Internetcriminelen geven zich opnieuw uit voor pastorale beroepskrachten

Internetcriminelen geven zich in e-mails uit voor pastorale beroepskrachten in een poging om de ontvanger aan te sporen geld over te maken. Na eerdere incidenten in de bisdommen Breda en Den Bosch is er recent opnieuw een dergelijk incident gemeld. Het is goed om in de parochie aandacht te vragen voor dergelijke incidenten, zodat zowel medewerkers, vrijwilligers als parochianen alert blijven.

Wat gebeurt er?

Criminelen maken gebruik van bijvoorbeeld Gmail om een nieuw e-mailadres aan te maken dat er geloofwaardig uitziet. Vanuit dit e-mailadres versturen ze een bericht waarin ze bijvoorbeeld zeggen de pastoor te zijn. Het nep e-mailadres wijkt vaak maar heel weinig af van het echte e-mailadres van de pastoor. Tips over hoe u een nep e-mail kunt herkennen leest u hier.

Beveiliging en alertheid

Het up-to-date houden van de beveiliging van e-mailboxen en e-mailadressen is belangrijk. Toch zijn niet alle vormen van fraude te voorkomen. Daarom is het belangrijk dat medewerkers, vrijwilligers en parochianen alert blijven op mogelijke fraude door het gebruik van nep-e-mails. U kunt via uw website of parochieblad bijvoorbeeld hiervoor aandacht vragen. Duidelijkheid helpt hierbij. Meld de parochianen bijvoorbeeld dat u nooit via een e-mail van de pastoor om geld vraagt en dat een mail met die boodschap dus altijd nep is.

Ook kunt u aangeven bij wie parochianen terecht kunnen in geval van twijfel over een e-mail. Meer informatie over nepmails is te vinden op de speciale website van de Rijksoverheid.

Is er sprake van een datalek?

Als u een phishing mail ontvangt en niet op een link, knop of bijlage in het bericht hebt geklikt, is het niet waarschijnlijk dat deze e-mail schade heeft toegebracht. Het enkele feit dat u de phishing mail hebt ontvangen en geopend, is nog geen beveiligingsincident of datalek. Het is wel belangrijk dat u de phishing mail direct verwijdert uit uw mailbox en postvak met ‘verwijderde berichten’. Zo kunnen andere personen die toegang tot de mailbox hebben, zich niet meer vergissen.

Wat als u wel op een link in een phishing mail hebt geklikt? In dat geval is er sprake van een beveiligingsincident. De contactpersoon die in uw parochie verantwoordelijk is voor de AVG en de veiligheid van persoonsgegevens, kan in dat geval samen met een systeembeheerder onderzoeken wat er aan de hand is.