Voorbereiding op een Cyberaanval

✓ Print deze checklist

BEWUSTZIJN EN DIGITALE VEILIGHEID

- Begrijp de potentiële dreigingen van cyberaanvallen en hun gevolgen.
- Zorg ervoor dat alle software op je apparaten up-to-date is om beveiligingslekken te dichten.
- Gebruik sterke, unieke wachtwoorden voor al je accounts en activeer tweefactorauthenticatie waar mogelijk.
- Maak regelmatig back-ups van belangrijke gegevens en bewaar deze op externe harde schijven of in de cloud.

FYSIEKE VOORBEREIDINGEN EN NOODPLANNEN

- Stel een communicatieplan op voor je gezin of huisgenoten voor het geval standaard communicatiemiddelen uitvallen.
- Creëer een noodpakket met essentiële items zoals water, niet-bederfelijk voedsel, basismedicijnen, een eerstehulpkit, zaklampen, extra batterijen, een handmatige blikopener, contant geld, en kopieën van belangrijke documenten.
- Leer basis eerste hulp vaardigheden.
- Investeer in alternatieve energiebronnen zoals zonnepanelen of een noodgenerator voor essentiële energiebehoeften.
- Verzamel fysieke kaarten van je omgeving en oefen met het gebruik ervan voor navigatie zonder GPS.
- Bespreek met je gezin of huisgenoten een verzamelplan voor tijdens een cyberaanval.

MAATSCHAPPELIJKE VOORBEREIDING

- Werk samen met je buren en lokale gemeenschap om een netwerk van ondersteuning en middelen op te bouwen.
- Deel kennis over cyberveiligheid binnen je gemeenschap.

ACTIES TIJDENS EEN CYBERAANVAL

- Schakel indien mogelijk over op vooraf geplande noodcommunicatiemiddelen.

- Evalueer snel de omvang en het type cyberaanval en pas je acties dienovereenkomstig aan.
- Volg officiële richtlijnen en instructies van overheidsinstanties en cybersecurity-experts.

HERSTEL EN REFLECTIE NA EEN AANVAL

- Beoordeel de schade en start het herstelproces voor aangetaste systemen.
- Identificeer welke voorbereidingen effectief waren en welke verbeterd kunnen worden.

OPBOUWEN VAN LANGETERMIJN VEERKRACHT

- Blijf op de hoogte van de nieuwste cyberveiligheidstrends en -praktijken door voortdurende educatie.
- Versterk de samenwerking binnen je gemeenschap om samen sterker te staan tegen toekomstige dreigingen.
- Moedig beleidsmakers aan om te investeren in cyberveiligheid en publieke bewustwordingscampagnes.

Deze checklist dient als een uitgebreide gids om je voor te bereiden op, te handelen tijdens, en te herstellen van een cyberaanval, en om op de lange termijn veerkracht tegen dergelijke dreigingen op te bouwen.

Cybercrimeinfo.nl (ccinfo.nl)
De bibliotheek voor de bestrijding van digitale criminaliteit
www.ccinfo.nl