NATIONAL CYBERSECURITY ALLIANCE

SECURITY TIPS FOR USING PUBLIC COMPUTERS & WIRELESS NETWORKS

Public computers in libraries, schools, and other locations are convenient and can be great resources for many Internet users; however, it's important to remember good online safety habits when using these devices.

TIPS AND BEST PRACTICES:



REMEMBER ME NOT

When you log into any account on a shared computer, don't check the box to "remember me" for that account. Checking "remember me" will make it easy for the next user to access your sensitive accounts.

Also, if you have to make a purchase on a public computer, do not save your financial information in the account. The best case scenario is to not use public computers to access sensitive information (such as banking) or to complete financial transactions (such as purchases).

LOG OUT

Anyone can access public computers, and you wouldn't want just anyone to have access to your personal information and accounts. Close all browser tabs and log out of your accounts when you are done using a public device. Simply clicking "x" in your internet browser does not log you out of accounts. Log out of every single account you logged into on the shared computer.

DEFINITION OF CYBERSECURITY:

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

NATIONAL CYBERSECURITY ALLIANCE

SECURITY TIPS FOR USING PUBLIC COMPUTERS & WIRELESS NETWORKS

TIPS AND BEST PRACTICES



DELETE YOUR BROWSING HISTORY
Simply use the browser tools available to delete your cookies and history when you are finished using a public computer.



AVOID SHOULDER SURFERS
Be aware of your surroundings. Others might be able to peer over your shoulder to see your screen or what you're typing. Be extra aware, especially if you have to access a sensitive account on a public computer, such as a banking site.



LOCK DOWN YOUR LOGIN
Create long and unique passphrases for all accounts and use multifactor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.



GET SAVVY ABOUT WIFI HOTSPOTS
Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi, and avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.

ADDITIONAL RESOURCES

- **NCSA:** Own Your Role in Cybersecurity: Start with the Basics Tipsheet
  https://staysafeonline.org/resource/own-your-role-in-cybersecurity/
- **CISA:** What Is Cybersecurity?
  https://www.us-cert.gov/ncas/tips/ST04-001