity: “Passwords should be at least eight characters long and use combinations of uppercase and lowercase letters, numbers and punctuation.” Open at quote

Public Wi-Fi: “Avoid shopping on a public computer or public Wi-Fi network.” Open at quote

Password changes: “Regularly change passwords for every account.” Open at quote

Dept. of Homeland Security, Get Prepared: Cybersecurity
https://secure.in.gov/dhs/get-prepared/files/cybersecurity.pdf

Complexity: “Passwords should be at least eight characters long and use combinations of uppercase and lowercase letters, numbers and punctuation.” (page 2) Open at quote

Public Wi-Fi: “Avoid shopping on a public computer or public Wi-Fi network.” (page 2) Open at quote

Password changes: “Regularly change passwords for every account.” (page 3) Open at quote

Office of Technology 2026 password policy (employees)
https://www.in.gov/iot/files/2026-New-Password-Requirements_Indiana-State.pdf

Password changes: “New Password will be required every 365 days.” (page 2) Open at quote Not counted. Password policy for state employees.

Office of Technology QR tip sheet (KnowBe4 template)
https://in.gov/iot/files/QR_Codes_Enjoy_Safe_Scanning.pdf

QR codes: “never scan QR codes placed in random locations” (page 1) Open at quote Milder hacklore. Limited to codes in random locations; stricter than the FAQ but not "never scan."

Iowa

Workforce Development flyer for unemployment claimants, Oct 2023
https://workforce.iowa.gov/media/1379/download

- **Complexity:** “Include a combination of upper and lowercase letters, numbers, and special characters.” (page 1) Open at quote
- **Public Wi-Fi:** “If using Wi-Fi from other public locations, use a Virtual Private Network.” (page 1) Open at quote

Kentucky

Kentucky Public Pensions Authority Cybersecurity page
https://kyret.ky.gov/About/Pages/Cybersecurity.aspx

- **Password changes:** “Be cautious and change your email passwords often and use unique passwords for each online account you have.” Open at quote

Louisiana

Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), "Cybersecurity"
https://gohsep.la.gov/preparedness/cybersecurity/

- **Complexity:** “Your password should include a variety of uppercase letters, lowercase letters, numbers, and special characters.” Open at quote

Maine

Maine CDC (part of DHHS) Drinking Water Program bulletin, 2025-10-08
https://content.govdelivery.com/accounts/MEHHS/bulletins/3f60ee2

- **Complexity:** “Length and Complexity: Use a mix of upper and lower-case letters, numbers, and special characters.” Open at quote
- **Password changes:** “Change Passwords Regularly: Regular updates help maintain security.” Open at quote

Maryland

Maryland Insurance Administration, "Cybersecurity" (Tips for Small Business Owners) (small businesses)
https://insurance.maryland.gov/Consumer/Pages/Cybersecurity.aspx

- **Password changes:** “Require employees to change passwords at least every three months.” Open at quote

Massachusetts

Office of Consumer Affairs and Business Regulation, "Cybersecurity for Consumers"
https://www.mass.gov/info-details/cybersecurity-for-consumers

- **Complexity:** “Choose strong passwords – stay away from common words and include uppercase & lowercase letters, numbers and characters.” Open at quote
- **Public Wi-Fi:** “Limit your access to banking accounts and other sensitive personal information when using public Wi-Fi.” Open at quote
- **Password changes:** “Do not use the same password for all of your accounts and change your password routinely.” Open at quote

Office of the Comptroller, 2023-10-24 (employees)
https://www.macomptroller.org/announcement/say-no-to-public-wi-fi/

This page was taken down.

- **Removed by November 14, 2026. Public Wi-Fi:** “Public Wi-Fi is not secure, even if VPN is used.” Not counted. Notice for state staff.

