
Goede Doelen
Nederland
Brancheorganisatie

Goede Doelen Nederland
Brancheorganisatie

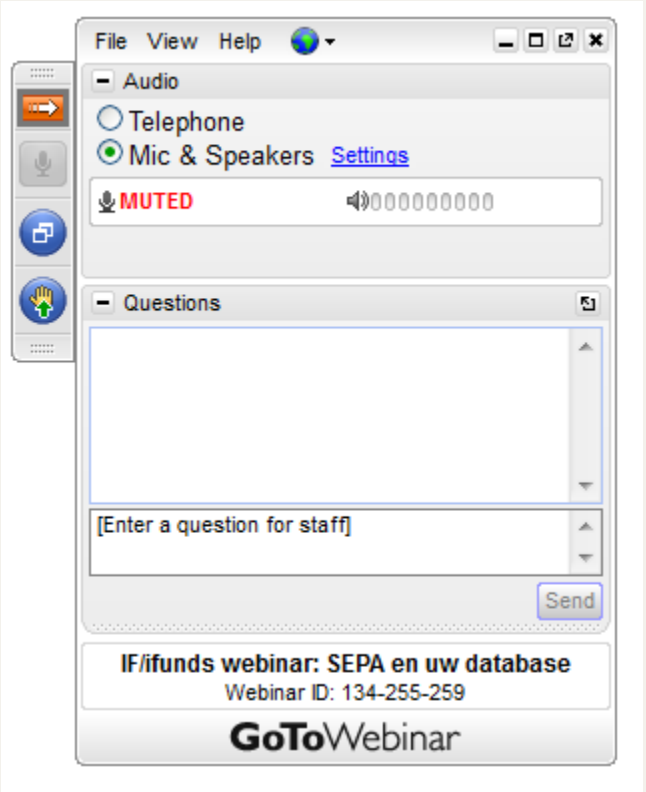
Webinar:

Cybersecurity voor goede doelen: trends, uitdagingen en maatregelen

22 juni 2023

Goede Doelen Nederland
Brancheorganisatie

Hoe volg je dit webinar?



Onze collega's van de service desk helpen je graag:

Marijn Onwezen via marijn.onwezen@ifunds.nl

Ondervind je tijdens het webinar technische problemen? Meld het ons via de chat-functie.

Speciale dank gaat uit naar: ifunds nonprofit CRM solutions

Goede Doelen Nederland
Brancheorganisatie

Spelregels

- Duur: 10.00 – 11.00 uur
- Vragen: stel ze via de chat-functie
- Opname: je ontvangt morgen een mail met de link naar de opname en de presentatie(s)
- Enquête: ontvang je direct na afloop; vul deze a.u.b. in!

Goede Doelen Nederland
Brancheorganisatie

Wie zijn wij?

Denise van Holstein

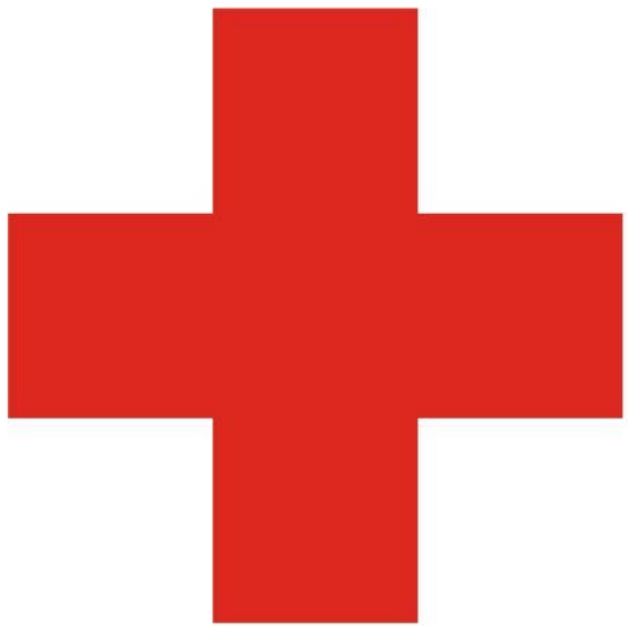
Cyber Security Advisor van *Het Rode Kruis*

Ed van Velzen

IT Manager van *Amnesty International Nederland*

Willem Visser (moderator)

Directeur van onderzoeksbureau *Effectmeting*



Rode
Kruis

Cyber Security Trends

Denise van Holstein – Cyber Security Adviseur Rode Kruis Nederland

Rode Kruis

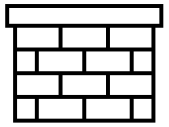
Inhoud

- Wat is hacken?
- Trends
- Uitdagingen voor NGO’s
- Meest voorkomende aanvallen
  - Social Engineering
  - Menselijke fouten
- Voorkomen is beter dan genezen

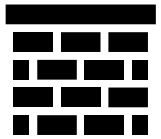
Rode Kruis

Hacken

Wat is het eigenlijk?



Kwetsbaarheid



Misbruik

“Het identificeren en uitbuiten van kwetsbaarheden in een computer systeem of netwerk met het doel om ongeautoriseerde toegang te krijgen tot persoonsgegevens of gevoelige informatie van organisaties”.

Rode Kruis

Trends

Cyber Security Trends die gevaarlijk zijn voor NGO’s

- Van “if” naar “when”
- Gijzelsoftware met drievoudige afpersing
- RaaS
- Zero-Day aanvallen
- Migratie naar de Cloud
- Polarisatie en internationale conflicten

Rode Kruis

Uitdagingen

De grootste uitdagingen voor NGO’s

- Het gebruik van IoT’s
- De opkomst van AI
- Menselijke fouten
- Social Engineering

Rode Kruis

Meest voorkomende aanvallen

Social engineering

Het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.

Zowel fysiek als digitaal

- Phishing, Spear Phishing, Vishing
- Baiting
- Scareware
- Catfishing
- Tailgating, Piggybacking

Rode Kruis

Meest voorkomende aanvallen

Menselijke fouten

88% van de data incidenten worden veroorzaakt door menselijke fouten

Rode Kruis

Voorkomen is beter dan genezen

Voorkomen

- Bewustwording: nieuwe én bestaande medewerkers
- Aanvalssimulatie (phishing / disaster recovery)
- Risicoanalyses: weet waar de gaten zitten
- Beleid en processen
- Incident Response Plan

Rode Kruis

Voorkomen is beter dan genezen

Wat doe je als het mis gaat?

Crisis communicatie:

- **Plan vooruit:** denk na over scenario's en een gepaste reactie.
- **Handel snel:** erken een crisissituatie onmiddellijk. Zo minimaliseer je geruchten en laat je weten dat je de regie in handen hebt.
- **Wees verantwoord transparant:** neem verantwoordelijkheid en vertel de waarheid.

Never waste a good crisis!

Rode Kruis

Handige Tips

Templates, achtergrond informatie en inspiratie

- Digital Trust Centre (DTC): Stappenplan risicoanalyse
- Nationaal Cyber Security Centrum (NCSC): Basis maatregelen
- De Nederlandse Bank (DNB): Beleid en maatregelen
- ENISA (EU): Maturity Assessment Tool
- Cyberpilot: Bewustwordingsposters (Privacy & Security)
- MITRE Attack Framework
- The Cyber Security Hub - LinkedIn

Rode Kruis