Mandatory Stand-Up Talk

Dec. 23, 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.

# # #

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.

# # #