Emploware
Cybersecurity & Awareness

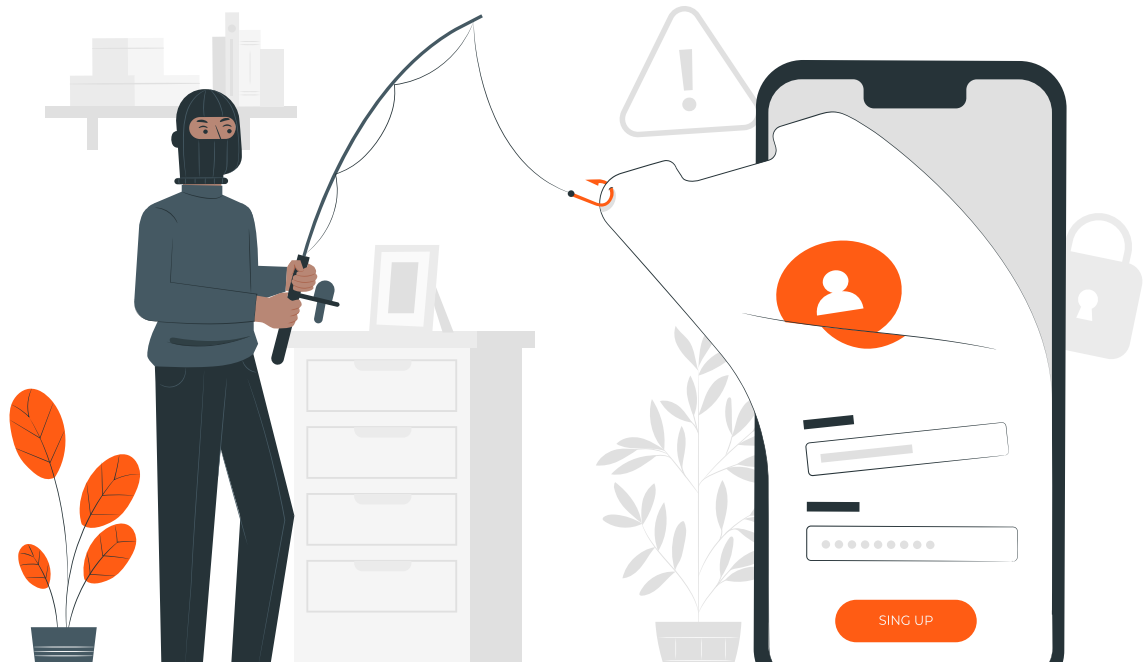
Cybersecurity Awareness Training

Introductie

Waar cybercriminaliteit voorheen wellicht voor velen iets was, wat alleen grote bedrijven trof, is dat vandaag de dag compleet anders. Ook kleinere bedrijven worden met regelmaat aangevallen. Volgens Cyberint vindt 43% van alle aanvallen plaats op het midden en kleinbedrijf. Eenieder die waardevolle informatie bezit, is een potentieel doelwit van hackers.

Hoewel u wellicht alle mogelijke technische beveiligingen in uw bedrijf hebt doorgevoerd, bent u enkel zo sterk als de zwakste schakel. Het is een cliché, maar helaas waar. Binnen het gebied van cybersecurity is die zwakke schakel vaak de menselijke factor.

Hoe goed uw verdediging ook is, wanneer een medewerker op een phishing link klikt en gevoelige data invult, kan deze actie veel schade aanrichten binnen uw bedrijf. Het aanbieden van de juiste training aan medewerkers, om bewustzijn te creëren, is daarom ook essentieel geworden. Meer dan 90% van alle inbreuken zijn het gevolg van een menselijke fout. Technische beveiliging alleen, is niet langer afdoende.



01 Wat is **Cybersecurity Awareness**?

Wat is cybersecurity awareness? Kort gezegd is cybersecurity awareness de mate waarin eindgebruikers op de hoogte zijn van:

- De dreigingen waarmee hun netwerken worden geconfronteerd,
- Alsmede de risico's die ze introduceren, en
- De beste werkwijze om deze risico's te beperken.

Met andere woorden, bij cybersecurity awareness draait het om het trainen van het bewustzijn van bedreigingen en hoe men hier op reageert. Hierbij ligt de focus dus niet enkel op kennis, maar ook op het gedrag en de houding.