Michigan

Attorney General / Consumer Protection, "Beware of Juice Jacking" consumer alert (undated)
https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/id-theft-telemarketing/beware-of-juice-jacking

USB charging: “Stay away from public charging kiosks or portable wall chargers if you can.” Open at quote

Attorney General, 2025-10-14
https://www.michigan.gov/ag/news/press-releases/2025/10/14/attorney-general-nessel-reissues-consumer-alert-on-ransomware-during-cybersecurity-awareness-month

Public Wi-Fi: “Avoid using public Wi-Fi networks, since many of them are not secure, and cybercriminals can snoop on your internet usage.” Open at quote

Attorney General, 2026-02-10
https://www.michigan.gov/ag/news/press-releases/2026/02/10/ag-nessel-reissues-online-shopping-consumer-alert-ahead-of-valentines-day

Public Wi-Fi: “If shopping online using public Wi-Fi, consumers can install a Virtual Private Network (VPN)” Open at quote

Consumer Protection, "Credit Card Safety"
https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/shopping/credit-card-safety

Public Wi-Fi: “Do NOT use public Wi-Fi to shop, conduct financial transactions, or even check your accounts.” Open at quote

Dept. of Technology, Management & Budget (DTMB), Best Practices
https://www.michigan.gov/dtmb/services/cybersecurity/cybersecurity-resource-hub/best-practices

Complexity: “Use strong, unique passwords that are a combination of uppercase and lowercase letters, numbers, and special characters.” Open at quote

Governor's Cybersecurity Awareness Month proclamation, 2026
https://www.michigan.gov/whitmer/news/proclamations/2026/10/01/october-2026-cybersecurity-awareness-month

Password changes: “creating unique passwords and changing them regularly” Open at quote

Minnesota

MNIT (state IT agency), "Cybersecurity on the move," 2025-04-25
https://mn.gov/mnit/media/blog/?id=38-486805

Public Wi-Fi: “If you must use public WiFI, use a virtual private network (VPN)” Open at quote

USB charging: “Avoid using public charging stations such as those in airports and hotels that may contain viruses or malware.” Open at quote

Bluetooth: “Turn off WiFi and Bluetooth on your device when not in use to protect your privacy and save battery life.” Open at quote Milder hacklore. Privacy and battery rationale, not the security claim the letter retires.

MNIT, "Mobile Device Safety Tips," 2023-10-16
https://mn.gov/mnit/media/blog/?id=38-593619

Public Wi-Fi: “Avoid using sensitive information, such as passwords and credit card numbers, on public WiFi.” Open at quote

Bluetooth: “Keep an eye on the Bluetooth or WiFi feature of your device in public locations and disable it if needed to reduce the possibility of an attack.” Open at quote

Attorney General, "Using Public Wi-Fi Networks"
https://www.ag.state.mn.us/consumer/Publications/PublicWiFi.asp

Public Wi-Fi: “it can be best to avoid using mobile apps for relaying important information on public Wi-Fi networks altogether” Open at quote

Mississippi

ITS (state IT agency) newsletter, Nov 2022

https://www.its.ms.gov/sites/default/files/ServicesPDFs/2022_11_newsletter_Shop-Smart-and-Stay-Safe-This-Holiday-Season.pdf

- **Public Wi-Fi:** “Abstain from using public Wi-Fi at all costs while purchasing and placing orders.” (page 1) Open at quote Not counted. MS-ISAC newsletter written for an organization's end users at work.
- **Password changes:** “Change your passwords regularly.” (page 2) Open at quote Not counted. MS-ISAC newsletter written for an organization's end users at work.

ITS newsletter, Oct 2022

https://www.its.ms.gov/sites/default/files/ServicesPDFs/2022_10_newsletter_Protect-Your-Identity-Cybersecurity-Awareness-Month.pdf

- **Public Wi-Fi:** “Use a VPN to encrypt your data whenever possible” (page 1) Open at quote Not counted. MS-ISAC newsletter written for an organization's end users at work.

ITS newsletter, Dec 2020

https://www.its.ms.gov/sites/default/files/ServicesPDFs/2020_12_Newsletter_10_Cybersecurity_Shopping_Tips_Holiday_Season.pdf

- **Public Wi-Fi:** “Do not use public Wi-Fi for any shopping activity.” (page 1) Open at quote Not counted. MS-ISAC newsletter written for an organization's end users at work.
- **Cookies:** “periodically clear your offline content, cookies, and history” (page 3) Open at quote Not counted. MS-ISAC newsletter written for an organization's end users at work.

