DOs & DON'Ts to Help Keep Your Business Credentials Secure

ADP A more human resource.

Protect Passwords

Do

Create long and strong passwords by using a phrase you can remember and only you will know. Add numbers and special characters to make it complex.

Change your password frequently–at least every 3 months.

Don't

Don't use the same password for all of your accounts. If it is hard to remember different passwords, create a base password that is easy to remember, like *Mydaughteramyis5!* then add the name of the website to the end of it for each of your different accounts, like *Mydaugtheramyis5!amazon*.

Don't share an account or password with someone else, all employees should have their own usernames and passwords.

Beware of Phishing

Do

Enable Domain Message Authentication Reporting and Compliance (DMARC), an email authentication protocol that can be used to determine whether an email was actually sent by ADP or one of our trusted partners. ADP utilizes DMARC, but your receiving email server must also be configured to check DMARC to block forged messages.

When inspecting links contained in emails, always hover over the link so that you can see where the link is taking you. Ensure that the web address that appears is the one you are expecting to go to.

Check to see if the link is routing you to a website that begins with https://. The "s" stands for secure and usually means that websites have taken security measures to protect users.

Don't

If an email seems suspicious, do not click on any links or open any attachments in the message. They may contain malware which could infect your computer or steal your credentials. Be suspicious of messages that:

- Seem urgent and require your immediate response. Do not call the number given in the message or respond to the message.
- Require personal information such as user ID, password, PIN, email address, Social Security number, or other logon credentials, even if it appears to be coming from a legitimate source. Remember that legitimate organizations, like ADP, will not require this type of sensitive personal information via unsolicited email, phone or internet-based communications.
- Are addressed generically, such as "Dear Customer."

If you receive a suspicious email that appears to come from ADP, don't click on any links or open any attachments and forward it as an attachment to abuse@adp.com. Then delete the email.

Combat Malware and Viruses

Do

Install anti-virus and anti-spyware programs from reputable sources and keep them up-to-date.

Keep all applications on your computer current with the latest releases.

Process payroll using a dedicated computer that is not used for any potentially non-secure purposes.

Always enable pop-up blockers on your internet browser.

Don't

Do not download anything in response to a warning you receive from a program you did not install or do not recognize.

Never disable your firewall.

Safeguard

- Only provide confidential information when you are sure of a person's identity.
- Be sure you are sending data securely or encrypted.
- Review the data you are about to send to be sure it includes only necessary information and nothing extra.
- Double check the address or distribution list that you are sending data to before you send it.

Educate

- Have security and privacy policies in place that clearly define employee responsibilities.
- Offer security and privacy training (make it mandatory) so that employees can help detect and prevent security threats.
- Instruct employees if something is suspicious or they witness a security incident to report it to your IT or security team.

Monitor

- Set up workflow notifications within your ADP product, if available, to alert you to account requests or changes and require review or approval to proceed.
- If available within your ADP product, enable banking protections, like Prenote, for direct deposits to verify the accuracy of account data, such as routing numbers and account numbers.

The information contained above is for information purposes only. The recommendations contained in this document are not intended to cover all possible steps to take to secure business credentials. Following these recommendations does not guarantee that your security will not be compromised.