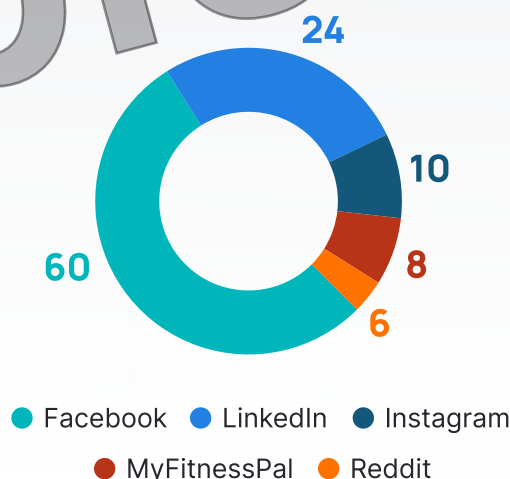
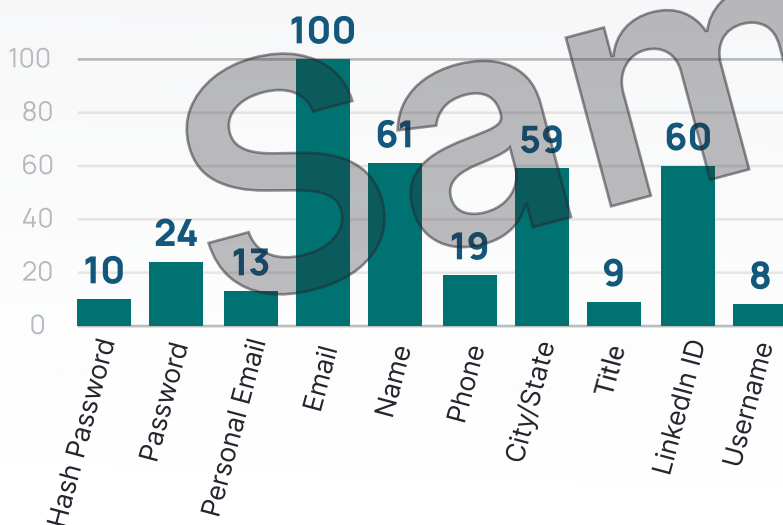


SUMMARY OF FINDINGS

Cowbell is pleased to share a comprehensive report of our Dark Web findings related to your organizations's domain — www.dixonvalve.com.

The report the LinkedIn breach as the leading data source where information was exposed. Through our analysis of the results, it appears that most of the compromised information was related to personal identifiable information (PII), LinkedIn ID, and approximately **34%** of emails had their password credentials leaked. We've provided a snapshot of how many times each criteria was exposed and our data source findings. We do encourage you to review the entire data set, which is provided in the later section.

363	Total number of exposed information
34	Total number of exposed credentials with passwords (plain text or hash)
19	Total number of exposed passwords (plain text or hash) in 2021



Recommendations

Enable Multi-Factor Authentication (MFA)

Common practice for an added layer of protection to keep accounts more secure and prevent unauthorized access. Consider a mix of elements like authenticator applications, secure ID tokens, and security questions.

Robust password policy

A strong password policy would include at least 10 characters — a combination of uppercase and lowercase letters, numbers, and symbols or special characters.

Embrace cybersecurity awareness training and education

Conduct workshops to educate employees regularly given the evolving cybersecurity threat landscape.

Good email hygiene

Verify opening suspicious emails, take cations with links/attachments/URLs from unrecognized senders, and encourage employees to report susicious activity to IT.

Patch management on both software and hardware

EMAILS LEAKED	PW LEAKED	DATE PUBLISHED	DATA SOURCE	SENSITIVE INFORMATION
sampleemail@company.com	Hash	2022-01-22	Facebook	Email and Password
sampleemail@company.com	Yes	2022-01-22	MyFitnessPal	Email and Password
sampleemail@company.com	Hash	2022-01-22	Linkedin	Email and Password
sampleemail@company.com	Yes	2022-01-22	Reddit	Email and Password
sampleemail@company.com	Hash	2022-01-22	Instagram	Email and Password
sampleemail@company.com	Yes	2022-01-22	MyFitnessPal	Email and Password
sampleemail@company.com	Hash	2022-01-22	Instagram	Email and Password
sampleemail@company.com	Yes	2022-01-22	LinkedIn	Email and Password
sampleemail@company.com	Hash	2022-01-22	Facebook	Email and Password
sampleemail@company.com	Yes	2022-01-22	Reddit	Email and Password
sampleemail@company.com	Hash	2022-01-22	Linkedin	Email and Password
sampleemail@company.com	Yes	2022-01-22	MyFitnessPal	Email and Password
sampleemail@company.com	Hash	2022-01-22	Instagram	Email and Password