Awareness training

In een tijd van het nieuwe werken, waar medewerkers flexibeler en op afstand werken, worden steeds meer leidinggevenden binnen bedrijven zich bewust van de noodzaak van een specifieke awareness training. De training richt zich op de beveiligingsaspecten van cyber security, zoals veilig gebruik van thuisnetwerken en bescherming van bedrijfsinformatie tijdens virtuele vergaderingen.

Actief betrokken bij cybersecurity

Het doel van een security awareness training is een veiligheidsbewuste cultuur te bevorderen en medewerkers uit te rusten met de nodige kennis voor veilig werken buiten en binnen de traditionele kantooromgeving. Bedrijven streven naar een actieve betrokkenheid van alle teamleden om een veilige en productieve werkomgeving, ongeacht de locatie, te waarborgen.

Bewustwording als eerste veiligheidsmaatregel

Een cybersecurity awareness training vergroot de bewustwording en bevordert de veiligheidsbewuste praktijken onder de collega's van uw bedrijf.
De training richt zich op het verminderen van het risico op cyberdreigingen door medewerkers te voorzien van de nodige kennis en vaardigheden om cyberveiligheid in hun dagelijkse werkzaamheden te integreren. De training is bedoeld voor alle medewerkers, ongeacht hun afdeling of functie.
Het is ontworpen om rekening te houden met verschillende niveaus van technische kennis en ervaring.

Inhoud van de training

- **Phishing Preventie:** Herkennen van phishing-aanvallen, identificeren van verdachte e-mails en meldingsprocedures.
- **Wachtwoordbeheer:** Bevordering van sterk wachtwoordbeleid, inclusief het gebruik van wachtwoordbeheertools.
- **Veilig Gebruik van Bedrijfsmiddelen:** Bewustwording creëren voor veilig gebruik van bedrijfsapparaten, netwerken en software.
- **Mobiele Beveiliging:** Veilig omgaan met bedrijfsgegevens op mobiele apparaten en bescherming tegen verlies of diefstal.
- **Social Engineering:** Herkennen van sociale technieken en het voorkomen van manipulatie.
- **Data Privacy:** Begrip van de vereisten voor gegevensprivacy en de rol van medewerkers bij de bescherming van persoonlijke en zakelijke informatie.
- **Incident Response:** Het melden van verdachte activiteiten en de juiste stappen bij een cybersecurity-incident.

Trainingsmethoden:

De training zal een mix van interactieve methoden bevatten, waaronder presentaties, scenario-gebaseerde voorbeelden, discussies en een demo. Er zal voldoende ruimte zijn voor vragen om de betrokkenheid te vergroten.

Evaluatie:

Na afloop van de training worden deelnemers geëvalueerd om de effectiviteit van de training te meten. Feedback zal worden verzameld om eventuele aanpassingen voor toekomstige sessies te informeren. Ook kan desgewenst een van de awereness-onderwerpen getest worden door e-Quest om te bepalen in hoeverre de medewerkers opgedane kennis in de praktijk toepassen.

e-Quest
Uw IT-partner altijd dichtbij

0492 - 392626 info@e-Quest.nl e-Quest.nl