

Five ways to keep scammers and hackers away

By

Alvaro Puig
Consumer Education Specialist, FTC
August 23, 2024

We're living in the data age. The things we do on our phones and computers, on our internet-enabled smart devices, and on websites leave a trail of our activities and our personal information. That personal information has value — not just to us, but to scammers and hackers who want to steal our identities. Here are five things you can do to keep scammers and hackers at bay.

1. Secure your accounts so they're hard to crack. Use a strong password. And enable two-factor authentication (2FA) on sensitive accounts like your email or financial accounts. 2FA adds an extra layer of security by requiring a second form of verification.
2. Keep your security software, operating system and internet browsers and apps up to date to defend against the latest threats.
3. Your wireless network is the gateway to all the Wi-Fi enabled devices in your home. To protect your connected devices, replace the default Wi-Fi network password and router admin password with a strong password. And encrypt your network to prevent unauthorized access.
4. Set your computer and phone to lock when you're not using them. That'll prevent unauthorized access to your computer if you step away or to your phone if you lose it.
5. Create a backup copy of your information. That way you can recover it if your device gets infected, hacked, stolen, or lost. Back up your data to the cloud or an external drive.

Report scammers and hackers at [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft). If someone stole your personal information, report it, and get recovery steps, at [IdentityTheft.gov](https://www.ftc.gov/identity-theft).