Missouri

Attorney General, Identity Theft Prevention

https://ago.mo.gov/identity-theft-prevention/

- **Complexity, Password changes:** “Change them every 60 days and choose combinations of letters, numbers, and symbols.” Open at quote
- **Public Wi-Fi:** “When working remotely or traveling, use a VPN or a secure, private connection to keep your data protected.” Open at quote
- **Public Wi-Fi:** “Avoid entering personal or financial information on public Wi■Fi networks.” Open at quote

Office of Administration, Secure at Home

https://cybersecurity.mo.gov/secure-at-home/

- **Complexity:** “use a combination of upper-case and lower-case letters, numbers, and symbols if possible” Open at quote

Attorney General, 2025-12-02

https://ago.mo.gov/attorney-general-hanaway-warns-missourians-to-stay-alert-for-holiday-scams/

- **Public Wi-Fi:** “Avoid making online purchases while connected to public Wi-Fi, which may not be secure.” Open at quote

Montana

Disaster & Emergency Services, Cyber Attack page (same text as Ready.gov and Nevada)

https://des.mt.gov/Preparedness/Cyber-Attack

- **Complexity:** “Create strong passwords by using upper and lower case letters, numbers and special characters.” Open at quote Same text as Ready.gov and Nevada.
- **Password changes:** “change passwords regularly” Open at quote

Nebraska

Attorney General, Online Safety

https://protectthegoodlife.nebraska.gov/online-safety

- **Complexity:** “Combine capital and lowercase letters with numbers and symbols to create a more secure password.” Open at quote
- **Public Wi-Fi:** “Limit what you do on public Wi-Fi and avoid logging into key accounts like email or financial services.” Open at quote
- **Bluetooth:** “To avoid this, you may disable Wi-Fi and Bluetooth when not in use.” Open at quote Milder hacklore. Privacy rationale (store tracking), and hedged: "you may disable."

Attorney General, Cyber Security Awareness Month release, around 2017
https://protectthegoodlife.nebraska.gov/news/nebraska-attorney-general%E2%80%99s-office-recognizes-cyber-security-awareness-month

- **Complexity:** “Use complex passwords with a combination of numbers, symbols, and letters.” Open at quote
- **Password changes:** “Change your passwords regularly, especially if you believe they have been compromised.” Open at quote

Attorney General, National Consumer Protection Week release
https://protectthegoodlife.nebraska.gov/attorney-general-peterson-announces-national-consumer-protection-week

- **Password changes:** “Set strong passwords, change them regularly, and keep them private” Open at quote

Nevada

Office of Emergency Management, Cybersecurity Awareness (same text as Montana)
https://www.oem.nv.gov/emergency-management/threats-hazards/cybersecurity-awareness/

- **Complexity:** “Create strong passwords by using upper and lower case letters, numbers and special characters.” Open at quote Same text as Ready.gov and Montana.
- **Password changes:** “change passwords regularly” Open at quote

New Hampshire

Judicial Branch, republished MS-ISAC newsletter, 2021
https://www.courts.nh.gov/sites/g/files/ehbemt471/files/documents/2021-07/what_is_cybercrime.pdf

- **Complexity:** “When creating a password, use at least 10 characters, with a combination of uppercase and lowercase letters, numbers, and symbols.” Open at quote Not counted. Republished MS-ISAC newsletter written for an organization's end users at work.

New Jersey

NJCCIC (state cyber agency), Guidance and Best Practices main page
https://www.cyber.nj.gov/guidance-and-best-practices

- **Complexity:** “The inclusion of multiple character sets - uppercase and lowercase letters, numbers, and special characters (@#!$%&, etc.) will further enhance the strength of your password.” Open at quote Open the "Passwords" section to see it.
- **Public Wi-Fi:** “Avoid using public computers and public Wi-Fi connections to log into accounts and access sensitive information.” Open at quote Open the "Internet Safety" section to see it.
- **Password changes:** “Avoid using the same password for multiple accounts, and change them every three to six months.” Open at quote Open the "Passwords" section to see it.
- **Bluetooth:** “Disable all Bluetooth functions when not in use” Open at quote Open the "Device Security" section to see it.

