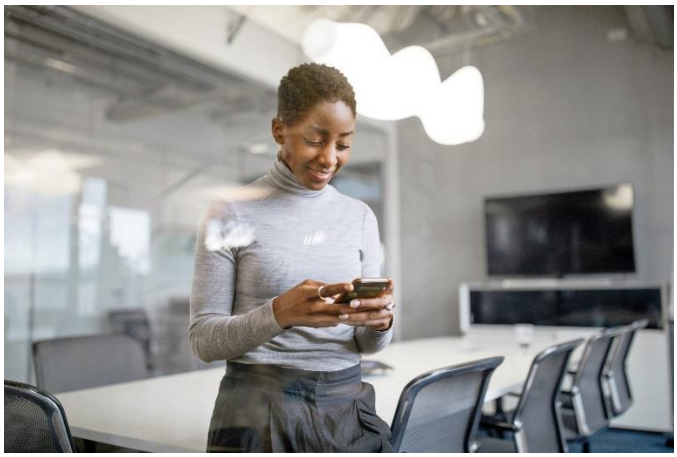
Defend Yourself Against Fraud



Help Defend Yourself Against Fraud with These Easy Tips

At ADP, protecting your security has been, and always will be, a top priority. We work to keep your data and funds safe by leveraging multi-layered protection and our advanced security intelligence platform. However, scammers are growing more sophisticated and are targeting you and your accounts through emails, texts, phone calls, and deepfake audios and videos. It's important that we partner to help prevent fraud and adopt best practices. It's critical that you are aware of the signs of fraud and these types of scams, and how you can help protect yourself.

4 tips to help you protect yourself:

1. **Don't get caught by social engineering threats**
    - Don't trust the display name that pops up in your email account – that is easily spoofed and scammers can make it say anything. Be cautious about trusted brands, logos, copyright and legal disclaimers.
    - Look but don't click on links – hover your mouse over a hyperlink to see exactly where it will take you.
    - Don't click on links or attachments, in emails or text messages.
    - If something seems suspicious, be extra vigilant – would the CEO of your company really ask you to transfer money, especially in a communication channel you don't normally use or that is not approved by your company? Ask yourself (and then validate) if the request makes sense before acting.

Copyright © 2026 ADP, Inc.

2. **Don't give out personal information to strangers**
    - ADP will never ask for your account information, SSN, pin or password over the phone or through email. Most other companies that collect sensitive information follow similar practices, so be extra careful when someone is asking.
    - Double check the requestor and phone number provided in a message is valid through a known source. The best way to do this is to go directly to the company's website and get the information independently or through known contact information you already have.

3. **Keep passwords safe**
    - When creating your own passwords, make them easy for you to remember, but hard for others to guess. It's best to use a passphrase that is personal to you - like your favorite song lyrics or line from a poem – and use symbols and numbers.
    - Don't reuse your password across accounts. Scammers use stolen passwords and assume that they can use them on other accounts too – and they are often right!

4. **Manage your social settings**
    - Set your privacy settings on social media accounts to the strongest that the system allows. Scammers can utilize publicly available information to find common answers to security questions – like your birthday, place of birth, and mother's maiden name.
    - Make sure that you know who you are connecting with. On most sites, once you connect with someone, you are giving those connections more access to your information. If you see or suspect something suspicious, make sure to report it to the site.

Copyright © 2026 ADP, Inc.