Dodge the Scam

Easy tips to protect yourself against fraud

At ADP®, protecting your security has been, and always will be, a top priority. We help to keep your data and funds safe by leveraging multi-layered protection and our advanced security intelligence platform.

Scammers are growing more sophisticated and are targeting you and your accounts through emails, texts and phone calls. Fraudsters are constantly changing their tactics to find better ways to steal personal and business information and money. We're working hard to protect your data, but your participation in security and privacy are essential. It is critical that you are aware of the signs of these scams and how you can help protect yourself.

Don't get caught by a "phish" hook

Don't believe everything you see: 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. Scammers know that you are looking for these items and try to replicate them.

- Look but don't click – hover your mouse over a hyperlink to see exactly where it will take you.
- If an email seems suspicious, do not click on any of the links or open any attachments in the email. If you do, your computer can become infected with malware.
- Let us know right away if you receive a suspicious email that looks like it is coming from ADP. Forward the original email you received as an attachment or a screenshot of the text message to abuse@adp.com.
- When you visit a website, beware of pop-up messages that prompt you to take an action immediately, including updating your computer.

You can get our ADP phishing alerts emailed to you by visiting our website: **adp.com/about-adp/data-security/alerts.aspx** ("Don't Miss a Thing" section on the right side).

Don't give out personal information to strangers

- ADP will not request sensitive personal information such as Social Security Numbers, login credentials, or bank or credit card information via unsolicited phone, email, or internet-based communications. If this information is ever requested in a communication that you did not initiate, it's an indicator of a scam.
- Double check that any phone number or link provided to you in a text or email is valid before clicking on it or calling it. The best way to do this is to go directly to the company's website and get the information independently.

Keep safe passwords

- 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!
- Use a reputable password manager to electronically store very complex and unique passwords for each of your accounts

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
- Once you connect with someone on most sites, you are giving those connections more access to your information. Make sure that you know who you are connecting with and that if you see or suspect something suspicious to report it to the site.

If you suspect fraud, contact your ADP representative immediately.
We hope this information helps you and your business to be more secure.
For more information about Security at ADP, visit **adp.com/trust**

Always Designing for People™