Work Securely Everywhere

These small actions make a big difference, no matter where you do your work.

### Apply Updates

- **Set your software to update automatically** and reboot weekly. *Commonly used malware won't work on an up-to-date computer.*
- **Update the security settings** on your personal devices using [security.harvard.edu/personal-device-security-guides](http://security.harvard.edu/personal-device-security-guides).

### Use Strong Passwords

- **Create unique passwords** for:
  - **Home Wifi** - This password keeps people off your network, so don't get stuck using the default.
  - **Computer** - This password keeps your work private while you're away from the keyboard.
  - **Online services** like email and social media.

  *Too many passwords to remember? Let a password manager do the work for you. Get started at security.harvard.edu/LastPass.*

### Know Your Data

- **Connect to Harvard's VPN** while working. Like clicking your seatbelt before driving, connecting to VPN gives you peace of mind that:
  - No one can view or edit what you send to Harvard's Network.
  - World class security tools can detect suspicious activity.
  - Websites known to be used for cyber attacks are blocked.

### Click Wisely

- **Watch out for scams.** Phishing messages are designed to make you feel anxious, unsure, and reactive. *Trust your gut.* When something feels off, skip the link and go to the source.

  - **Sensational Headline?** Do a web search for the headline or go to a trusted news source directly.
  - **Urgent IT Alert?** Check your support website or contact support to confirm changes.
  - **Odd request from someone you know?** Call or text to verify the message is legit.

*Forward phishing emails to phishing@harvard.edu. Quick reporting from savvy people at Harvard has saved others in the past!*