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 and phone calls. It is critical that you are aware of the signs of these scams and how you can help protect yourself.

4 tips to help you protect yourself:

1. **Don't get caught by a "phish" hook**

Don't believe everything you see. Scammers know that email is one of the most commonly utilized communications tools and they use that to their advantage.

- 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 – hover your mouse over a hyperlink to see exactly where it will take you.
- Don't click on links or attachments.
- If it smells "phishy" be extra vigilant – would the CEO of your company really ask you to transfer money? Would your boss really ask for a download of payroll information be sent externally? Ask yourself (and then validate) if the request makes sense before acting.

Sign up for ADP's Security Updates to receive real-time information about common phishing scams that target ADP clients and their employees.

2. **Don't give out personal information to strangers**

   - ADP will never ask for your account information, SSN, paycard information, 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 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.

3. **Keep passwords safe**

   - Use a reputable password manager to electronically store very complex and unique passwords for each of your accounts.
   - When creating your own passwords, make them easy for you to remember, but hard for others to guess. Its best to use a phrase that is personal to you -like your favorite song lyrics or line from a poem - and then substitute the letters for characters. Then, add in the account that you are using it for.
     - For example, Tw!nk[eTw!nk[e[!ttle$tarAmazon or Tw!nk[eTw!nk[e[!ttle$tarEbay
   - 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**

   a. 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.

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

For more information on ADP's commitment to data security, click here.

Always Designing
for People™