

# Your Green™ - Did you know?

## Protect Yourself from Identity Theft

### WiFi

When using public WiFi make sure it's an authenticated network. Avoid free networks with lookalike names. Make sure your mobile devices do not connect to WiFi automatically. Secure your home WiFi by making sure the router's encryption features are on.



### Credit cards

Jiggle card readers if you suspect a skimmer is on it. If it moves or seems loose, avoid using it. Avoid using debit cards - credit cards have greater protection against fraud.



### Cyber Security

Install up-to-date security software with firewall protection, anti-virus, and anti-malware programs. Create unique passwords at least 10-12 characters long and change often. Limit what you share on social media. Never log in or send personal information to unencrypted websites.

### Email Security

Never click an unknown link, even if you think you know the sender. Update your password often.

### Signs of Identity Theft

You may notice errors or unfamiliar transactions on your financial statements. Your credit report contains inquiries in response to applications you didn't make. Expected mail doesn't arrive. Medical records report a condition you don't have. You receive bills for transactions you didn't make.



### What to do

Immediately place an initial fraud alert on your files by contacting one of the three major US credit reporting agencies. Order a credit report and correct report errors. File a complaint online with the Federal Trade Commission at [ftccomplaintassistant.gov](http://ftccomplaintassistant.gov).