awaretrain
Security Awareness

Communication Guide

Awaretrain
Kerkenbos 1053K
6546 BB Nijmegen

+31 (0)88 018 16 20
cs@awaretrain.com
awaretrain.com

Wat is het doel van deze guide?

Met deze communication guide willen we je inspireren met aanvullende communicatie die je tijdens de security awareness campagne kan inzetten. Communiceer deze aanvullende communicatie bijvoorbeeld via het intranet, interne nieuwsbrieven of gezamenlijke bijeenkomsten. Overweeg daarnaast om deze communicatie aan te vullen met goodies, zoals webcamcovers of bedrukte koffiebekers.

Per thema zie je welke modules het thema behandelen en welke posters en cartoons we voor het thema aanbieden. Het getoonde nummer is de tag van de desbetreffende module in het Awaretrain-platform. De posters en cartoons kunnen in acht talen gedownload worden via de downloadlink.

Zorg voor een goede spreiding van de verschillende modules en aanvullende communicatie. Wij adviseren om maximaal 12 modules per jaar uit te rollen, zodat de werklast voor de gebruikers niet te hoog wordt en het draagvlak hoog blijft.

1. Het belang van security awareness

Modules over dit thema:	*T01, T34, T43*
Poster(s):	*P01 Kick-off, P10 - Checklist, P13 Cybersecurity myths & facts*
Cartoon(s):	*C01 Human factor*

Een goed begin is het halve werk. Dit thema is bedoeld als kick-off van het e-learningprogramma om medewerkers te laten begrijpen wat het belang van security awareness is of om de voortgang van het programma te evalueren. Ideeën voor aanvullende communicatie zijn:

- Laat de CEO of een ander directielid een filmpje inspreken over het belang van informatieveiligheid voor de organisatie en benadruk de belangrijke rol van de medewerkers hierin.
- Deel voorbeelden van incidenten/datalekken uit het verleden binnen de eigen organisatie of bij branchegenoten.
- Deel een voorbeeld over wat het zou betekenen als de interne IT-systemen er voor een bepaalde periode uit zouden liggen.
- Maak het gevaar tastbaar en deel inzichten over dreigingen, zoals het aantal interne meldingen van verdachte situaties en het aantal geblokkeerde dreigingen door technische oplossingen.

2. Wachtwoorden

Modules over dit thema:	*T02, T08, T30, T35, T47, T49, T55, T57*
Poster(s):	*P02 Passwords*
Cartoon(s):	*C02 Never share your password*, *C05 Change your password regularly*

In de modules over dit thema leggen we het belang uit van lange wachtwoorden, het gebruik van een wachtzin, het gebruik van multi-factorauthenticatie en het gebruik van een passwordmanager. Aanvullend kan je:

- Aangeven wat de minimale wachtwoordlengte binnen de organisatie is.
- Of en hoe vaak men het wachtwoord moet wijzigen.
- Of er wel eens briefjes met wachtwoorden worden gevonden.
- Communiceren welke wachtwoordmanager er binnen de organisatie gebruikt wordt en waar men informatie kan vinden over het gebruik hiervan.
- Aangeven op welke systemen multi-factorauthenticatie wordt gebruikt en waar men dit eventueel zelf moet inschakelen.

3. AVG & Privacy

Modules over dit thema:	*T25, T27, T28, T42*
Poster(s):	*P09 Privacy, P11 GDPR*
Cartoon(s):	*C09 Privacy, C12 GDPR*

In de modules over dit thema geven we algemene uitleg over de AVG-wetgeving en privacy in het algemeen. Aanvullend kan je:

- Communiceren waar en welke persoonsgegevens de organisatie verwerkt.
- Laten zien waar mensen terecht kunnen met vragen over privacy en de AVG of in geval van (vermoedelijke) datalekken.
- Medewerkers informeren over (bijna) datalekken uit het verleden.

