Talking Points- Special Bulletin

Stop the Press! This is your Special Bulletin edition of TSIB's Talking Points.

Talking Points- Special Bulletin provides you information on the latest developments for a high profiled news story which can affect the Insurance & Surety industry.

Look for the **TSIB Talking Point** that highlights the issue and keeps you informed.

If you have any questions about any of our articles, other Insurance & Surety concerns, or have specific topics you would like to learn more about, please reach out to us directly at contact@tsibinc.com or visit our website.

Talking Points- Special Bulletin

26 Billion Records Leaked From Companies including LinkedIn

Earlier this week on Monday January 22nd, news outlets began reporting on a major data leak that has potentially compromised 26 billion records. The allegedly compromised information came from numerous companies, including LinkedIn, X (formerly Twitter), Dropbox, Adobe, Canva, Tencent, and Weibo.

According to researchers, the data came from known sources, but it does not appear at this time that the data is new data, rather it is compiled records from previous breaches and data leaks. However, this still creates risk since user logins and passwords were compromised.

On Tuesday, according to Forbes, a LinkedIn spokesperson shared:
"We are working to fully investigate these claims and we have seen no evidence that LinkedIn's systems were breached. You can find more information on how we keep members safe from scraping here."

There may be an increase of credential stuffing attacks in the coming weeks. This type of cyberattack is an automated attack that inserts stolen usernames and passwords into a system's login field to obtain full access for fraudulent purposes.

Credential stuffing attacks work because people use the same password for multiple accounts. For example, if someone uses the same password for both their grocery store loyalty program and bank account, the hackers attack the less defended database (ex. grocery store loyalty program). Then they use that information to try and get into the person's bank account. This is why it's important not to utilize the same password for multiple accounts.

Cybersecurity experts are recommending that users update their passwords to a strong, random password. It's vital that everyone is aware of the increasing prevalence of phishing emails. Users are encouraged to implement two-factor authentication as an additional security measure, when possible.

Experts have suggested utilizing a Cyber Data Leak Checker to find out if your accounts have been compromised. It may be too early to see if your data has been identified as compromised, and this should be checked regularly.

TSIB Talking Point: This breach is another reminder of how fragile our information systems are for cyber-attacks. The U.S. Government needs to work with the companies that are entrusted with our data to strengthen the data privacy laws. Until then, businesses and individuals must remain vigilant and active to protect our data with strong passwords and to be constantly aware of phishing attempts.

To read more about the topic, please click the following links:

- Warning 26 billion Records Leaked (Forbes)
- Time to Update your Password (MSN)