Waar een hacker aan slechts één enkele opening genoeg kan hebben, is het zaak voor een organisatie om voor volledige beveiliging te zorgen. Iedere werknemer, en ieder apparaat dat op uw netwerk is aangesloten, is daarbij een potentieel lek.

TIP: Hanteert u een 'Bring Your Own Device' (BYOD) policy, waarbij medewerkers hun eigen apparatuur meenemen en aansluiten op het bedrijfsnetwerk? In dat geval is het 't beste om hier een apart netwerk voor op te zetten, zoals een gastnetwerk, zonder dat deze apparaten verbinding maken met het bedrijfsnetwerk. Anders kunnen deze apparaten namelijk het bedrijfsnetwerk infecteren met malware, wat zij wellicht vanuit een andere omgeving hebben meegekregen.

02 Het belang van **Security Awareness**

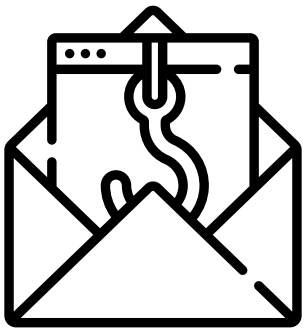
Twijfelt u wellicht nog aan het belang van security awareness? Cybersecurity kan niet langer worden genegeerd en zeker niet beschouwd worden als kostenpost. Zoals Easyjet-ondernemer Stelios Haji-Ioannou het voor de luchtvaartindustrie verwoordde: 'If you think safety is expensive, try having an accident!'. In zekere zin kan Cybersecurity in deze vergeleken worden met de luchtvaartindustrie.

Het is niet zozeer de vraag of u met een aanval te maken krijgt, maar vooral wanneer. En hoe bent u daar dan op voorbereid?

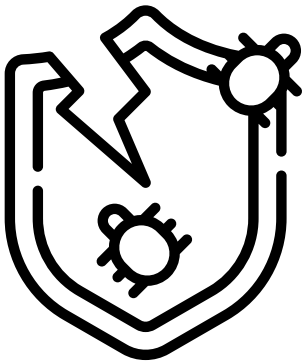
Alsof bovenstaande zaken nog niet genoeg vragen van een onderneming, brengen ook ontwikkelingen zoals thuiswerken nieuwe uitdagingen met zich mee. Werknemers hebben thuis doorgaans namelijk niet dezelfde beveiliging zoals een organisatie. Ook in die gevallen is het bijbrengen van bewustzijn de eerste stap om risico's te beperken.

Indien awareness training nu nog niet onmisbaar is, zal dit in de toekomst zeker het geval zijn. Bewustzijn helpt uw organisatie op de volgende punten:

REDUCEREN VAN RISICO



Doordat uw medewerkers kennis hebben opgedaan van levensechte scenario's zijn zij beter in staat om (potentiële) aanvallen te herkennen. Meer dan 90% van alle inbreuken zijn het gevolg van een menselijke fout. Door middel van educatie reduceert u dit risico aanzienlijk.

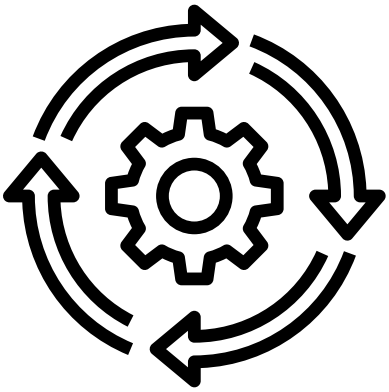


BEPERKEN VAN SCHADE

Het trainen van uw werknemers zorgt niet alleen voor een kleiner risico, het kan daarnaast ook de schade significant beperken. De gemiddelde kostenpost bij een gegevenslek is volgens een 2021 rapport van IBM $4.24 miljoen dollar. Uw organisatie kan met de juiste kennis, gedegen veiligheidsmaatregelen doorvoeren. Wanneer uw medewerkers dezelfde principes volgen zijn zij sneller in staat afwijkingen te identificeren en hierop te anticiperen, met als gevolg schadebeperking.

