UNITED STATES
POSTAL SERVICE

ALL EMPLOYEES

SUBJECT: Multifactor Authentication for LiteBlue

Cyber criminals continue to pose a threat to postal employees by creating fake websites that closely resemble LiteBlue. These bad actors leverage these fraudulent websites to capture employee identification numbers and passwords, which can be used to access personal information housed within PostalEASE, including direct deposit and other payroll information. These fake websites feature an address ("URL") that resembles the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org".

Over the last few weeks, the Postal Service has taken steps to educate you of the threats that cyber criminals pose and what you can do to protect yourself along with technology changes to enhance our existing security protocols. These steps include a targeted awareness communication campaign to include a letter sent to all employees' address of record and distribution of two required stand uptalks. We implemented email notifications to employees when changes have been made to their net-to-bank and allotment accounts and provided instructions to employees on how to set up this functionality.

Multifactor authentication (MFA) is an additional tool available to prevent cyberattacks and will provide additional protection for our employees and their personal information. MFA is a verification method requiring users to provide their username and password and an additional factor (authenticator app, one time passcode) prior to being allowed access to an application.

On Sunday, January 15, the organization is deploying the MFA solution for LiteBlue as an additional security measure to protect employees' IDs, passwords, and other personal data from unauthorized access and misuse. At this time, you are required to sign up for MFA in to obtain access to LiteBlue. As a part of the MFA implementation, there are a few steps employees must complete. These steps include:

1. Reset your Self-Service Profile (SSP) password.
2. Verify answers to security questions.
3. Verify the last four digits of your Social Security Number (new security enhancement).
4. Establish MFA preferences.

As a part of our plans to mitigate the risk of continued attacks, transactions of net-to-bank and allotments were temporarily disabled for all employees; as MFA is successfully deployed, this functionality will be re-activated.

For information on setting up MFA or to view support materials, please visit the Multifactor Authentication page via the QR code below.

Jennifer D Utterback

Jennifer D. Utterback
Vice President
Organization Development

Heather L Dyer

Heather L. Dyer
Vice President
Chief Information Security Officer