NJCCIC, Stay Cyber Safe This Holiday Season
https://www.cyber.nj.gov/guidance-and-best-practices/cyber-hygiene/stay-cyber-safe-this-holiday-season

- **USB charging:** “Avoid Connecting Devices to Public Charging Stations” Open at quote Section heading.

NJCCIC, Cyber Safe Travel Tips
https://www.cyber.nj.gov/guidance-and-best-practices/cyber-hygiene/cyber-safe-travel-tips

- **Public Wi-Fi:** “If you must connect to a public Wi-Fi network, use encrypted connections such as via a Virtual Private Network (VPN)” Open at quote
- **Password changes:** “Change all passwords on accounts that were accessed while overseas.” Open at quote Not counted. Triggered by international travel, not a schedule.
- **USB charging:** “Refrain from charging your devices in taxis, Ubers, or rideshare vehicles.” Open at quote

NJCCIC, Mobile Device Security
https://www.cyber.nj.gov/guidance-and-best-practices/device-security/mobile-device-security

- **Public Wi-Fi:** “Connect to virtual private networks instead of widely-used and public WiFi networks.” Open at quote

NJCCIC, Virtual Private Networks
https://www.cyber.nj.gov/guidance-and-best-practices/wi-fi-network-security/virtual-private-networks

Public Wi-Fi: “The use of VPNs is highly advised for when connected to unsecured or public networks.” Open at quote

NJCCIC, Cybersecurity for Small and Medium-Sized Businesses (business)
https://www.cyber.nj.gov/guidance-and-best-practices/cyber-hygiene/cybersecurity-for-small-medium-sized-businesses

Public Wi-Fi: “Only allow public Wi-Fi use in conjunction with a virtual private network (VPN).” Open at quote Not counted. Business policy for staff on public Wi-Fi; a work VPN is a use the FAQ supports.

Attorney General / Division of Consumer Affairs flier, 2016
https://nj.gov/lps/library/OAG-Cyber-Security-Flier.pdf

Public Wi-Fi: “Don’t use public WiFi, especially for financial or other sensitive transactions” (page 1) Open at quote 2016 flier.

Dept. of Children and Families, Safety Tips for Wi-Fi Hotspots, 2021
https://www.nj.gov/dcf/documents/Safety%20Tips%20for%20WIFI%20Hotspots.pdf

Public Wi-Fi: “Avoid using public computers and public Wi-Fi connections to log into accounts or to access confidential or sensitive information.” (page 1) Open at quote

NJCCIC, Cybersecurity Awareness Month 2026
https://www.cyber.nj.gov/connect/events/cybersecurity-awareness-month-cam

Complexity: “Strong passwords are at least 15 characters long and include a variety of characters.” Open at quote

New Mexico

Educational Retirement Board, 2026-08-28
https://www.erb.nm.gov/2026/08/28/simple-habits-to-keep-your-online-accounts-and-personal-information-secure/

Complexity: “A strong password should be a long phrase mixing letters, numbers, and symbols.” Open at quote

Office of Broadband Access & Expansion, "Password Tips" infographic
https://connect.nm.gov/uploads/1/4/1/9/141989814/password_tips.pdf

Complexity: “Lowercase, uppercase, symbols, and numbers can all have a home in your password.” (page 1) Open at quote In the "Password Tips" infographic linked from the page.

