

Angående dataintrånget mot systemleverantören Miljödata och att Stockholms stad samtliga anställdas personuppgifter har läckt

Så här skriver tidningen Mitt i:

*"Angriparen har kommit åt personuppgifter om alla anställda i Stockholms stad," står det i brevet som skickats ut till de anställda.*

*"Möjliga konsekvenser av incidenten är att du riskerar att förlora kontrollen över dina egna personuppgifter och att personuppgifterna används på ett bedrägligt sätt. [...] Vi följer nära den information som staden får från Miljödata och den polisutredning av incidenten som nu pågår," skriver staden.*

Vanliga onlinebedrägerier på arbetsplatsen inkluderar:

- Nätfiske - när bedragare använder falska e-postmeddelanden eller meddelanden för att lura offer att avslöja personlig information eller ladda ner skadlig programvara.
- Smishing - en typ av nätfiske som använder textmeddelanden (SMS) i stället för e-post.
- Spear phishing - en mer riktad form av nätfiske som fokuserar på specifika individer, ofta genom att utge sig för att vara någon som offret känner, till exempel en chef eller kollega.

Förhindrande av bedrägeriförsök sker genom att vara proaktiv och mäts i färre lyckade bedrägeriförsök, starkare detekteringssystem och mer informerade användare som kan känna igen och rapportera hot.

Vi vill:

-att förvaltningen redovisar hur de arbetar proaktivt för att motverka bedrägeriförsök mot de anställda.

-att förvaltningen redovisar om det finns framtagna nyckeltal förvaltningen använder för att mäta framstegen i att förhindra bedrägeriförsök och andra cyberattacker.