Digitale weerbaarheid | Podium

Gemeente kan burgers ondersteunen bij online veiligheid

7 december 2022

cybersecurity, gemeente, hacking, veiligheid

Burgers weten weinig over hoe zij hun online veiligheid kunnen vergroten en bij hen ontbreekt vaak het gevoel van urgentie om daadwerkelijk maatregelen te nemen. De gemeente kan burgers ondersteunen met informatiepunten en extra ondersteuning van kwetsbare groepen. Kenniscentrum Cybersecurity van de Haagse Hogeschool deed onderzoek bij twee gemeen

Vrijwel iedereen weet dat je verschillende wachtwoorden moet gebruiken. | Beeld: shutterstock

2,5 miljoen Nederlanders slachtoffer zijn geworden van online dreigingen. Deze dreigingen kunnen crimineel zijn (zoals online oplichting), niet crimineel maar wel opzettelijk (zoals cybervandalisme en cyberpesten), of onopzettelijke fouten (zoals per ongeluk een mailtje naar een verkeerde bestemming sturen).

> *Ongeveer 2,5 miljoen Nederlanders zijn in 2021 slachtoffer geworden van online dreigingen.*

Het bestuur van de Vereniging van Nederlandse Gemeenten (VNG) onderkent dat online veiligheid steeds belangrijker wordt en heeft het thema op de agenda gezet. Verscheidene gemeenten constateren dat online dreigingen een groeiend probleem zijn en noemen dit onderwerp als prioriteit in hun Integrale Veiligheidsplan. Vanuit het oogpunt van Openbare Orde en Veiligheid zien gemeenten een rol voor zichzelf in het beschermen van haar burgers tegen online dreigingen. Het is voor veel gemeenten echter nog onduidelijk hoe ze deze rol het beste in kunnen vullen. Om deze rol duidelijk te krijgen, is het van belang om eerst te kijken naar de burger zelf in relatie tot digitale veiligheid. In dit artikel kijken we naar het online gedrag van de burger, het slachtofferschap van online dreigingen, de kennis van online veiligheid en de houding ten opzichte van online veiligheid. Vanuit deze inzichten, in combinatie met suggesties van burgers, worden aanbevelingen gedaan over de rolinvulling van de gemeente.

