

DEC 27 2022

LABOR RELATIONS



December 23, 2022

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

Dear Ivan:

As a matter of general interest, 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 a safety measure, the Postal Service has recently implemented a new email notification that will notify you of changes via your personal email address on record. Instructions are included outlining how you can access Employee Self-Service to update your personal contact information – including the email address and phone number you have on file with the agency.

Enclosed are letters that will be sent to all employees concerning the potential risk, letters that will be sent to impacted employees, and an enclosure that will be included with both letters. Also enclosed is a Stand-up Talk (SUT) on the issue which will be given to all employees.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "James Lloyd".

James Lloyd
Director (A)
Labor Relations Policies and Programs

Enclosures

Fraud Alert: Cyber criminals defrauding Postal Service employees using fake LiteBlue websites

Securing the privacy of your personal data is a shared priority between you and the Postal Service. Your private information stored online is a target for criminals who seek to compromise this data for their financial gain.

We have become aware of a fraud scheme by cyber criminals using fake USPS LiteBlue websites to target USPS employees. These websites appear as near-exact replicas of the official LiteBlue website. Some sites use web addresses, or URLs, that substitute spelling variations of "Lite" or "Blue" in place of the correct website address.

Scammers use these fake websites to collect employee usernames and passwords – or "credentials". When you attempt to log in to a fake site, the scammer records your credentials. They can use this information to enter PostalEASE – the self-service web application accessed through LiteBlue, that provides you access to employment-related services. There, scammers may access your sensitive data, which they manipulate and leverage for their 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 mimicked LiteBlue websites.

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

You can reduce the possibility of compromise by navigating directly to the website at (*spell out-loud*) W-W-W - "." - L-I-T-E-B-L-U-E - "." - G-O-V. If you visit LiteBlue frequently, you should bookmark the site as one of your favorites.

We are assisting employees affected by this fraud and providing them with credit monitoring services. We are also taking additional precautions across our network to mitigate the risk of further impact to our employees.

The Postal Service's Corporate Information Security Office, Office of Inspector General, and Postal Inspection Service are investigating this matter.

If you suspect you are a victim of this fraud, or if you encounter a fake LiteBlue website, please contact cybersafe at cybersafe@usps.gov

Mandatory Stand-Up Talk

Dec. XX, 2022

Fraud Alert:

Be on the lookout for fake LiteBlue websites

Securing the privacy of your personal data is a shared priority for you and the Postal Service. Any private information stored online is a potential target for criminals.

We have become aware of a fraud scheme by cyber criminals using fake USPS LiteBlue websites to target Postal Service employees.

These websites appear as near-exact replicas of the official LiteBlue website. Some sites use web addresses, with spelling variations of "Lite" or "Blue" instead of the correct website address.

Scammers use these fake websites to collect usernames and passwords. When you attempt to log in to a fake site, the scammer records your information. They can use this 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 their own 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 faked LiteBlue websites.

If you use a search engine such as Google or Yahoo to navigate to LiteBlue, you may find the fake 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 going to a fake site by navigating directly to the official USPS website at (*spell aloud*) W-W-W - "dot" - L-I-T-E-B-L-U-E - "dot" - G-O-V. If you visit LiteBlue frequently, you should bookmark the site as one of your favorites.

We are assisting employees affected by this fraud and providing them with credit monitoring services. We are also taking additional precautions across our network to mitigate the risk of further impact to our employees.

The Postal Service's Corporate Information Security Office, Office of Inspector General, and Postal Inspection Service are investigating this matter.

If you suspect you are a victim of this fraud, or if you encounter a fake LiteBlue website, please contact CyberSafe by email at cybersafe@usps.gov.

Thank you for listening.

###

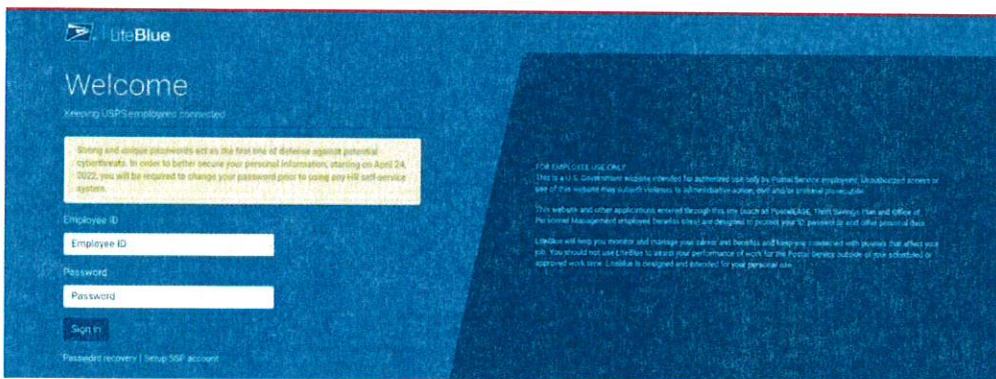
Keeping Your Private Information Secure

Example of the legitimate LiteBlue login site (www.liteblue.usps.gov)