WERKNEMERS PRESTEREN BETER

Uit onder andere onderzoek van Research Scholar, Department of Business and Financial Studies, University of Kashmir blijkt dat training een positief effect heeft op de arbeidsprestaties van de werknemers. Training is een motiverende factor die de kennis van de werknemer ten aanzien van zijn werk vergroot, waardoor werknemers beter worden in hun werk en in staat zijn betere resultaten te leveren..[1]

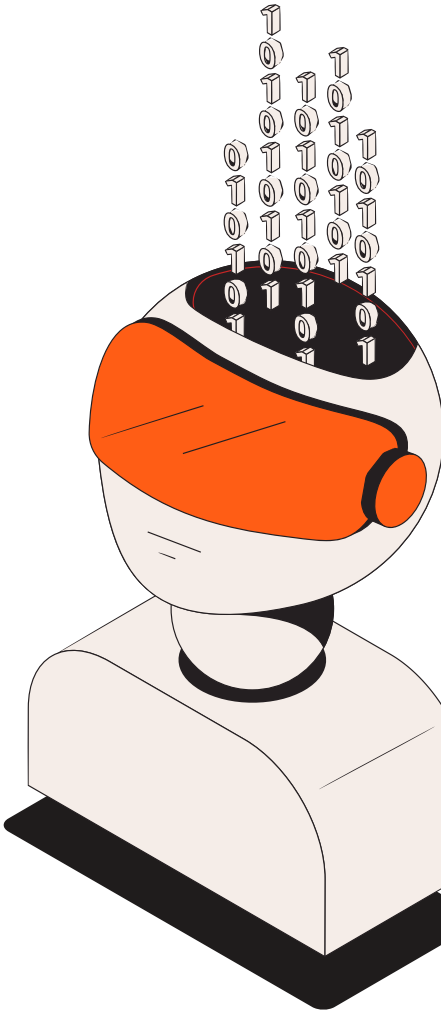


EENVOUDIGE IMPLEMENTATIE

De awareness training van Employware is volledig online. Daarnaast kunnen uw medewerkers in hun eigen online omgeving inloggen en met slechts een aantal minuten per week hun kennis en bewustzijn vergroten.

[1] https://www.researchgate.net/publication/262843202_Impact_of_Training_on_Employee_Performance_A_Study_of_Retail_Banking_Sector_in_India

03 De Training



Awareness training is de basis voor elke organisatie, maar wel volgens het tempo en schema van uw werknemers. De trainingen zijn zodoende kort, volledig online, in meer dan 15 talen beschikbaar en in uw eigen tempo te volgen. Met frequente updates blijven wij ook actueel en is er het gehele jaar door nieuwe stof voor uw medewerkers.

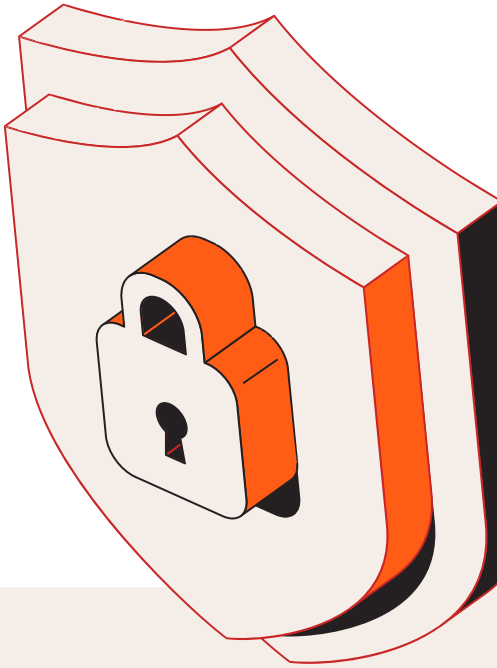
Met een besteding van slechts enkele minuten per week trainen uw medewerkers zichzelf. Zij doen dit door het bekijken van levensechte, korte video's en het beantwoorden van quizvragen.