New York

Dept. of State, juice-jacking alert, 2023-06-05
https://dos.ny.gov/news/consumer-alert-new-york-department-states-division-consumer-protection-warns-new-yorkers-juice

USB charging: “Use the wall plug-in socket to charge your devices.” Open at quote

Dept. of State, "Protecting Yourself When Online"
https://dos.ny.gov/protecting-yourself-when-online

Complexity, Password changes: “Use complex passwords and change them regularly.” Open at quote

Public Wi-Fi: “Don’t transmit sensitive information in a public wi-fi hotspot you don’t trust, even if the transmission is encrypted.” Open at quote

Cookies: “Periodically delete your web browser’s “cookies.”” Open at quote

ITS (state IT agency), 2024-05-13
https://its.ny.gov/news/add-cybersecurity-your-vacation-checklist

Public Wi-Fi: “Consider using a virtual private network (VPN) on your device to encrypt your internet connection, shielding your information from prying eyes.” Open at quote

USB charging: “Only charge your device with a charger plugged directly into an electric wall outlet.” Open at quote

Bluetooth: “allow your device to connect wirelessly via Bluetooth with other devices, like headphones or infotainment systems in vehicles. This could allow unwanted devices to access your data, so it is best to toggle them off when in public.” Open at quote

ITS, 2021-01-28
https://its.ny.gov/news/dont-get-scammed-tips-secure-your-private-information

Complexity: “Use 10 to 12 characters in a combination of letters (upper and lower case), numbers, and symbols.” Open at quote

Public Wi-Fi: “Limit what you do on public Wi-Fi and avoid logging into sensitive accounts.” Open at quote

Password changes: “Regularly change your passwords” Open at quote

ITS password security page (employees)
https://its.ny.gov/password-security

Complexity: “DO use complex passwords and change them in accordance with your agencies' policy.” Open at quote Not counted. Password guidance for state employees.

North Carolina

NCDIT (state IT agency), Holiday tips
https://it.nc.gov/resources/online-safety-privacy/tips-guidance/holiday-cybersecurity-tips

Public Wi-Fi: “Use a VPN or your mobile hotspot instead of public Wi-Fi.” Open at quote

NCDIT, Traveling tips
https://it.nc.gov/resources/online-safety-privacy/tips-guidance/cybersecurity-while-traveling

Bluetooth: “Disable remote connectivity and Bluetooth.” Open at quote

NC Dept. of Justice (DOJ), 2025 Data Breach Report
https://ncdoj.gov/2025-data-breach-report/

Password changes: “Use strong, unique passwords for each account and change them regularly.” Open at quote

NC DOJ, Wi-Fi Safety
https://ncdoj.gov/internet-safety/wi-fi-safety/

Complexity: “Use a mix of numbers, alphanumeric symbols (@,!,%, etc.), and upper and lowercase letters in your password.” Open at quote

Governor's Cybersecurity Awareness Month proclamation, 2026
https://governor.nc.gov/governor-stein-proclaims-cybersecurity-awareness-month-0

Password changes: “creating strong and unique passwords and changing them periodically” Open at quote

North Dakota

Insurance Dept., Cybersecurity page
https://www.insurance.nd.gov/consumers/insurance/cybersecurity

Complexity: “Keep passwords private and complex.” Open at quote

Password changes: “implement settings encouraging regular password changes” Open at quote In advice for small businesses.

Ohio

Attorney General, CHIPP "Stay Safe in Cyberspace"
https://www.ohioattorneygeneral.gov/Files/Publications-Files/Publications-for-Consumers/General/CHIPP-Stay-Safe-in-Cyberspace

Complexity: “All passwords should be at least 12 characters long and include capital and lowercase letters, numbers and symbols.” (page 6) Open at quote

Public Wi-Fi: “Consider using a reputable virtual private network (VPN) to help better secure your data and protect your privacy.” (page 6) Open at quote

Password changes: “Use strong and unique passwords for each of your online accounts and change them regularly.” (page 7) Open at quote

Bluetooth: “Turn off Bluetooth and Wi-Fi features when not in use.” (page 4) Open at quote

Attorney General, Consumer Advocate newsletter, October 2026
https://www.ohioattorneygeneral.gov/Media/Newsletters/Consumer-Advocate/October-2026/Cybersecurity-Awareness-Month-Don-t-make-it-easy-o

Complexity: “Make passwords at least 16 characters, including uppercase and lowercase letters, numbers, and special characters” Open at quote

Oklahoma

OMES Cyber Command (state cyber unit), travel tips, 2023-06-16, modified 2025-12-09
https://oklahoma.gov/omes/services/information-services/is/cybercommand/newsroom/2023/cybersecurity-tips-to-travel-safe.html

