Richtlijn met tips en checklist

Fraudeurs en criminelen weten de kerk inmiddels (ook) te vinden

Regelmatig bereiken ons berichten van kerken die slachtoffer zijn geworden van fraude via internet of e-mail. Vooral in periodes die anders zijn dan normaal, zoals bijvoorbeeld tijdens de zomervakantie en rondom de feestdagen, neemt het aantal fraudegevallen toe. Door de komst van AI hebben fraudeurs online een nog betere toolkit in handen om nog echter over te komen, door het gebruik van stemmen, video en niet meer van echt te onderscheiden documenten. Wat kun je als kerk doen om te voorkomen dat je slachtoffer wordt van online fraudeurs?

TEKST JOOST SCHELLING **BEELD** ADOBE STOCK

Met input van verschillende VKB-partners (Marsh, Bestuursgemak en SKG Gouda) hebben we een beleidsrichtlijn met checklist opgesteld, die is bedoeld voor kerkenraden, colleges van kerkrentmeesters en diakenen om fraude via internet, e-mail en door middel van AI te voorkomen. Het beleid geldt voor alle communicatie en financiële processen binnen de gemeente.

Veelvoorkomende vormen van fraude

1. Bankhelpdeskfraude
Nepbankmedewerkers bellen over 'problemen' met je rekening. Ze maken je bang en zetten je onder druk om persoonlijke informatie of bankgegevens te delen en betalingen uit te voeren. Ook kunnen oplichters aan de deur komen om betaalpassen op te halen. Soms vragen ze zelfs om andere waardevolle spullen. Hang op en geef géén bankproducten of waardevolle spullen mee. Bel 112.

2. Investeringsfraude
Via social media lokken oplichters met bekende namen. Ze willen dat je investeert in nepbeleggingen – met gegarandeerde winst. De schade kan oplopen tot tienduizenden euro's.

3. Factuurfraude
Valse rekeningen van overheid, energieleverancier of telefoonmaatschappij. Check altijd of je echt een rekening hebt openstaan en wie deze heeft gestuurd.

4. Emotionele fraude (onder andere dating of situaties van extreme armoede)
Oplichters maken online nepprofielen aan en bouwen eerst vertrouwen op. Daarna vragen ze om geld. Ze verzinnen vaak noodsituaties en spelen zo in op je gevoel. Maak nooit geld over naar iemand die je niet in het echt hebt ontmoet.

5. Voorschotfraude
Criminelen beloven geld, maar je moet eerst 'kosten' betalen. Ze gebruiken officieel uitziende documenten. Maar hoe echt is die prijs uit de loterij, erfenis of lening?

6. Identiteitsfraude
Criminelen maken een profiel van de predikant of bestuurder aan en gebruiken bijna identieke e-mailadressen. Vervolgens vragen ze om (snel) geld over te maken. Vaak klopt er aan het e-mailadres net iets niet: de punt staat ergens anders, na de @ staat een andere provider, etcetera. Let dus op: volg niet de omschrijving van het e-mailadres, maar bekijk altijd goed het e-mailadres zelf, zeker als je twijfelt aan de echtheid van het bericht.

7. Fraude door middel van AI
Oplichters maken in toenemende mate gebruik van AI-gegenereerde berichten (via e-mail en telefoon) die foutloos en overtuigend lijken en helaas ook steeds beter worden. De verwachting is dat deze vorm steeds echter zal worden (met beeld of spraak van de identiteit van degene die ze aannemen).

Preventieve maatregelen

De maatregelen die je kunt treffen om fraude via e-mail en internet te voorkomen, zijn te verdelen in technische en organisatorische maatregelen:

Technische maatregelen:
- Gebruik multi-factor authenticatie (MFA) voor e-mail en financiële accounts, de zogenaamde tweestapsautorisatie (wachtwoord in combinatie met een authenticatorapp of sms-bericht).
- Stel SPF, DKIM en DMARC in om e-mailspoofing tegen te gaan.[1]
- Gebruik sterke wachtwoorden en een password manager.
- Vernieuw je wachtwoorden regelmatig.