4. Veilig op het internet

Modules over dit thema:	*T03, T04, T05, T06, T09, T36, T53*
Poster(s):	*P03 Hackstore*
Cartoon(s):	*C03 HTTPS, C13 Online dangers*

In de modules over dit thema geven we uitleg over de gevaren op het internet en de maatregelen die hiertegen genomen kunnen worden. Aanvullend kan je:

- Communiceren wat het beleid is over het bezoeken van bepaalde websites. Denk hierbij ook aan het privégebruik van bepaalde systemen.
- Aangegeven welke clouddiensten binnen de organisatie zijn toegestaan en welke expliciet niet.
- Uitleggen welke internet- en e-maildomeinen binnen de organisatie gebruikt worden.

5. Phishing

Modules over dit thema:	*T07, T10, T29, T31, T32, T33, T37, T44, T50, T56*
Poster(s):	*P04 Phishing*, *P14 How to recognise phishing*, *P15 Clicking on phishing*
Cartoon(s):	*C04 Phishing*, C11 CEO fraud

In de modules over dit thema behandelen we alles rondom diverse vormen van phishing. Aanvullend kan je:

- Het resultaat van de afgelopen phishing simulatie(s) delen.
- Overwegen om een interne challenge te starten om te zien welke afdeling het beste scoort op phishing simulaties. Beloon het best presterende team.
- Communiceren hoeveel meldingen van phishing er periodiek worden gedaan.
- Communiceren hoeveel phishingmails geblokkeerd worden door technische systemen.
- Verwijzen naar publicaties zoals 'Cybersecuritybeeld Nederland' of 'Verizon Data Breach
- Investigations Report', waaruit blijkt dat bij het grootste gedeelte van alle digitale aanvallen een vorm van phishing wordt gebruikt.
- Laten zien waar en hoe mensen melding moeten doen van verdachte e-mails en in geval van (vermoedelijke) incidenten.

6. Veilig mobiel

Modules over dit thema:	*T15, T16, T17, T18, T21, T23, T24, T40, T41*
Poster(s):	*P08 Fairytales*
Cartoon(s):	*C08 Never leave your laptop unattended*, *C10 Internet of things*

In de modules over dit thema leggen we uit hoe men op een juiste manier met mobiele apparaten omgaat en hoe men zorgt voor adequate beveiliging van deze apparaten? Aanvullend kan je:

- Het beleid over het gebruik van mobiele apparatuur communiceren, zoals:
  - Niet toegestaan om apparatuur onbeheerd achter te laten.
  - Welke apparatuur mag gebruikt worden en voor welk doel.
  - Of het gebruik van mobiele datadragers (USB-sticks) is toegestaan.
- Communiceren hoe het wifi-netwerk voor gasten gebruikt mag worden.

7. Veilige werkplek

Modules over dit thema:	*T11, T12, T13, T19, T22, T38, T46, T51*
Poster(s):	*P06 Lock your screen*
Cartoon(s):	*C06 Lock your screen*

In de modules over dit thema vertellen we hoe men bijdraagt aan een veilige werkplek, waarin zorgvuldig wordt omgegaan met informatie. Aanvullend kan je:

- Het beleid over de veilige werkplek communiceren:
  - Wat wordt er van men verwacht op het gebied van clean desk.
  - Wat wordt er van men verwacht op het gebied van het vergrendelen van het scherm.
  - Wat wordt er van men verwacht als het gaat om back-ups en updates.

8. Social engineering

Modules over dit thema:	*T14, T20, T26, T29, T39*
Poster(s):	*P05 Nothing is what it seems*, *P07 Voice phishing*
Cartoon(s):	*C07 Social engineering*

In de modules over dit thema behandelen we alles over diverse vormen van social engineering, zoals ongewenste bezoekers en telefonisch phishing. Aanvullend kan je:

- Communiceren wat het bezoekersbeleid is binnen de organisatie:
  - Moeten bezoekers een zichtbare bezoekersbadge dragen?
  - Dienen bezoekers zich altijd vooraf aan te melden?
  - Dienen bezoekers wel of niet begeleid worden?
- Een social engineering onderzoek laten uitvoeren, zoals een telefonisch phishing onderzoek of mystery guest bezoek.
- De resultaten van een uitgevoerd social engineering onderzoek delen of laten presenteren tijdens een interactieve sessie.