Complexity: “use strong passwords that include a mix of letters, numbers and special characters” Open at quote

Public Wi-Fi: “Use a VPN (virtual private network): A VPN encrypts and converts data on public Wi-Fi into untraceable form.” Open at quote

USB charging: “Be cautious of public charging stations: Though public charging stations are convenient, they can also be a hotspot for cybercriminals.” Open at quote

Office of Management and Enterprise Services (OMES), "31 Days of Cybersecurity" checklist (PDF), October 2026
https://oklahoma.gov/content/dam/ok/en/omes/documents/31-days-cs-checklist-UA.pdf

Complexity: “Change a weak password to something complex and unique.” (page 1) Open at quote

Password changes: “Update all account passwords.” (page 1) Open at quote

OMES, Cybersecurity Awareness Month release, 2026-10-01
https://oklahoma.gov/omes/newsroom/2026/oklahoma-looks-to-the-next-250-years-during-cybersecurity-awaren.html

Complexity: “create unique, complex passwords (or passphrases) for each account” Open at quote

Oregon

Division of Financial Regulation
https://dfr.oregon.gov/financial/protect/pages/protect-your-identity.aspx

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

Password changes: “Consider changing out your passwords every 90 days.” Open at quote

Office of Emergency Management, 2025-10-15
https://apps.oregon.gov/oregon-newsroom/OR/OEM/Posts/Post/Cybersecurity-Awareness-Month-2025

Public Wi-Fi: “Avoid using public Wi-Fi for sensitive matters, including financial transactions; use a Virtual Private Network (VPN) if needed.” Open at quote

Pennsylvania

Attorney General, Identity Theft Preventative Measures Checklist
https://attorneygeneral.gov/protect-yourself/identity-theft/identity-theft-preventative-measures-checklist

Password changes: “Never use the same password for all of your accounts and change your passwords every month.” Open at quote

Attorney General, Proper Secure Passwords
https://www.attorneygeneral.gov/protect-yourself/identity-theft/identity-theft-proper-secure-passwords/

Complexity: “Get creative with mixing numbers, symbols, and uppercase letters in your own way.” Open at quote

Password changes: “Change your password regularly.” Open at quote

Dept. of Banking and Securities
https://www.pa.gov/agencies/dobs/cybersecurity

Complexity: “at least 8 characters in length with a mixture of letters, numbers, and symbols” Open at quote

Public Wi-Fi: “Avoid using unsecured, public wireless access points, such as those found in airports, coffee shops, and hotels.” Open at quote

Rhode Island

Dept. of Business Regulation (DBR) Insurance Division, Consumer Alert 2018-6
https://dbr.ri.gov/sites/g/files/xkgbur696/files/documents/divisions/insurance/consumers/Consumer_Alert_2018-6.pdf

- **Complexity:** “Experts recommend passwords with a combination of upper and lowercase letters, numbers and symbols.” (page 2) Open at quote

State Police, "Computing Safely"
https://risp.ri.gov/safety-education/internet-safety/computing-safely

- **Complexity:** “Strong, unique passwords have eight characters or more and use a combination of letters, numbers and symbols” Open at quote
- **Public Wi-Fi:** “Avoid connecting to any Wi-Fi network unless you know it's secure.” Open at quote

South Carolina

Dept. of Consumer Affairs, 2025-12-15
https://consumer.sc.gov/news/2025-12/tis-season-holiday-and-travel-scams

- **Public Wi-Fi:** “Avoid public Wi-Fi.” Open at quote
- **USB charging:** “Avoid public USB charging stations.” Open at quote

Dept. of Consumer Affairs, Cyber Security Basics PDF, Nov 2023
https://consumer.sc.gov/sites/consumer/files/Documents/Identity%20Theft/Cybersecurity_Basics.pdf

- **Complexity:** “Make sure your password is at least 12 characters long with uppercase and lowercase letters, numbers and symbols.” (page 2) Open at quote
- **Public Wi-Fi:** “Public Wifi networks are not secure, which means that anyone may see what you are doing while you are connected.” (page 1) Open at quote
- **Password changes:** “Change your passwords every three months to keep your accounts safe.” (page 2) Open at quote