Organisatorische maatregelen:
- Voer het vier-ogen-principe in voor betalingen.
- Bespreek regelmatig in de vergadering het betaalprotocol door: wie mag tot welk bedrag welke betalingen zelfstandig klaarzetten?
- Accepteer geen betaalverzoeken via e-mail zonder verificatie via een tweede kanaal. Let op: word je meteen gebeld door een bestuurder? Stel voor dat je hem/haar zelf terugbelt over het verzoek.
- Organiseer een periodieke phishing-training voor kerkenraad en vrijwilligers.
- Overweeg het afsluiten van een cyberrisico-verzekering: www.kerkrentmeester.nl/home/vkb-verzekeringen/verzekeringsoplossingen/cyberrisks/

Incidentprotocol

Volg bij een vermoeden van fraude het volgende incidentprotocol:
1. Meld direct bij de penningmeester van het college en voorzitter kerkenraad.
2. Waarschuw gemeenteleden via website en nieuwsbrief voor deze fraude.
3. Neem contact op met je bank via de helpdeskfraude. Loopt het betalingsverkeer via SKG Gouda, dan kun je contact opnemen via het algemene telefoonnummer van SKG, 0182 - 588 000 om fraude(pogingen) te melden.
4. Evalueer en verbeter beveiligingsmaatregelen. Neem indien nodig een deskundige in de arm.

[1] *SPF (Sender Policy Framework): Controleert of een e-mail afkomstig is van een server die gemachtigd is om namens jouw domein te verzenden. Je stelt in je DNS-records vast welke mailservers mogen mailen voor jouw domein. DKIM (DomainKeys Identified Mail): Voegt een digitale handtekening toe aan uitgaande e-mails. Ontvangers kunnen controleren of de inhoud van de e-mail onderweg niet is aangepast en of deze echt van jouw domein komt. DMARC (Domain-based Message Authentication, Reporting & Conformance): Combineert SPF en DKIM en bepaalt wat er gebeurt als een e-mail niet door deze controles komt (bijvoorbeeld weigeren, markeren als spam). Geeft ook rapportages over pogingen tot spoofing.*

Checklist

Voorkomen van internet, e-mail- en AI-fraude

1. Beveiliging van communicatie

- ☐ Gebruik functionele e-mailadressen (bijvoorbeeld penningmeester@kerknaam.nl) in plaats van privé-adressen.
- ☐ Publiceer geen persoonlijke e-mailadressen van kerkenraad of predikant op de website.
- ☐ Controleer regelmatig of de domeinnaam van de kerk correct wordt gebruikt (voorkom spoofing).

2. Technische maatregelen

- ☐ Activeer multi-factor authenticatie (MFA) op alle e-mail- en financiële accounts.
- ☐ Stel SPF, DKIM en DMARC in om e-mailspoofing tegen te gaan.
- ☐ Maak, als je met meerdere personen/gezinsleden op dezelfde computer werkt, eigen profielen aan, in plaats van het werken onder hetzelfde account.
- ☐ Gebruik sterke wachtwoorden en een password manager, zoals Proton Pass of Bitwarden.
- ☐ Zorg voor up-to-date antivirussoftware en beveiligingsupdates.

3. Betaalprocedures

- ☐ Voer altijd het vier-ogen-principe in: geen betaling zonder goedkeuring van minimaal twee personen.
- ☐ Leg vast dat geen betaalverzoeken via e-mail worden uitgevoerd zonder verificatie via een tweede kanaal (telefoon of app).
- ☐ Gebruik een vaste betaalstructuur: de predikant vraagt nooit rechtstreeks om geld.
- ☐ Hoeveel haast kan er werkelijk bij een betaling zijn? Gun jezelf als penningmeester de rust van 48 uur tot een betaling.

4. Bewustwording en training

- ☐ Informeer gemeenteleden: predikanten vragen nooit via e-mail om geld of cadeaubonnen.
- ☐ Leer signalen herkennen: formele toon, spoedverzoeken, afwijkende ondertekening, maar ook: vakantieperiodes. Juist als dagen en weken anders lopen, ben je vatbaarder voor het afwijken van de reguliere procedures.
- ☐ Organiseer periodieke phishing-training voor kerkenraad en vrijwilligers.
- ☐ Vertrouw je het niet: ga offline. Ga bij de betreffende bestuurder of voorganger zelf langs en neem via een ander kanaal contact met hem/haar op.

5. AI-gerelateerde risico's

- ☐ Wees alert op perfecte taal en foutloze e-mails (AI-gegenereerd).
- ☐ Controleer altijd via een tweede kanaal bij twijfel.
- ☐ Overweeg een verificatiecode-systeem voor financiële verzoeken.

6. Incidentprotocol

- ☐ Stel een meldpunt binnen het college van kerkrentmeesters in voor verdachte e-mails.
- ☐ Loopt het betalingsverkeer via SKG Gouda, dan kun je contact opnemen via het algemene telefoonnummer van SKG, 0182 - 588 000 om fraude(pogingen) te melden.
- ☐ Documenteer en rapporteer pogingen tot fraude bij de kerkelijke instanties, zoals de PKN en de VKB.
- ☐ Informeer direct betrokkenen en update beveiligingsmaatregelen.