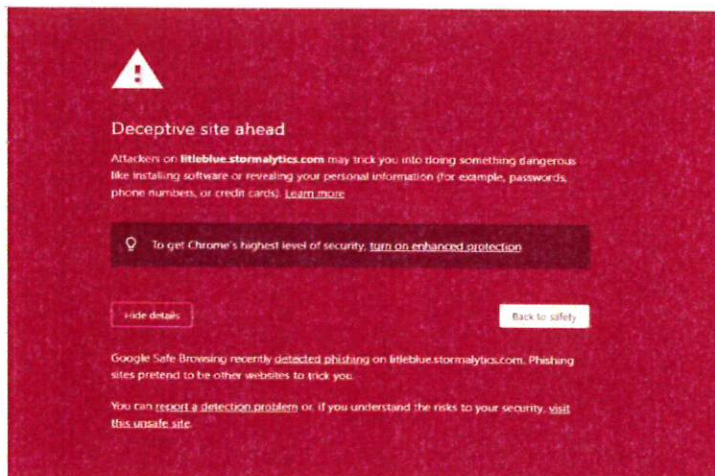
Notice: The web pages appear the same

Example of a spoofed LiteBlue login site ([www.\[litelbue-secure\].com](http://www.[litelbue-secure].com))



The only difference is the address in the web browser


If you see a Deceptive Site Warning as shown below DO NOT proceed



Updating Your Preferred Email Address

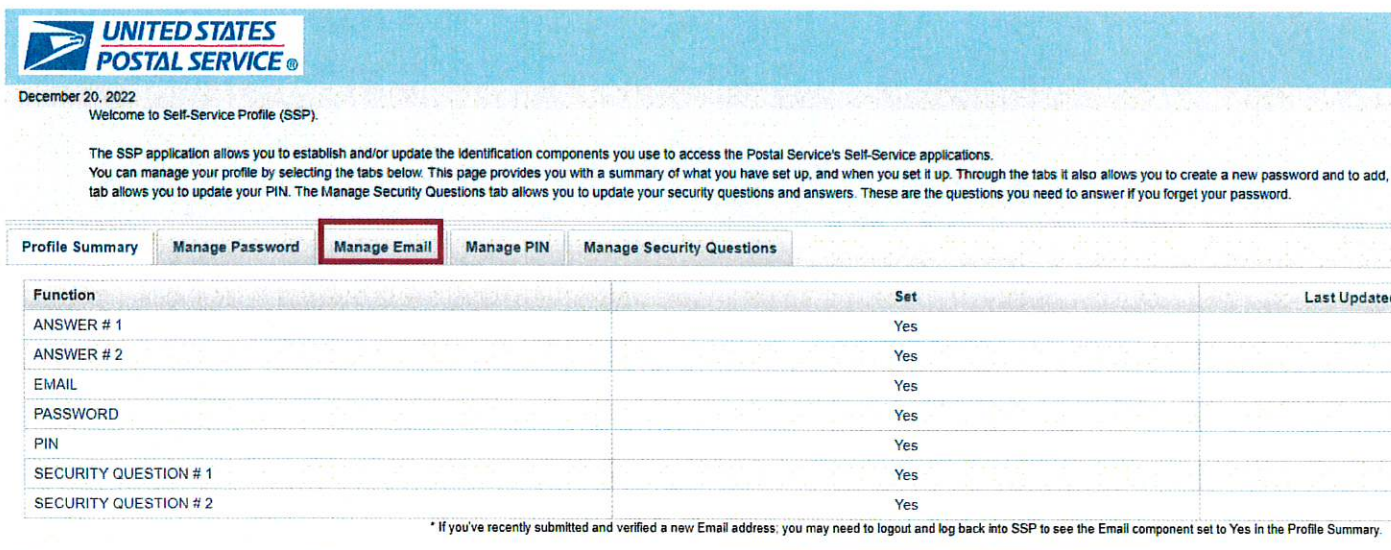
Log in to LiteBlue.usps.gov

- On any computer or smart device, navigate to LiteBlue at liteblue.usps.gov
- Select **Setup SSP account** under the sign-in button
- Select **Enter SSP** and login with your Employee ID and Password



Enter preferred email address

- Select **Manage Email** tab and enter preferred email address



Function	Set	Last Updated
ANSWER # 1	Yes	
ANSWER # 2	Yes	
EMAIL	Yes	
PASSWORD	Yes	
PIN	Yes	
SECURITY QUESTION # 1	Yes	
SECURITY QUESTION # 2	Yes	

Your new email address will require verification. Please follow the steps in the email to successfully update your email address on file.

December xx, 2022

ALL EMPLOYEES

SUBJECT: Keep your private information secure

Maintaining the privacy of your personal data is a shared priority for you and the Postal Service. Your private information stored online is a target for criminals who seek to compromise this data for their financial gain.

Cyber criminals continue to be a threat by creating fake websites that closely resemble LiteBlue. These fake websites may feature an address ("URL") that is similar to the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org", see the included handout ("Keeping Your Private Information Secure"). These fake websites may even forward you to the actual LiteBlue website once you enter your credentials. If you access one of the fake websites that closely resemble LiteBlue, cyber criminals can capture your employee identification number and password, which they can use to access your personal information housed within PostalEASE, including your direct deposit and other payroll information.

