

Steps to protect your UI account and lower your vulnerability to cyber fraud

# PROTECT YOUR UNEMPLOYMENT INSURANCE (UI) ACCOUNT FROM CYBER FRAUD

## Create a Strong Password

Include a combination of upper and lowercase letters, numbers, and special characters. Avoid reusing passwords, easy to guess words such as, family member names, pet names, and birthdates. Consider using a password manager tool to securely create and store your passwords. Never write down your passwords.

## Review your UI Claim Often

Make sure your password, direct deposit banking information, and address have not been changed.

## Beware of Fraud Schemes

Fraudsters try to steal your personal information by directing you to click on a link in an email or text message which often contain threats that your UI benefits will be affected or terminated if you do not respond. If you receive such a message, immediately contact the UI agency, and check the website for alerts on scams affecting UI claimants.

## Enable Multi-Factor Authentication (MFA)

If offered, enable MFA to help protect your UI account. MFA adds a second layer of security by requiring a one-time code from a secondary device, such as your cell phone, to complete the login process.

## Use Secure Internet Connections

If you need to use public Wi-Fi to access your UI account, go to a secure site such as a public library or a state agency workforce office. If using Wi-Fi from other public locations, use a Virtual Private Network. Always make sure no one can see your login credentials.

## Keep Device Software Updated

Ensure your computer, smartphone, and other electronic devices are updated and be sure to add anti-virus and anti-malware software for monitoring.



**REPORT ANY SUSPICIOUS  
ACTIVITY ON YOUR ACCOUNT  
IMMEDIATELY TO THE UI AGENCY!**

**Report fraud:**  
[workforce.iowa.gov/fraud](https://workforce.iowa.gov/fraud)