Malicious Email Warning

We believe that the Entertainment Industry Flex Plan and Entertainment Industry 401(k) Plans did NOT suffer a data breach.

IF YOU RECEIVE AN EMAIL THAT CONTAINS A ZIP FILE, DELETE THE EMAIL AND DO NOT OPEN THE ZIP FILE. If you clicked on the .ZIP file, please see below.

How to tell if you received a legitimate email:

- Emails from the Flex Plan and 401(k) Plan will only come from noreply@flexplan.com and noreply@entind-401kplan.com
- The emails in question did not come from noreply@flexplan.com or noreply@entind-401kplan.com
- You will never receive an email with a .ZIP attachment from us, and most of our emails do not contain attachments.
- We will never provide a password with a document in the same email.
- The emails that members shared with us were not sent from noreply@flexplan.com or noreply@entind-401kplan.com
- We do not include Social Security Numbers, dates of birth, or protected health information in emails. Any protected information could only be accessed through a link (not an attachment) and is password protected with a PIN.
- If you are ever unsure about a message from us, please call our Member Services Department before opening the message.

Additional Information if you clicked on the .ZIP file attachment of a malicious email

Our Security Consultants have reviewed the phishing emails and determined the following:

- The malware tries to connect to a website; however, the website has been down/unavailable
- Windows Defender is sufficient in deleting the malware on Windows
- The malware was tested and did not run on a MAC

Please delete the suspicious email and do not click on the attachment.

Always be careful when clicking on attachments, especially .ZIP files. Please do not open a .ZIP file unless you are expecting it. It is always a good idea to contact the

sender before opening a .ZIP file to ensure it is legitimate. The Flex Plan and 401(k) Plan will never send an email with an attachment or a .ZIP file.

If you clicked on the attachment in the phishing email, here are some recommendations by Operating System:

Windows:

Run a system scan using Microsoft's built-in Microsoft Defender Antivirus application

- Open file explorer (hold down the Windows Key and press "E")
- When the file explorer window opens up on the left pane
    - Right-click on "Local Disk (C:)" and then
    - Click on: Scan with Windows Defender

MAC:

- Delete the file that may have been created if you clicked on the link in the phishing email; the file will most likely be in your downloads folder.
- The virus does not run on a MAC.