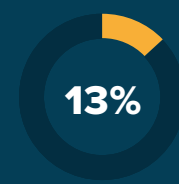


## Cyberveilig gedrag. **Waarom doen we het nog niet?**

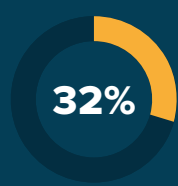
Waar mensen werken, ontstaan kwetsbaarheden. De cybercrimineel weet hier gretig misbruik van te maken door medewerkers op een slimme manier te beïnvloeden. Cyberaanvallen worden immers in 66% van de gevallen veroorzaakt door werknemers. Bij Hoffmann doen we voortdurend onderzoek naar de kwetsbaarheden in organisaties en kijken we naar de oorzaken die hieraan ten grondslag liggen.



70% geeft wachtwoord aan onbekende 'collega' per telefoon of per mail



13% vult gegevens in na het klikken op link in phishing mail

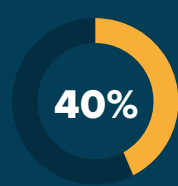


32% van de medewerkers logt in op een onbeveiligd publiek WiFi-netwerk met hun zakelijke apparaten

Willis Towers Watson 2017 Cyber Risk Survey

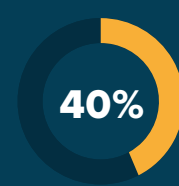


95% schenkt geen aandacht aan onbekende zonder bezoekerspas



40% van de Nederlanders hergebruikt hetzelfde wachtwoord

PanelWizard, 2018 i.o.v. J&V



40% van de wachtwoorden is binnen 24 uur te kraken



### 1 op de 3 organisaties investeert in awarenesstrainingen

Er is veel aandacht voor bewustwordingssessies binnen de informatiebeveiliging. Maar zelfs als organisaties een sterk veiligheidsbeleid mét awarenesstrainingen volgen, blijken regels niet voldoende om cyberveiligheid te borgen. Waarom? De kloof tussen 'weten' en het daadwerkelijk 'doen' is te groot.

Digital Trust Insights 2018

### Regels blijken niet voldoende om cyberveiligheid te borgen. Hoe komt dit?



Het ontbreekt regelmatig aan motivatie



De werkomgeving is er niet goed op ingericht



Medewerkers krijgen onvoldoende ondersteuning



Risico's en impact worden vaak onderschat



Er is sprake van beperkte awareness



Vriendelijkheid gaat vaak boven veiligheid

#### Meer dan awareness

Gedrag is afhankelijk van 3 factoren: capaciteit, gelegenheid en motivatie. Oftewel: wil iemand het doen, is iemand in staat om het te doen en krijgt iemand de kans om het te doen? Awareness is hierin een noodzakelijke stap, maar niet voldoende om op zichzelf tot effectieve gedragsverandering te leiden. Er is meer voor nodig om uw medewerkers te wapenen tegen cybercriminelen.

Meer weten? Ga naar [www.cyberveiliggedrag.nl](http://www.cyberveiliggedrag.nl)