*Let op! Als je teksten uit dit document wilt knippen/plakken naar de tekstverwerker in het Burgernet portaal, doe dat dan VIA het kladblok. Op deze manier blijven de spaties in het bericht juist in stand!*

**Digitale criminaliteit: ‘dat overkomt mij toch niet!’***Beluister de podcast*

U hoort het uzelf waarschijnlijk zeggen; phishing? Whatsapp-fraude? Dat overkomt mij niet.

Maar de manieren waarop cybercriminelen werken, wisselen snel en vaak en hun methodes worden steeds geavanceerder. Terwijl alle vormen van criminaliteit dalen, stijgt cybercriminaliteit juist. Bijna 2 miljoen mensen worden jaarlijks slachtoffer. In Midden-Nederland zien we dat veel slachtoffers tussen de 40 en 60 jaar zijn. Gemiddeld raken ze maar liefst €1500,- kwijt. Bij slachtoffers van 60 jaar en ouder is de schade gemiddeld zelfs meer dan €5000,-. En de impact is veel groter dan alleen een geldbedrag.

*Kruip in het hoofd van een slachtoffer*

Slachtoffers schamen zich dat het hen is overkomen en kunnen er letterlijk wakker van liggen. We delen daarom een unieke podcastserie over cybercrime waarin slachtoffers hun verhaal doen. Met de podcast ‘Digitaal Beroofd’ kruip je als luisteraar in het hoofd van een slachtoffer en ontdek je hoe daders te werk gaan. Maar ook: hoe je jezelf en je omgeving kunt beschermen en wat politie en OM in onze regio doen om deze internetcriminelen op sporen.

De podcast is te beluisteren via je eigen podcastkanaal of via deze [link](https://veiligheidscoalitie.nl/digitaalberoofd)

**Herkent u de signalen van helpdeskfraude?**

U denkt via internet het telefoonnummer gevonden te hebben van een ‘Nederlandse klantenservice’? Of u krijgt een pop-up-berichtje op uw computer, dat vermeldt dat u contact op moet nemen met een helpdesk? Digitale fraude neemt in Midden-Nederland ook in 2022 weer sterk toe. Vooral helpdeskfraude komt veel voor. Ook u kunt dus met oplichters te maken krijgen.

*Op slinkse wijze toegang tot uw computer*

De oplichters bieden allerlei oplossingen aan. Allereerst zeggen ze dat het nodig is om naar een bepaalde site te gaan om software te downloaden. Met die software zouden ze op afstand uw ‘probleem’ kunnen oplossen. Als u hierop ingaat, hebben criminelen toegang tot uw computer. Deze software kan criminelen uiteindelijk toegang geven tot uw online bankomgeving. Zo sluizen ze geld weg naar hun eigen rekening, zonder dat u dit in de gaten heeft. Ook is het mogelijk dat u naar frauduleuze websites wordt geleid. Hier wordt naar uw persoonlijke of financiële informatie gevraagd, zoals uw creditcardgegevens.

*Herken de signalen en voorkom dat u slachtoffer wordt:*

* Krijgt u een Engelstalige helpdeskmedewerker aan de lijn? Hang op! Softwarebedrijven bellen u nooit en vragen ook nooit naar uw beveiligingsinstellingen en/of wachtwoorden.
* Installeer nooit software op verzoek van de beller.
* Geef nooit toegang tot het meekijken in en het overnemen van de computer.
* Maak geen geld over op verzoek van de beller.
* Informeer uw familie, vrienden en kennissen over deze oplichting en waarschuw hen.
* Zorg dat uw computer up-to-date is
* Maak gebruik van een antivirusprogramma en een firewall.

Heeft u nog vragen over dit bericht? Neem dan contact op met [contactgegevens, bijvoorbeeld de afdeling veiligheid van de gemeente]