

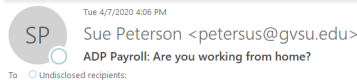
Date: Wednesday, April 8, 2020
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP Payroll: Are you working from home?"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: Sue Peterson petersus<AT>gvsu[.]edu with the following subject line: "ADP Payroll: Are you working from home?".

Message Sender:
Sue Peterson petersus<AT>gvsu[.]edu

Message Subject:
ADP Payroll: Are you working from home?

These emails do not originate from ADP and our analysis has revealed that they may contain malicious content. We're working with our fraud prevention team and anti-phishing vendor to address this incident. Please see the example below which may vary in content and sender.



SP Tue 4/7/2020 4:06 PM
Sue Peterson <petersus@gvsu.edu>
ADP Payroll: Are you working from home?
To Undisclosed recipients:

Providing effortless and accurate payroll and human resources management is ADP's priority under any given circumstances. Following the current lockdown in many states of America due to the Covid-19 we have put in place measures to process payroll and manage human resources without any interruption.

Please let us know below if employees in your organization are working from home as a result of the current situation in order to provide you with information needed as to process payroll from home.

If you process payroll from home please click below:

https://workforcenow.adp.com/adplearning/workfromhome_id=oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503

(If the link didn't work please copy and paste it on your browser)

If you are not working from home please see below for few things to keep in mind:

<http://mmz-servis.by/wordpress/wp-content/>

To avoid interruptions all ADP Workforcenow practitioners must keep to the given instructions.

AUTOMATED DATA PROCESSING

How to Report a Phishing Email

Be alert for this fraudulent email and follow the instructions below if you receive any 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, then delete it.
- If you clicked any link or opened an attachment in the email, immediately contact your IT support.

The ADP Global Security Organization continues to actively monitor this situation. Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.