Het platform biedt:

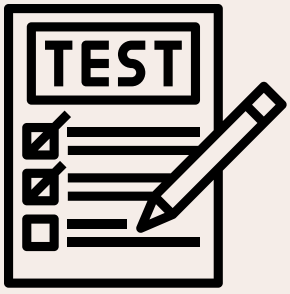
- Meer dan 20 trainingsprogramma's
- Meer dan 15 talen
- Quizvragen
- Inzicht in kwetsbare afdelingen
- Training met slechts enkele minuten per week

04 Andere **trainingsvormen**

Het creëren van bewustzijn door middel van trainingen is de eerste stap naar een sterkere organisatie. De theorie moet echter wel in de praktijk toegepast worden. Met behulp van de volgende twee trainingsmethoden kunt u ook zien hoe de uitvoering in de praktijk is, zonder dat dit nadelige gevolgen heeft voor uw bedrijf.



SOCIAL ENGINEERING



Met de term social engineering doelen wij op de 'kunst' van het manipuleren van mensen, zodat zij vertrouwelijke informatie vrijgeven. Het is een overkoepelende term om diverse technieken te beschrijven. Voorbeelden van social engineering zijn:

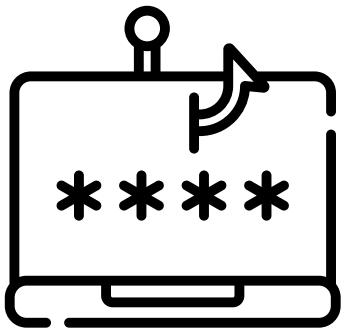
- Een usb-stick met malware achterlaten, met het doel een nieuwsgierige medewerker te triggeren om de usb stick in zijn computer te stoppen;

- Tailgating: waarbij het doel is om iemand te volgen tot in een beveiligde of beperkt toegankelijke zone;
- Vishing: voice phishing, ofwel telefonische phishing, waarbij per telefoon wordt getracht om gevoelige data te achterhalen.

Als u de mensen binnen uw organisatie wil testen, kunnen wij diverse social engineering tactieken, met uw goedkeuring, toepassen. Dit kunnen de reeds genoemde voorbeelden zijn, of varianten die voor uw organisatie van belang zijn.

PHISHING SIMULATIE

Phishing is een specifieke techniek, die binnen de koepelterm ‘social engineering’ valt. Het gaat hierbij dus ook om het verkrijgen van gevoelige informatie en normalerwijs gebeurt dit bij phishing per e-mail. Bij phishing draait het vaak om inloggegevens of credit card details. Aanvallers bereiken dit door bekende instanties, zoals een bank, na te bootsen en mensen naar een malafide website te lokken.



Bij een phishing simulatie krijgen uw medewerkers op al dan niet aangekondigde momenten niet schadelijke phishing mails. Door middel van ons systeem kunt u zien welke werknemers een link openen, aanklikken of wellicht zelfs bijlagen downloaden.

05 Statistieken

88% van de organisaties wereldwijd kreeg in 2019 te maken met spear phishing-pogingen. (Proofpoint)

In 2020 duurde het gemiddeld **207** dagen om een inbreuk vast te stellen. (IBM)

In 2018 werden gemiddeld **10,573** kwaadaardige mobiele apps per dag geblokkeerd. (Symantec)

De gemiddelde kosten van een ransomware-aanval op bedrijven bedragen **$133,000** (SafeAtLast)

Elke minuut gaat er **$17,700** verloren door een phishingaanval. (CSO Online)

Tegen 2023 zal het totale aantal DDoS-aanvallen wereldwijd **15.4M** bedragen (Cisco)

Aanvallen op IoT-apparaten verdrievoudigd in de eerste helft van **2019** (CSO Online)

1 op de 36 mobiele apparaten heeft apps met een hoog risico geïnstalleerd. (Symantec)

Bij **20%** van de organisaties hebben thuiswerkers een inbreuk op de beveiliging veroorzaakt. (Malwarebytes)

43% van alle cyberaanvallen is gericht op het midden- en kleinbedrijf (Cyberint)

94% van alle malware wordt per email verzonden (CSO Online)

IoT-apparaten De term IoT is een afkorting voor Internet of Things en daarmee doelen wij op fysieke voorwerpen die verbonden zijn met het internet en gegevens kunnen verzenden. Dit zijn bijvoorbeeld auto's, slimme deurbellen, smartwatches etc.

DDOS-aanval: Tijdens een DDoS-aanval wordt een server van een website overbelast, door in een specifieke periode, heel veel aanvragen te verzenden. De server kan dit daardoor niet meer verwerken en functioneert zodoende niet meer goed.