LABOR RELATIONS

UNITED STATES POSTAL SERVICE

December 30, 2022

Mr. Ivan D. Butts
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Dear Ivan:

This is in further reference to the correspondence dated December 22, where you were notified that the United States Postal Inspection Service, Office of Inspector General, and Corporate Information Security Office (CISO) have discovered fake LiteBlue websites that closely resemble LiteBlue. The website may feature an address ("URL") that is similar to the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org."" Upon accessing fake sites, cyber criminals will capture your employee identification number and password and may even forward you to our correct site.

As an additional precaution, the Net to Bank and Allotment functionalities have been disabled online in the PostalEASE application accessed externally through LiteBlue via a personal computer as of December 29 until further notice.

Employees may cancel allotments, establish net to bank, or make changes to net to bank via the PostalEASE Interactive Voice Response (IVR) system. IVR is a telephone-based system and may be accessed by calling the Human Resources Shared Service Center (HRSSC) at 877-477-3273, menu option 1. Employees using the IVR system will need to have their employee identification number (EIN) and personal identification number (PIN).

These services can be conducted online via PostalEASE when accessed using a USPS-owned laptop or desktop computer, connected to the USPS network.

The LiteBlue and PostalEASE applications have not been compromised. A limited number of employees have reported unusual account activity involving their PostalEASE accounts, which has been attributed to their prior interaction with the fake LiteBlue websites.

Enclosed is a stand-up talk concerning the information above.

Please contact Bruce Nicholson at extension 7773 if you have questions concerning this matter.

Sincerely,

James Lloyd
Director (A)
Labor Relations Policies and Programs

Enclosure

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4100
WWW.USPS.COM

LRPP 2022-225

Mandatory Stand-Up Talk

Dec. 30, 2022

Fraud Alert Update:
Net to Bank and Allotment Disabled Online in PostalEASE

The stand-up talk issued Friday Dec. 23, 2022, discussed a fraud scheme by cyber criminals using fake LiteBlue websites to target Postal Service employees.

When you attempt to log in to a fake site, scammers collect your username and password. Scammers can record this information and use it to enter PostalEASE — the self-service application reached through LiteBlue for employment-related services. There, scammers may access your sensitive data, which they can manipulate for financial gain.

The LiteBlue and PostalEASE applications have not been compromised. A limited number of employees have reported unusual account activity involving their PostalEASE accounts, which has been attributed to their prior interaction with the fake LiteBlue websites.

As an additional precaution, the Net to Bank and Allotment functionalities have been disabled online in the PostalEASE application accessed externally through LiteBlue via a personal computer as of Dec. 29, 2022, until further notice.

Employees may cancel allotments, establish net to bank, or make changes to net to bank via the PostalEASE Interactive Voice Response (IVR) system. IVR is a telephone-based system and may be accessed by calling the Human Resources Shared Service Center (HRSSC) at 877-477-3273, menu option 1. Employees using the IVR system will need to have their employee identification number (EIN) and personal identification number (PIN).

These services can be conducted online via PostalEASE when accessed using a USPS-owned laptop or desktop computer, connected to the USPS network.

If you use an online search engine such as Google or Yahoo to navigate to LiteBlue, you may find fake LiteBlue websites in your search results. We are working with the internet service providers to remove the fake websites. However, they often reappear as quickly as they are removed.

You can reduce the chances of encountering a fake website by navigating directly to the official USPS website at *(spell aloud)* W-W-W - "dot" - L-I-T-E-B-L-U-E - "dot" - U-S-P-S - "dot" - G-O-V or www.liteblue.usps.gov. If you visit LiteBlue frequently, you should bookmark the site as one of your favorites.

We are also taking additional precautions across our network to mitigate the risk of further impact on our employees.

If you suspect you are a victim of this fraud or encounter a fake LiteBlue website, please contact USPS CyberSafe by email at *cybersafe@usps.gov*. Employees should also report any instance of suspected account tampering to the USPS Accounting Service Center helpline at 1-866-974-2733.

Thank you for listening.

###