Fraudulent Emails Copy TWC's Graphics

Date: December 27, 2021

The Texas Workforce Commission (TWC) warns those filing for Unemployment Benefits about fraudulent emails pretending to be from TWC. The email provides a link to a webpage that copies the appearance of TWC's Unemployment Benefit Services (UBS) online system and attempts to get personal information from the customer. Unfortunately, these fraudsters are using TWC's graphics to make their emails and website appear to be legitimate.

TWC is reminding all customers to practice caution when providing personally identifiable information. Scammers often say there is a problem with your account, and you need to verify information to solve the issue. Instead of clicking a link or calling a phone number provided in an email, go to the website you know is trustworthy. If in doubt, please call 800-939-6631 for assistance. We are here to serve you.

Below are some indications that will help you identify when an email and website are an attempted scam by someone pretending to be from TWC.

- Although the link in the email shows that it goes to "twc.texas.gov" it does not. Instead, the link goes to "texas.twc.online.onlinebeaupros.com." or another non *.gov or *.state.tx.us website. A common trick used by scammers is to display a legitimate web or email address but once you select the link, you are taken to a different address. **Make sure you check the URL, which is the address shown at the top of the page, to verify you are on the correct page.**
    - You can hover your cursor over a link to show the URL address. If you select the link, make sure to look at the address shown at the top of the web page.
    - The website linked from the email example shown below **is not a legitimate TWC page.**
- The fraudulent logon page is made to look like TWC's UBS system, but the page asks for nine (9) pieces of personal information for you to log on.
    - To log in to TWC's UBS application, you only need to enter your User ID and password. Once you are logged on, UBS displays your name and the last 4 digits of your Social Security number. **TWC does not ask you to reenter all your personally identifying information to log on.**
    - The correct URL for UBS is https://apps.twc.state.tx.us/UBS/security/logon.do or https://apps.twc.texas.gov/UBS/security/logon.do.
- The fraudulent logon page asks for your Personal Identification Number (PIN).
    - **TWC staff will never ask for your PIN.**
    - **The UBS application never requests your PIN to log on.** UBS will request your PIN only when you change your payment method or your address after you've successfully logged on.
- The fraudulent logon page asks for your email address and the password used for your email.
    - **TWC will never ask you to provide the password used on another website or application.**

Image of Fraudulent Email

The email looks like it comes from GovDelivery. While it's correct that TWC uses GovDelivery to send emails, this message did not come from TWC. The link provided in the email does not go to TWC's official page (twc.texas.gov).

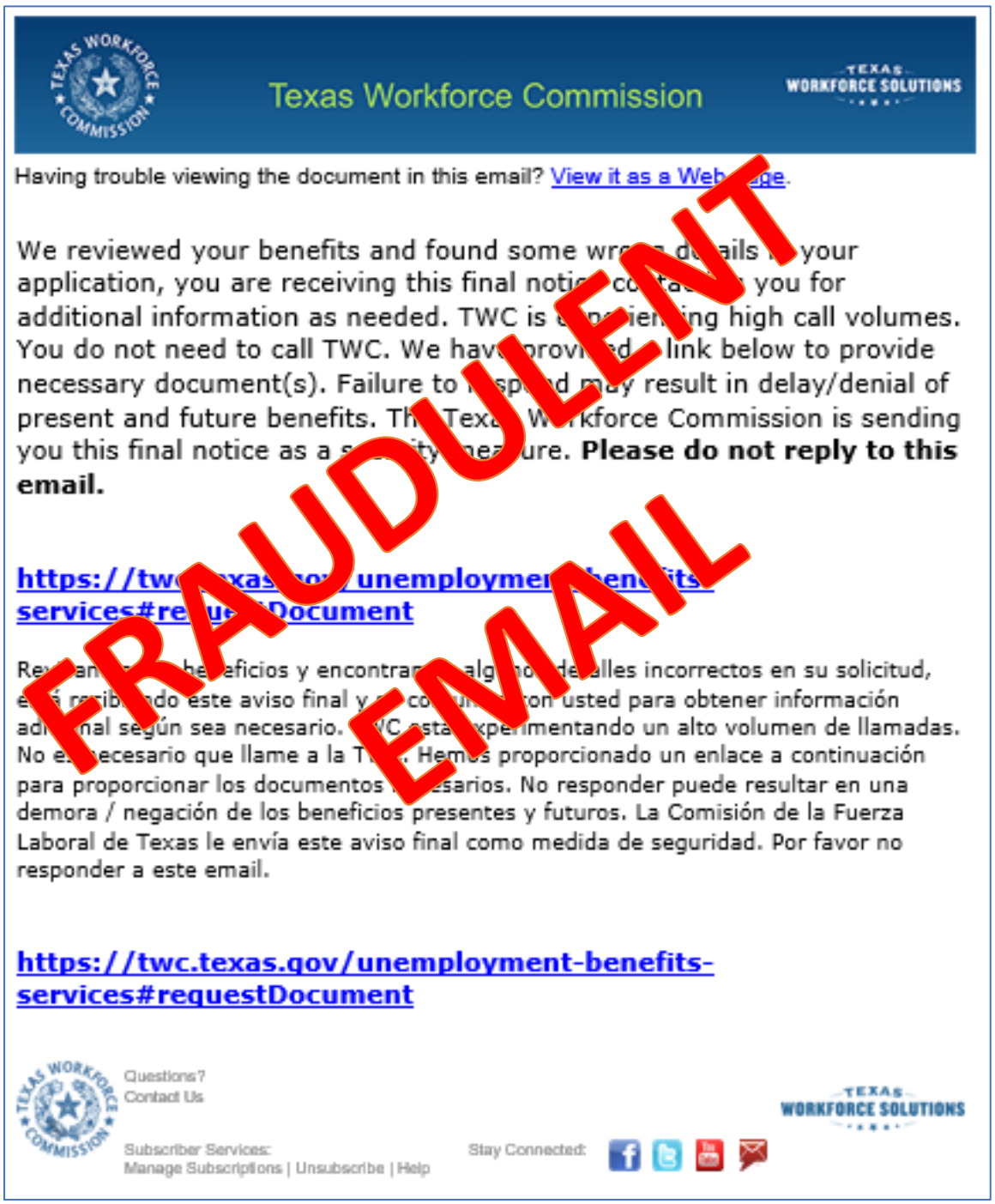

Image of Fraudulent Website

The link in the email goes to a page that looks like TWC's UBS application, but it is not. Notice the address at the top is different than the UBS system, and the page asks for multiple pieces of identifying information simply to log on.