Dept. of Consumer Affairs, Smartphone Safety PDF
https://consumer.sc.gov/sites/consumer/files/Documents/Spotlight/Smartphone_Safety.pdf

- **Bluetooth:** “Disable Bluetooth When Not in Use.” (page 1) Open at quote

Dept. of Revenue, Security Center
https://dor.sc.gov/tax-education/security-center

- **Complexity:** “Contain at least one capital letter (A-Z), one lowercase letter (a-z), one number (1, 2, 3…), and one special character (*!#>/%@…)” Open at quote
- **Password changes:** “Be changed on a regular basis or once a year” Open at quote

Tennessee

Dept. of Commerce & Insurance, 2018-10-05
https://www.tn.gov/commerce/news/2018/10/5/tdci--secure-your-information-during-cyber-security-awareness-month.html

- **Complexity:** “Make passwords strong by using a combination of uppercase and lowercase letters, numbers, and symbols.” Open at quote 2018 release.
- **Password changes:** “occasionally change the login and password” Open at quote About home routers.

Attorney General, 2024-08-20
https://www.tn.gov/attorneygeneral/news/2024/8/20/pr24-66.html

- **QR codes:** “Only scan QR codes from trusted sources, such as reputable businesses or official websites.” Open at quote Not counted. Consistent with the hacklore.org FAQ on tampered and unsolicited codes.

Texas

Dept. of Information Resources (DIR, state IT agency), 2024-10-17
https://dir.texas.gov/news/cybersecurity-practices-remote-work

- **Public Wi-Fi:** “Always connect through a virtual private network (VPN) for an additional layer of security.” Open at quote
  Not counted. Remote-work page; an employer VPN is a use the FAQ supports.
- **Public Wi-Fi:** “Avoid public or unsecured Wi-Fi connections, which are often targeted by cybercriminals.” Open at quote
  Not counted. Remote-work guidance about connecting to an employer's network, like the VPN tip on the same page.

Dept. of Public Safety (DPS) Cyber Security Newsletter, May 2023, written for staff
https://www.dps.texas.gov/InformationTechnology/Cyber/Newsletters/2023/2023-05.pdf

- **Complexity:** “Aim for a password that is at least 12 characters long and uses a mix of upper and lowercase letters, numbers, and special characters.” (page 2) Open at quote Not counted. Staff newsletter.
- **USB charging:** “Avoid using a public USB charging station.” (page 3) Open at quote Not counted. Staff newsletter.

Texas.gov, "Cybersecurity"
https://www.texas.gov/family-support-services/public-safety/cybersecurity

- **Public Wi-Fi:** “Avoid connecting to public Wi-Fi in coffee shops, libraries, or other shared locations whenever possible.” Open at quote
- **Cookies:** “Delete your browsing history, cookies, and search history regularly.” Open at quote

Utah

Attorney General, 2019-10-29
https://attorneygeneral.utah.gov/cyber-security-awareness-month-2019/

- **Complexity:** “Use a mixture of upper and lowercase letters as well as numbers and symbols.” Open at quote 2019 release.
- **Public Wi-Fi:** “Either use a virtual private network (VPN) or use your phone as a hotspot.” Open at quote

Vermont

Agency of Digital Services, Ready Vermont weekly series, 2024-10-08
https://ready.vermont.gov/cybersecurity-awareness-month-weekly-series-password-complexity

- **Complexity:** “Use a mix of uppercase and lowercase letters, numbers, and special characters.” Open at quote

Virginia

Attorney General, Computer Crime Section, "Cybertips"
https://www.oag.state.va.us/ccsweb2/index.php/internet-safety/cybertips

- **Complexity:** “Use a combination of letters, numbers, and special characters when creating a password.” Open at quote
- **Bluetooth:** “Disable Bluetooth technology when you are not using it.” Open at quote
- **Cookies:** “Limit the use of cookies in your web browser.” Open at quote

Attorney General, Computer Crime Section, "Computer Security Tips"
https://www.oag.state.va.us/ccsweb2/index.php/internet-safety/computer-security-tips

