Ways to Fight ID Fraud Online

1. **Keep your computers and mobile devices up to date.** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
2. **Set strong passwords.** A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.
3. **Watch out for phishing scams.** Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from unfamiliar sources.
    a. Forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov – and to the company, bank or organization impersonated in the email.
4. **Keep personal information personal.** Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know.
5. **Secure your internet connection**. Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it. Consider using a Virtual Private Network (VPN) app to secure and encrypt your communications when connecting to a public Wi-Fi network. (See the Federal Trade Commission's tips for selecting a VPN app.)
6. **Be careful in the cloud.** While using the cloud makes it easier to store and share large amounts of files, understand that it also opens other avenues for attack.
7. **Shop safely.** Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with *https.* Also, check to see if a tiny locked padlock symbol appears on the page.
8. **Read the site's privacy policies.** Though long and complex, privacy policies tell you how the site protects the personal information it collects.
9. **Report any suspected fraud to your bank immediately.**