Zo veilig is NGKdePelgrim.nl

Je persoonlijke gegevens moeten veilig zijn. We doen er daarom alles aan om het Intranet van NGK de Pelgrim en het online-ledenadministratiesysteem zo veilig mogelijk te maken. En je kunt natuurlijk zelf ook de nodige maatregelen treffen.

Wij nemen beveiliging heel serieus

We doen alles om onze website en het bijbehorende Intranet zo veilig mogelijk te maken:

Beveiligde verbinding

Als je inlogt in Intranet op onze website, ontstaat er een beveiligde verbinding tussen onze computer en jouw computer. Of met je mobiel of tablet natuurlijk. Wij gebruiken hiervoor de beveiligingstechniek Transport Layer Security (TLS) versie 1.2. TLS is als beveiligingsstandaard de opvolger van Secure Sockets Layer (SSL) en is bedoeld om op internet persoonlijke informatie te beveiligen. Als de TLS-verbinding opstart, zie je een gesloten slotje in je browser. TLS zorgt ervoor dat je er als bezoeker van de website zeker van kunt zijn dat de gevonden server inderdaad degene is die hij zegt te zijn (onze website dus). Bovendien wordt de communicatie tussen de server/website en de bezoeker versleuteld met een 128-bits versleuteling. Hiermee zijn jouw gebruikersnaam en wachtwoord veilig bij het inloggen.

Je wordt vanzelf uitgelogd

Het zou niet veilig zijn als je nog uren ingelogd blijft als je vergeet uit te loggen. Daarom log je automatisch uit als je 5 minuten niets hebt gedaan. Je kunt natuurlijk altijd weer inloggen om verder te gaan.

We blokkeren soms een gebruikersnaam en wachtwoord

Als het binnen 5 minuten 10 keer is mislukt om in te loggen, blokkeren we tijdelijk je account. Dat is misschien vervelend als het een foutje was, maar wel zo veilig tegen cybercriminelen. Ook wordt jouw IP-adres (het adres van de computer waarmee je probeert in te loggen) in een logbestand genoteerd. Na een half uur wordt de blokkade opgeheven en kun je opnieuw inloggen, met opnieuw maximaal 10 pogingen. Daarnaast worden inlogpogingen met bepaalde standaard gebruikersnamen zoals ‘admin’ direct geblokkeerd en de computer vanaf welke deze inlogpoging wordt ondernomen, wordt meteen geblokkeerd en heeft daarmee geen toegang meer tot de website.

Externen mogen geen profielinformatie opvragen

Niet-leden en zogenaamde ‘bots’ (kleine programmaatjes die het internet afstruinen op zoek naar informatie) hebben geen toegang tot de leden-informatie die in de profielen zijn opgenomen. We hebben de toegang m.b.v. meerdere beveiligingsmethoden afgegrendeld, onder meer door bescherming tegen zgn. ‘brute force attacks’ en ‘auto enumeration’ en het dichtzetten van ‘directory listing’ op de server. We gebruiken een uitgebreide Firewall waarbij zoveel mogelijk beveiligingsmaatregelen aan staan.

Verplicht sterk wachtwoord voor alle gebruikers

Onze beveiliging gaat na of een wachtwoord van een bepaalde minimumlengte is en dat het niet overeenkomt met bekende, simpele wachtwoorden. Via een puntensysteem wordt de sterkte van het wachtwoord berekend. Daarbij wordt bijvoorbeeld gekeken naar of er naast gewone kleine letters ook minstens een getal, een hoofdletter en een speciaal teken in het wachtwoord staat. Als het gekozen wachtwoord niet voldoet, zal de website de gebruiker vragen een moeilijker wachtwoord te kiezen.

Registratie van nieuwe leden wordt handmatig gecheckt

Het is niet mogelijk voor niet-leden om automatisch een nieuwe gebruikersaccount voor de website aan te maken zonder dat de webbeheerder dit goedkeurt. In feite staat de hele registratie-optie voor externen uit en maakt alleen de webbeheerder nieuwe accounts aan.

Wat kun je zelf doen aan de veiligheid?

Voor veilig internetten kun je zelf ook maatregelen treffen:

Ga voorzichtig om met je persoonlijke gegevens

Jouw Intranet login-gegevens op ngkdepelgrim.nl zijn - voor volwassenen, tieners en kinderen met een eigen emailadres - strikt persoonlijk. Geef daarom nooit je gebruikersnaam en wachtwoord aan iemand anders. Niet via e-mail, niet als je met ons belt, gewoon nooit. Let ook op dat er niemand meekijkt als je je wachtwoord intikt. Als je je inloggegevens toch aan iemand geeft, ben je zelf aansprakelijk voor de gevolgen van eventueel misbruik. Voor kinderen en voor tieners geldt dat de ouders medeverantwoordelijk zijn en hun kind begeleiden bij het gebruik van het Intranet.

Laat je computer nooit onbewaakt achter

Loop je weg bij je computer, zorg dan dat je je computer vergrendeld of, liever nog, uitlogt.

Verander regelmatig je wachtwoord

Het is goed om ieder half jaar je wachtwoord te wijzigen. En kies dan niet voor iets makkelijks als ‘wachtwoord’ of ‘123456’. Je wachtwoord moet minimaal bestaan uit:

- 8 karakters
- 1 cijfer, liefst meer
- 1 hoofdletter
- 1 speciaal teken zoals ‘_ & !’

Het is niet slim om gebruik te maken van browsers die je gebruikersnaam en wachtwoord op je computer opslaan. En maak liever geen gebruik van automatische wachtwoordhulpen (auto-aanvullen).

Gebruik de nieuwste versie van je internetbrowser

Controleer regelmatig of je de nieuwste versie van je internetbrowser hebt. Die is altijd beter beveiligd dan oudere versies. Kijk op de website van Internet Explorer, Chrome, Edge of Firefox voor de nieuwste versie.

Controleer of je een beveiligde verbinding hebt

Als je de website van NGK de Pelgrim bezoekt, zie je een slotje vooraan in de adresbalk van je browser verschijnen. Dat wil zeggen dat de verbinding beveiligd is. Klik je op dit slotje, dan zie je ons certificaat, geverifieerd door COMODO Ca Limited.

Installeer anti-virussoftware en voer scans uit

Maak gebruik van anti-virussoftware. En dan moet het programma natuurlijk ook bijgewerkt en actief zijn. Doe regelmatig een scan om te zien of er nog virussen op je computer staan.

Download en installeer geen illegale en onbekende software

Soms krijg je in een e-mail of op een website een onbekend programma aangeboden. Installeer die niet, want ze kunnen ook dingen veranderen in bestaande programma’s. Dat brengt risico’s met zich mee.