9 WAYS YOUR EMPLOYEES' WORK CREDENTIALS CAN LEAD TO A BREACH

When your employees use their work email on websites like the ones listed below, it makes your business vulnerable to a breach. With our Dark Web Monitoring, we can detect if your company is at risk due to exposed credentials on 3rd party websites.

HR & PAYROLL
blackbaud®
BenefitMall ADP
CERIDIAN

EMAIL SERVICES
yahoo!mail
Office 365
M

CRM
salesforce
HubSpot
CENTRALSQUARE TECHNOLOGIES

TRAVEL SERVICES
MGM RESORTS INTERNATIONAL
MARRIOTT AMTRAK
CWT

COMMUNICATIONS
verizon✓
AT&T Google
Virgin media T··Mobile··

E-COMMERCE
amazon
Staples THE HOME DEPOT
DOORDASH

BANKING & FINANCE
Capital One
intuit quickbooks.
BANK OF AMERICA

COLLABORATION
A Canva
evite zoom
GoDaddy aws

SOCIAL MEDIA
(Twitter) (LinkedIn) (Facebook)
(Instagram) (TikTok) (YouTube)

UNDERSTAND & MITIGATE YOUR RISK

EXTERNAL THREAT INTELLIGENCE
Are you monitoring for compromised data that can be used to exploit your business?

YES ☐ NO ☐

DATA BREACH & PRIVACY LAW COMPLIANCE
Do you have a compliant data breach response plan in place?

YES ☐ NO ☐

OF EXPOSED CREDENTIALS FOR YOUR COMPANY

[   ]