Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Digitale veiligheid van politieke partijen

24 februari 2022

NCTV

Digitale veiligheid

- De gemeenteraadsverkiezingen 2022 komen er aan! Het is daarom extra belangrijk stil te staan bij de digitale veiligheid. Immers, ook politieke partijen kunnen doelwit worden van bijvoorbeeld phishing, ransomware, oplichting en spam. Zorg er daarom voor dat de digitale veiligheid van uw partij op orde is. Onderstaande vijf video’s lichten acties toe die u zelf kunt nemen om uw veiligheid in de basis op orde te brengen.

1. Zorg voor veilige wachtwoorden

- Je smartphone, computer en accounts bescherm je met een wachtwoord. Het gebruik van wachtwoordkluizen kan het gebruik van veilige wachtwoorden stimuleren. Vermijd het delen van accounts en wachtwoorden. Zorg dus voor veilige wachtwoorden . Gebruik waar het kan tweestapsverificatie.

https://www.youtube.com/watch?v=6VLJveBafyk

2. Voer je updates uit

- Door regelmatig de updates van je slimme apparaten uit te voeren, zorg je ervoor dat deze veilig blijven. Door middel van updates zorgen fabrikanten ervoor dat de beveiliging van je apparaten altijd op orde zijn. Vergeet hierbij de router niet; die vormt de voordeur naar het internet.

https://www.youtube.com/watch?v=vjUA4z5B8eE

3. Gebruik een virusscan

- Cybercriminelen kunnen kwaadaardige software op computers of telefoons installeren via links of bijlages in e-mails, apps, SMS en links op websites. Een virusscanner controleert je apparaten op onder andere virussen, malware, en gecompromitteerde apps. Je hebt gratis en betaalde virusscanners. Zoek er één die bij jou past.

https://www.youtube.com/watch?v=hrSsLNVj13M

4. Maak regelmatig een back-up

- Als je gehackt wordt, kun je alles kwijt zijn. Maak daarom voor de zekerheid een kopie van je bestanden, zodat je in het geval van ransomware je nog altijd bij je bestanden kunt. Belangrijk hierbij is dat de back-up losgekoppeld is van het apparaat. Anders kan een virus ook de back-up besmetten, en heb je er niks aan. Het maken van een back-up werkt verschillend voor verschillende apparaten.

https://www.youtube.com/watch?v=-Sk6TqY6JZs

5. Voorkom phishing

- Een valse link kan je leiden naar een website die veilig lijkt, maar dat eigenlijk niet is. Op zo’n valse website vragen criminelen je inloggegevens, zoals je wachtwoord en gebruikersnaam. Als je die weggeeft, kunnen criminelen inloggen op jouw account, en dat kan je veel geld kosten. Als je een gevaarlijke bijlage downloadt, kan dit schadelijk zijn.

https://www.youtube.com/watch?v=emg5I7FS3WY

6. Desinformatie

- Naast de digitale veiligheid van uw organisatie is het belangrijk om alert te zijn op desinformatie en nepnieuws. Dit is onware of onnauwkeurige informatie die expres wordt gemaakt en verspreid om geld te verdienen of om iemand, een groep mensen, een organisatie of een land te beschadigen. Controleer daarom altijd of een bericht klopt:

- Check welke bron is gebruikt en of die betrouwbaar is
- Check de volledige inhoud van het bericht
- Check waar het bericht vandaan komt, wees kritisch
- Check waar de foto’s en video’s vandaan komen

Lees ook meer tips om desinformatie en nepnieuws te herkennen.

Aanvullende publicaties

- Wat te doen bij een cyberincident? (Digital Trust Center)
- In 10 stappen starten met cybersecurity (Digital Trust Center)
- Handreiking Cybersecuritymaatregelen (National Cyber Security Center)
- Kennisproducten van de informatiebeveiligingsdienst gemeenten (IBD)
- Handreiking desinformatie: meerdere opties om er verantwoord mee om te gaan (Rijksoverheid.nl)
- Meer informatie en praktische tips zijn te vinden op: www.veiliginternetten.nl en www.digitaltrustcenter.nl.