Having trouble viewing this email? View it as a Web page.

Your unemployment benefits account can easily be compromised by clicking on a phishing link, or going to the wrong web address for TWC, and giving your confidential information or answering questions that give details a hacker can use to figure out your login information.

You should always check the website's address (called a URL) before logging in or entering information. The URL should be at the top of your browser. You might have to click the address bar in your browser to view the full URL. Instead of clicking a link, type the address directly into the address bar, or by using a trusted search engine, or use a bookmark that you are sure is correct.

- TWC's Unemployment Benefit Services (UBS) address is https://apps.twc.texas.gov/UBS/security/logon.do.
- TWC's home page address is https://www.twc.texas.gov/
    - As you visit other pages on TWC's website, the name of the new page is included in the address. Example: TWC's Scams page is https://twc.texas.gov/services/report-fraud/avoid-scams-schemes.

IMPORTANT: TWC staff will never ask for your password, PIN, bank account number, credit or debit card number, answers to your security questions, or anything else that is used to log in to your account.

When creating a PIN, use a unique number. Do not use part of your SSN, address, birthday, or other personal information for a PIN or as part of a password.

Cybercriminals are increasingly tricky and successful at getting past spam filters and virus detection systems with phishing attacks. Scammers can mimic the look of official TWC correspondence and even create fake web pages that look exactly like TWC's Unemployment Benefit Services (UBS) web application.

TWC was recently notified of a scammer webpage "twc-texas.net" that mimics TWC's unemployment benefits log on screen. Even though it looks like UBS, it is a fake. Our web pages do not end in .net and we do not ask for the PIN to log on. After entering their confidential information into the fake website, the scammer webpage forward customers to the real TWC webpage, so customers do not realize their log on information has been compromised.

If you receive an email or text that appears to be from TWC, **DO NOT CLICK LINKS OR OPEN ATTACHMENTS**. Instead, go to TWC's website by typing the address or using a trusted search engine such as Google or Bing to search for "Texas Workforce Commission."

Want to Verify this Email Came from TWC? Go to the TWC website and search for "Scams." We added a copy to our Scams and Schemes page.