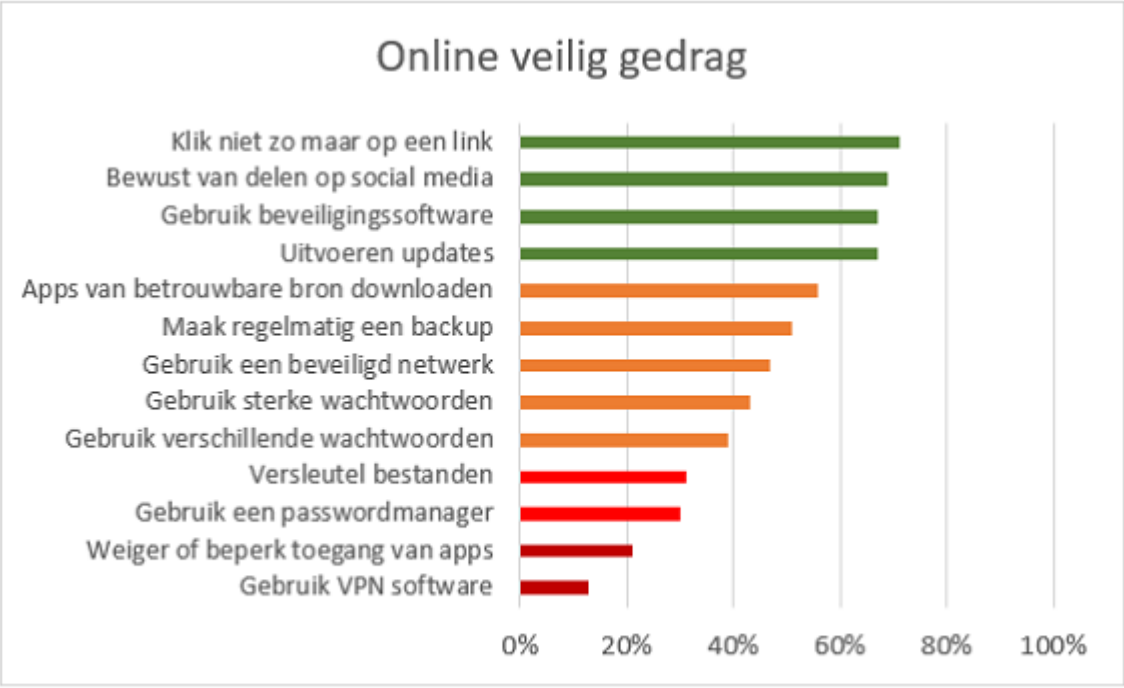
Onderzoek

Om dit in kaart te brengen, is onderzoek met behulp van een enquête gedaan bij een middelgrote gemeente (tussen de 50.000-100.000 inwoners) en een grote gemeente (100.000+ inwoners). Bij de middelgrote gemeente is de enquête via een app uitgezet, met een respons van 268 deelnemers. Bij de grote gemeente is de enquête uitgezet via een netwerk van buurtpreventiegroepen, met een respons van 127 deelnemers. De resultaten van de deelnemers uit deze twee gemeenten bleken vergelijkbaar te zijn en worden daarom samengevoegd behandeld. Door de wijze waarop de enquête is uitgezet, hebben weinig jongeren deelgenomen aan het onderzoek, waardoor de resultaten beperkt representatief zijn.

Gedrag

Iedereen kan slachtoffer worden van online dreigingen. Daarom is het nodig om daar maatregelen tegen te nemen. In eerste instantie speelt de burger zelf een grote rol speelt in diens eigen online veiligheid. Door geschikte maatregelen te treffen, ben je beter beschermd tegen online dreigingen en verklein je de kans om daar slachtoffer van te worden. In dit onderzoek wordt meer duidelijkheid verschaft over hoe (on)veilig het online gedrag van de burger is door in kaart te brengen welke maatregelen zoal worden getroffen.

deelnemers de rechten van apps beperkt. Maatregelen die maar door 1 op de 4 deelnemers worden getroffen, zijn het versleutelen van bestanden en het gebruik van een passwordmanager. Ongeveer 4 op de 10 deelnemers maakt gebruik van verschillende en sterkte wachtwoorden.

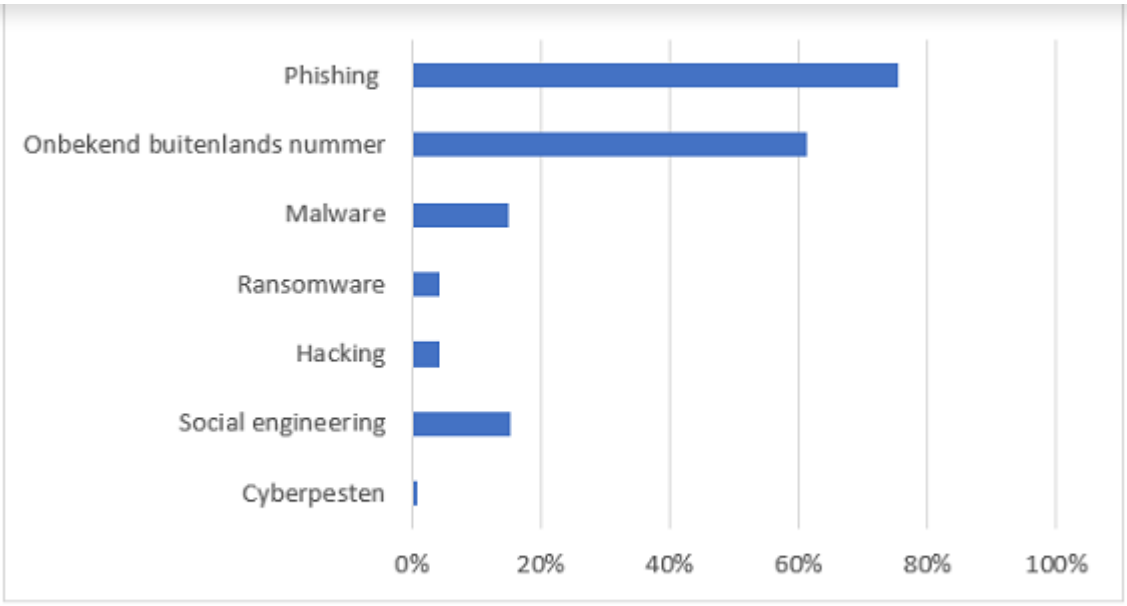


Figuur 1: Het percentage deelnemers dat een bepaalde maatregel treft.

