



In this day and age, nearly everything can be done on the go via Internet access from our computers, laptops, and cellular devices. We interact with our colleagues, handle personal information and photos, and receive news—all online. What we may take for granted—or perhaps not realize—is the great length our federal government goes to ensure our digital infrastructure is safe and secure.

Our digital infrastructure is a national asset, and maintaining its security falls on each of us. Thus, the President designated October as **National Cybersecurity Awareness Month**. The OSOP would like to take this opportunity to provide NIH staff with tips on how to protect their private information on government networks and digital devices.

Cybersecurity and Privacy 101

Review privacy policies. Before submitting your name, email address, or other personally identifiable information (PII) on a website, check out its **privacy policy**. A privacy policy informs you of how your information will be used and/or shared, and is an easy way to determine the website's legitimacy. If a company or organization's website does not have a privacy policy posted, give them a call and request one, or use an alternative website. Make sure you read the policy carefully: some privacy policies include opt-in and opt-out options for subscriptions to other mailing lists or services.

Make sure your information is protected. Even if a privacy policy is in place, many websites do not adequately protect the information you give them. Only use websites that use secured sockets layer (SSL) technology to encrypt your information. If an attacker breaks into a vendor's system and your information is unencrypted, you can be a victim of identity theft, fraud, or worse. You can tell if the website you are using encrypts your information if the URL begins with "https:" vs. "http:" or if there is a lock icon in the bottom right corner of the screen.

Limit actions that may expose your PII. There are many small things that you can do to protect yourself from cyber attacks. For example, try to limit your visits to websites that store your password. If an attacker is able to access your computer, any private information stored on that website will be readily accessible. You should also limit your use of websites that store cookies. A cookie is a small data packet that is saved on your computer's hard disk by websites. Illegitimate websites may store cookies containing malicious code on your hard disk that could harm the files on your computer. Additionally, if an attacker has access to your computer, he/she can access the cookies and gain access to your browsing history and other private information.

Maintaining control of your PII, and other personal information entrusted to you at work, takes vigilance and dedication. As the Internet and online technologies continue to evolve, you are responsible for ensuring the information you handle remains safe by staying informed about cyber risks. Please visit the following websites to learn more about security and privacy.

- [HHS Center for New Media Blog: Online Privacy and Web 2.0 @ HHS](#)
- [NIH Office of the Senior Official for Privacy SharePoint Website](#)
- [NIH Office of the Chief Information Officer \(OCIO\)](#)
- [HHS Cybersecurity Program Website](#)
- [United States Computer Emergency Readiness Team \(US-CERT\) Cybersecurity Tips Page](#)

Feedback/Questions? Please contact the OSOP at: privacy@mail.nih.gov or (301) 451-3426.