**Fakta 1: 90% av datainnbrudd**

**starter med en svindel-epost!**

Sikre bedriften ved å styrke den
interne sikkerhetskulturen. 

Et datainnbrudd kan resultere i stor skade for en bedrift. Å miste tilgang til sine data eller systemer kan få store konsekvenser. **Hvordan ville din bedrift blitt påvirket om tilgangen til å jobbe med systemer, e-post eller tilgang til dokumenter ble utilgjengelig?**

 **Fakta 2: Riktig system for bevisstgjøring
av ansatte senker faren for datainnbrudd:**

|  |  |
| --- | --- |
| Et bilde som inneholder tekst, skjermbilde, Font, line  Automatisk generert beskrivelse | Uavhengig av om bedriften er stor eller liten, **nettkriminelle vil gå etter det enkleste byttet**. Mange tror at de største bedriftene er mest utsatt, men tvert imot, så er de mindre bedriftene som blir oftest utsatt for datainnbrudd. |

|  |  |
| --- | --- |
| **Et bilde som inneholder Elektrisk blå, lilla, Grafikk, symbol  Automatisk generert beskrivelse** | **Ferdighetsvurdering**Begynn med en vurdering av bevissthetsnivåer blant deansatte. Velg standard konfigurasjon, eller tilpasset trening forforskjellige brukergrupper, avdelinger, eller lignende. |
|  | **Opplæring**Verdens største bibliotek med varierte moduler:interaktive moduler, videoer, spill, plakater og nyhetsbrev.Kampanjer er automatiserte og brukere får påminnelser. |
| **Et bilde som inneholder metallvarer, krok  Automatisk generert beskrivelse** | **Simuleringer**Test og kartlegg de ansattes reaksjonsmønster. Med kunstigintelligens vurderer systemet brukernes håndtering aveksempelvis svindel-epost, og tilpasser utfordringene mot resultaterfor best læringsutbytte. |
| **Et bilde som inneholder Grafikk, Font, design  Automatisk generert beskrivelse** | **Se resultatene**Rapportene viser bl.a. kontinuerlig fremgang for bedriften,slik at du lett kan male verdien av investeringen. |

Ved å benytte en løsning som vil trene og teste de ansatte kontinuerlig på en intuitiv og engasjerende måte, vil læringsutbyttet bli stort og bedriften stå bedre rustet mot et datainnbrudd. Siste linjen i forsvaret vil alltid være brukerne, og har de kunnskapen om å avsløre en falsk e-post, nettside eller andre svindelforsøk, så vil bedriftens sikkerhet styrkes betraktelig!

* **Simuleringer styrt av kunstig intelligens** for å best tilpasse seg brukerne individuelt og gi mest mulig reell testing og progresjon.
* Trening som vil sammenfattes av forskjellige kategorier med alt fra datahåndtering, forskjellige svindelmetoder og sosial manipulasjon, kryptovirus, fysisk sikring, passord, osv. Også her benyttes **kunstig intelligens for å tilpasse trening** for bedriten ut fra brukernes atferd på tester og tidligere treninger.
* Få rapporter med **bedriftens sikkerhetsscore** og se de utviklingen i sikkerhetskulturen.
* Gi de ansatte muligheten til å **varsle rett fra e-post** om de skulle være usikker på en melding, noe som bidrar til å minimere sjansen for at noen tar sjansen på noe de er usikker på.
* Læringssystemet kan også benyttes til **eget innhold som lastes opp** av hva man måtte ønske at de ansatte skal utføre. Da får man også gjennomføringsstatistikk på dette og hvordan man ligger an.
* … og mange flere funksjoner og muligheter inkludert!