As an additional safety measure, the Postal Service has recently implemented a new email notification that will notify you of changes via your personal email address on file with the Postal Service. Instructions are in the included handout ("Updating Your Preferred Email Address"), outlining how you can access Employee Self-Service to update your personal contact information, including the email address and phone number that you have on file with the Postal Service.

Additional measures you can take to keep your account information safe:

- Do not share login credentials with others, including managers, co-workers, and outside entities.
- Keep your Employee Identification Number (EIN) confidential.
- Connect to USPS applications using secure connections that avoid public Wi-Fi or public computers.
- Any time you login to LiteBlue, check your account for any unusual activity.
- Save the LiteBlue website address (<https://liteblue.usps.gov>) as a favorite.

As a reminder, passwords are the first line of defense against potential cyber threats. You should always maintain strong, unique passwords for your online accounts. USPS passwords require:

- A minimum of 15 characters;
- Upper- and lower-case letters (A-Z) (a-z); and
- Numbers (0-9)

If you believe your account has been compromised, contact CyberSecurity Operations Center (CSOC) immediately, at CyberSafe@usps.gov.

Sincerely,

Jenny Utterback
Vice President
Organization Development

Heather Dyer
Vice President
Chief Information Security Officer



Encl. Handouts (Keeping Your Private Information Secure; Updating Your Preferred Email Address)

DATE

Individual Name

Address/work and home

Redemption Code:

I am writing to inform you that the United States Postal Service's (Postal Service) Corporate Information Security Office (CISO) detected unusual log-in activity involving a limited number of employees' accounts within the Postal Service's PostalEASE system, including your account. Upon further investigation, it appears that your login credentials have been compromised. As a safety measure, your PostalEASE account has been auto locked and you will be required to reset your password and change your challenge questions and answers.

PostalEASE is a self-service web application that is your gateway to many postal employment-related services, including LiteBlue. The PostalEASE application has not been compromised; it remains secure. However, as noted, it appears that your login credentials have been compromised.

We believe your login credentials were compromised when you interacted with a fake LiteBlue website. We are unable to determine if this interaction was recent or whether it occurred sometime in the past.

The United States Postal Inspection Service, Office of Inspector General, and CISO discovered fake LiteBlue websites that accurately mimic the actual LiteBlue website. The official LiteBlue website is <https://liteblue.usps.gov>.

These fake websites may feature an address ("URL") that is similar to the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org." Scammers use these fake websites to collect employee login credentials. Once employees attempt to log in to the fake LiteBlue site using their credentials, the scammer records the information, which they can then use later to enter PostalEASE and access the employee's sensitive information. This information may be leveraged by the scammer or others for identity theft or other criminal purposes.

The Postal Service continues to take precautionary measures, including identifying and notifying potential victims; reviewing suspicious account activity; resetting credentials; and working with internet service providers to identify fake websites. We plan to continue investigating and monitoring the PostalEASE application on our network to mitigate the risk of unauthorized activity.

The Postal Service will purchase a 1-year credit monitoring service on your behalf due to the sensitive nature of the information about employees that is accessible through PostalEASE. Enclosed with this letter, you will find information on how to enroll in the credit monitoring service for 1-year at no cost to you. Please note the redemption code provided at the top of this letter, which will be required when you contact the credit monitoring company. You have 90 days from the date of this letter to take advantage of the credit monitoring service. We encourage you to take advantage of this service.

In addition to the Postal Service's ongoing monitoring efforts and the offered credit monitoring service, you will be required to reset your PostalEASE password and change the challenge questions and responses in PostalEASE.

To reset your password, go to liteblue.usps.gov and select "Forgot my Password." This will take you to the employee Self-Serve Password tool, where you will change your password and security

questions. Once reset, your password and new security questions will be available immediately. Please log in and verify your ability to access your PostalEASE account after you change your password and security questions.

You can increase the security of your account by selecting a new, unique password. We recommend making passwords unpredictable; avoid using names, including pets' names, dates, or often-used words that can be discovered. You should **never share your password** with anyone, including individuals or other third parties who request your EIN and password to provide financial or other services.

If you are interested in other resources that can be used to protect your identity, the Federal Trade Commission (FTC) is a good source of information. The FTC's website (www.ftc.gov) provides helpful information regarding identity theft and data protection. You can find information on identity theft from the FTC at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, or you may call the FTC's Identity Theft Data Clearinghouse at 1-877-438-4338 (TTY: 1-866-653-4261). In addition, you may also request a free credit report online at www.annualcreditreport.com.

Here are some additional resources to assist you going forward:

To report fake USPS websites, please email cybersafe@usps.gov

Should you identify any activity with your account that looks suspicious in the future, contact ISCCU@usps.gov

For PostalEASE account issues, contact the Human Resources Shared Services Center at 1-877-477-3273.

Please direct any questions regarding direct deposits or allotments to the Accounting Help Desk at 1-866-974-2733 and identify yourself as an active employee.