IN THE BUSINESS OF YOUR SUCCESS®

Fraudulent Emails Appearing to Come from ADP®

1. Was my information compromised?
We have no reasonable evidence or suspicion to believe that your personal information was compromised. In addition, we have no reasonable evidence or suspicion to believe that ADP® has been compromised. Please note that these fraudulent emails are not originating from ADP.

2. How did they obtain my email address?
There are many ways to obtain email addresses; for example, collecting email ID's from email harvesters (hackers who sell email ID's), from social networking sites and email address generation software.

Please note that these phishing attacks have hit many people who are not ADP clients, these attacks are random in nature and are not targeted specifically at ADP clients.

3. What is ADP doing to stop these phishing emails?
ADP is actively working with our security vendors and fraud prevention team to identify and contain the source of the incidents. We are also working closely with law enforcement agencies.

In addition, ADP utilizes Domain-based Message Authentication, Reporting & Conformance (DMARC) for its email systems in an effort to help protect the ADP brand and assist our clients in their defense from advanced phishing attacks and fraudulent emails. DMARC is a public open standard to help prevent the forgery of sender domains and addresses. In order for organizations to take advantage of ADP's DMARC record, they must implement specific anti-spam or anti-phishing products that support this framework. This is usually in the form of software or hardware email gateways and/or vendor supplied cloud-based services. These applications and/or devices utilize DMARC to identify and reduce the number of spam and fraudulent emails an organization receives. The individual user receiving the email does nothing to configure or install DMARC.

The record is published in the Domain Name System (DNS), which is commonly known as the "internet phonebook." Organizations receiving emails can validate that the received email passes Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) standards, which DMARC leverages to authenticate an email's sender.

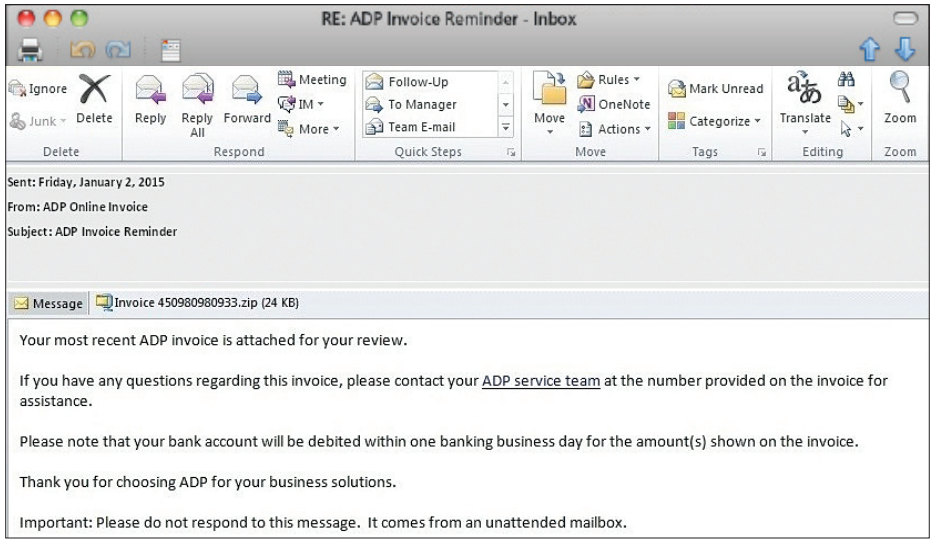
The ADP.com DMARC record is reliable, and directs receivers to reject non-matching email, the most stringent and effective response. Receiving systems may take this action with high confidence that legitimate ADP.com email will not be blocked.

Organizations that are capable of leveraging DMARC can significantly reduce the amount of spam, phishing, and fraudulent emails purporting to be from ADP that reaches individual user mailboxes. For more technical information regarding DMARC implementation in your organization, please refer your email server administrator to: www.dmarc.org.

4. How do I report an incident?
Please be on alert for fraudulent emails. If you receive a suspicious email:

- Do not click on any links or open any attachments within the message.
- Forward the email as an attachment to abuse@adp.com.
- Delete the email.

Please see one example of a fraudulent email below.



Protecting Yourself Against Phishing

Organizations should take several proactive safety measures to protect themselves against phishing and other forms of fraud which originate by means of electronic communications.

There are several different techniques to combat phishing, including training and technologies which are created specifically to protect against phishing. Organizations should consider updating their email filtering software and internet security suites as soon as possible, since these technologies are designed to handle the changing face of cybercrime. Some best practices to combat phishing include:

- Be suspicious of messages that:
  - Seem urgent and require your immediate response.
  - Request personal information such as user ID, password, PIN, email address, or Social Security number, even if it appears to be coming from a legitimate source.
  - Are addressed generically, such as "Dear Customer."
- If an email seems suspicious, do not click on any of the links or open any attachments. These links and attachments may contain malware which could infect your computer.
- Even if it sounds legitimate, do not call the number given in the message or respond to the message. Remember: Legitimate companies that have your sensitive data will not send emails or call you to ask for that data.
- If you have questions about an email that you received, please review ADP's security alerts which are posted on the ADP Trust Center at www.adp.com/trust.
- Always report suspicious emails and/or phone calls to ADP at abuse@adp.com.

Minimize the Risk of Computer Viruses and Malware

Computer viruses and malware can cause serious security issues for you and your company. Please read the tips below to protect your computer from viruses and malware:

- Process payroll using a dedicated computer that is not used for any potentially non-secure purposes.
- Keep your anti-virus software up-to-date at all times.
- Install anti-virus and anti-spyware programs from reputable sources.
- Do not download anything in response to a warning you receive from a program you did not install or do not recognize.
- Always keep software and applications on your computer up-to-date.
  - Cybercriminals are constantly inventing new and improved techniques to exploit vulnerabilities in software installed on your computer.
- Make sure that pop-up blockers are always enabled on your internet browser.
- Never disable your firewall.
  - A firewall places a protective block between your computer and the internet.
- Do not open email from people you do not know, and be sure that you can verify the source before opening attachments or clicking links in any email, IM, or posts on social networks.
  - Spam and phishing messages are one of the most popular ways cybercriminals deliver malicious content to users by tricking them to open attachments or clicking on links.
  - Disable auto-preview and automatic download settings in your e-mail system.

For more information regarding how ADP protects our clients' information and how clients can protect their personal information, please visit the ADP Trust Center at www.ADP.com/trust.

The ADP Logo, ADP and In the Business of Your Success are registered trademarks of ADP, LLC.
All other trademarks and service marks are the property of their respective owners.
04-3728-015 Printed in the USA Copyright © 2015 ADP, LLC. ALL RIGHTS RESERVED.

IN THE BUSINESS OF YOUR SUCCESS®