

Don't let the FUD factor (Fear, Uncertainty, and Doubt) keep you from using and enjoying the world of technology.



1. Use a Password Manager

- Set up a Last Pass Account
- Add any websites that store personally identifiable information (i.e., address, credit cards, account numbers, etc.)
- Make sure all accounts have unique passwords and usernames (if optional)
- Enable multi-factor authentication if optional

Pro Tip: Run Last Pass' Security Challenge to analyze your security. This process will show you accounts that are at risk and will take you step-by-step through improving your passwords.



2. Protect Your Email

- Add your email to Last Pass—make sure the password is unique and strong
- Enable multi-factor authentication

If your email doesn't support multi-factor authentication, change email providers:

- Open a Gmail account
- Forward email from your previous, insecure account to your new Gmail account

Pro Tip: Create a separate email account for your critical financial accounts. Use this only for your bank and credit cards—nothing else. Make the email address generic e.g., mybank@gmail.com



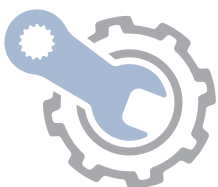
3. Monitor Your Accounts

- Sign up for Credit Karma
- Enable alerts for hard credit inquiries
- Log in monthly to check your credit scores

Pro Tip: Credit Karma will email you monthly—this is a good reminder to check your credit scores.

- Enable alerts and notifications on all your bank accounts and credit cards.

Pro Tip: If you use a personal financial manager (like Mint.com), you can use this to quickly summarize and verify your transactions weekly.



½ Auto-Update Devices

- Turn on auto-update for all devices that allow it
 - Computer/laptops
 - Tablets
 - Mobile phones
 - Routers