- **Complexity:** “Use variations of capital and lowercase letters, numbers, and special symbols of at least 8 characters.” Open at quote

Attorney General, Computer Crime Section, "Internet Safety Tips - Businesses" (small businesses)
https://www.oag.state.va.us/ccsweb2/index.php?view=article&id=15%3Ainternet-safety-tips-businesses&catid=9

- **Password changes:** “Require these passwords to be changed frequently, at least every 3 months.” Open at quote

Washington

WaTech (state technology agency), public Wi-Fi tips
https://watech.wa.gov/node/1300

Public Wi-Fi: “Even if you have a VPN, it is still not recommended to access personal bank accounts, or similar sensitive personal data like social security numbers, on unsecured public networks.” Open at quote

WaTech Office of Cybersecurity Wi-Fi tips, Korean-language version, Nov 2023
https://cybersecurity.wa.gov/sites/default/files/2023-11/WaTech_OCS_Safe_Wifi_Tips_Detailed_KO.pdf

Bluetooth: “익숙하지 않은 지역에 있을 때는 전화기와 다른 장치에서 이러한 기능을 꺼놓으십시오.” (page 2) Open at quote Korean. Means "Turn these features off on your phone and other devices when in unfamiliar areas."

WaTech, "Staying cyber safe on summer vacation"
https://watech.wa.gov/staying-cyber-safe-summer-vacation

USB charging: “Avoid public charging stations” Open at quote

WaTech Office of Cybersecurity, "Stay safe online while traveling"
https://watech.wa.gov/ocs/news/stay-safe-online-while-traveling

USB charging: “Avoid public charging stations” Open at quote

West Virginia

Board of Risk & Insurance Management (BRIM) Privacy Office, June 2026 tip (employees)
https://brim.wv.gov/media/636/download

Public Wi-Fi: “Avoid public Wi-Fi for anything involving a password.” (page 1) Open at quote Not counted. Tip for state employees.

USB charging: “never plug your phone into a public USB charging station” (page 1) Open at quote Not counted. Tip for state employees.

Broadband Enhancement Council
https://broadband.wv.gov/using-wifi-safely/

Public Wi-Fi: “Don’t shop online when using public Wi-Fi.” Open at quote

Bluetooth: “However, leaving Bluetooth on while in public places can pose a risk to your cybersecurity.” Open at quote

Wisconsin

Dept. of Agriculture, Trade and Consumer Protection (DATCP), Public Wi-Fi fact sheet
https://datcp.wi.gov/Documents/IDTheftWi-FiTips659.pdf

Public Wi-Fi: “If you regularly access online accounts through WiFi hotspots, use a virtual private network (VPN).” (page 2) Open at quote

Governor's Cybersecurity Awareness Month proclamation, 2025
https://evers.wi.gov/Documents/100125_Accessible%20Proclamation_National%20Cybersecurity%20Month.pdf

Password changes: “creating and regularly changing unique passwords” (page 1) Open at quote

Wyoming

Enterprise Technology Services (ETS), "Seasonal Tips"
https://ets.wyo.gov/cybersecurity/resources-campaigns/seasonal-tips

Complexity: “Mix letters, numbers, and special characters.” Open at quote

Public Wi-Fi: “Always use a virtual private network when connecting to public Wi-Fi.” Open at quote

ETS, "Public Wi-Fi: What Is It and What You Need to Know to Stay Safe"
https://ets.wyo.gov/cybersecurity/general-cybersecurity-practices/public-wi-fi-what-is-it-and-what-you-need-to-know-to-stay-safe

Public Wi-Fi: “The simple advice is NOT to access any confidential data while you are on a public network.” Open at quote

ETS, "QR Codes: What Are They and How Are They Used"
https://ets.wyo.gov/cybersecurity/general-cybersecurity-practices/qr-codes-what-are-they-how-are-they-used

QR codes: “avoid scanning QR codes from unknown sources, and instead type out URLs manually” Open at quote

Milder hacklore. Limited to codes from unknown sources; stricter than the FAQ but not "never scan."