City of Hendersonville Staff,

We have discovered the City of Hendersonville has been a recent target of a cybersecurity incident. I have made the management team aware of the situation but want to reach out directly to the entire staff to update you on the situation, how we are responding, and the steps you should take.

Upon identifying the issue, we have been closely working with the North Carolina Local Government Information Systems Association Strike Team (NCLGISA) as well as the National Guard and other local, state and federal law enforcement partners to investigate the incident, protect employee information, and prevent unauthorized access to our data or other systems.

We determined that an unauthorized actor has made employee data available online that may include employee names, addresses, email addresses, phone numbers and social security numbers. It appears that persons first employed after January 1, 2021, were not affected by the incident. We do not believe that any employee financial data or beneficiary information was part of this incident.

We will be offering complimentary credit monitoring and identity theft protection once we have determined the individuals that may have been impacted by this incident. While we conduct an extensive investigation into this incident with cybersecurity experts and law enforcement, we strongly encourage you to review the information below and attached and take appropriate action.

Passwords

1. Reset your Oracle password if you haven't already. A password change prompt email has already been sent out. Instructions are attached to this email, or you can use the 'Forgot Password' option on the login screen.
2. While we have no indication that personal passwords were compromised, we strongly encourage all employees to change all personal account passwords on a regular basis, with particular care to change passwords related to financial institutions, medical institutions, personal email accounts, and any other sensitive or valuable accounts that you have identified.
3. We strongly encourage staff to use strong passwords for all personal accounts and avoid using the same passwords on multiple sites.
4. Whenever possible, please leverage Multifactor Authentication (free options are available through Google and Microsoft) to add an additional layer of protection to your personal accounts.

Credit Monitoring

5. Remain vigilant by reviewing all account statements for any fraudulent activity. Any fraudulent activity should be reported to your financial institution or the platform where questionable activity is noticed.
6. We strongly recommend that all employees take additional precautions, such as placing alerts on their credit files.
    a. You may contact any of the following credit bureaus to ask that a fraud alert be placed on your credit files:
        - Equifax: 1-800-525-6285

- Experian: 1-888-397-3742
- TransUnion: 1-800-680-7289

7. We also recommend that employees take advantage of the free security freeze service to prevent fraudulent activity or the opening of credit using your data. This is the strongest protection available. You can request a free security freeze by visiting this website: https://ncdoj.gov/protecting-consumers/protecting-your-identity/free-security-freeze/
8. If you detect any suspicious activity, please notify the entity with which the account is maintained, and promptly report the suspicious activity to appropriate law enforcement authorities, including the State of North Carolina's Attorney General's Consumer Protection Division (877-566-7226) and the Federal Trade Commission Identify Theft Division (https://identitytheft.gov).

Social Security Number

9. You can request to block electronic access to your Social Security number. This is done by calling 1-800-772-1213. Once requested, any automated telephone and electronic access to your Social Security record is blocked. No one, including you, will be able to see or change your personal information on the internet or through the Social Security Administration's automated telephone service. If you have requested that the SSA block access to your record and change your mind in the future, you can contact the SSA and ask to have the block removed. You will be asked to prove your identity when you call.

Additional Resources and Reminders

- If any employees need access to computers to take these steps, they can visit HR and use the training laptops.
- If you experience any fraudulent activity or identity theft attempts, please make HR aware by filling out the form at https://www.cognitoforms.com/CityOfHendersonville4/IdentityTheftFraudulentActivity
- If you receive any media inquiries or public information requests, please refer them to Allison Justus at ajustus@hvlnc.gov
- A section of the Helpful Information & Links tab on the HUB has been established containing this information as well as additional identity theft protection tips.

The protection and security of our City systems and the data they contain, including our employees' data, is of the utmost importance to the City of Hendersonville and we will keep you updated if there are changes to the situation.

We value our staff and appreciate your dedication to serving the public. We take our responsibility to safeguard your personal information seriously, and we apologize for any inconvenience or concern this incident may cause.

Sincerely,

John Connet