De maatregelen die door ongeveer de helft van de deelnemers worden getroffen, zijn gebruik maken van een beveiligd netwerk, regelmatig een back-up maken en apps alleen van betrouwbare bron downloaden. Ten slotte zijn er ook maatregelen die door meer deelnemers worden getroffen, namelijk het uitvoeren van updates, gebruik van beveiligingssoftware, bewust zijn van het delen van informatie op sociale media en niet zomaar op een link klikken.
Al met al blijkt dat de burger over het algemeen nog te weinig doet voor de eigen online veiligheid en dat er veel ruimte voor verbetering is.

Slachtofferschap

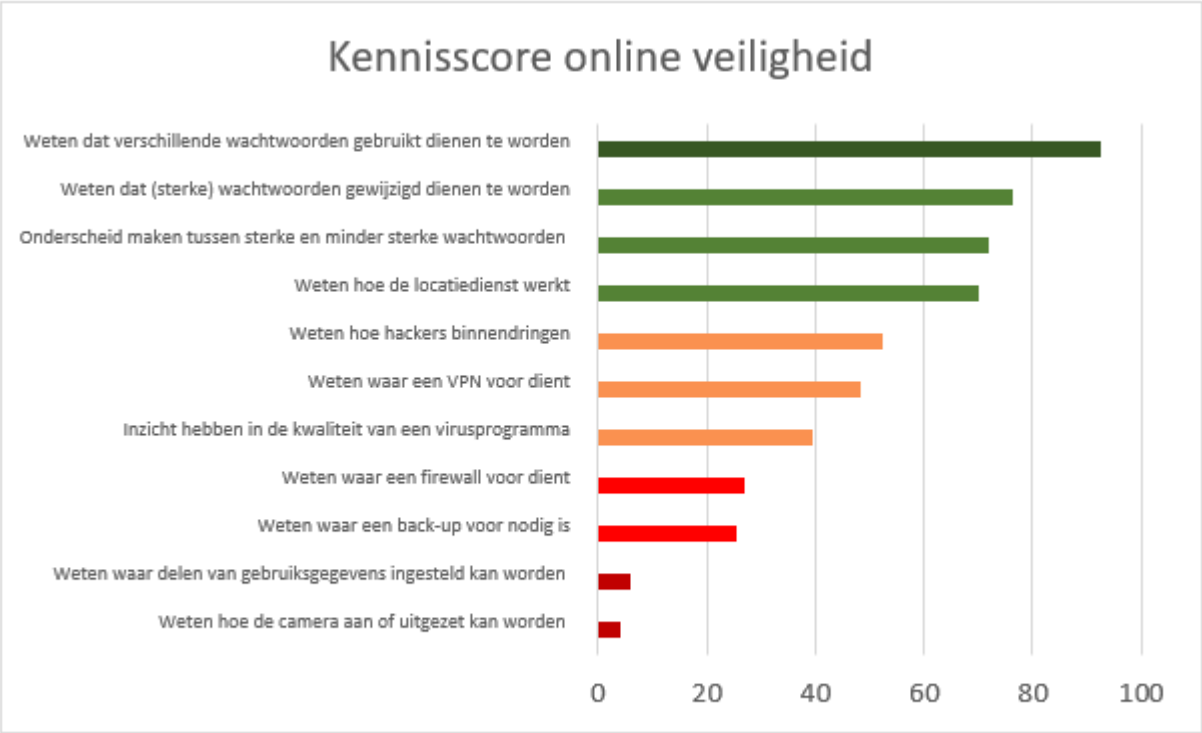
Het onveilige online gedrag is, wellicht in lijn met de verwachtingen, niet zonder gevolgen. Uit de resultaten van figuur 2 blijkt dat 9 op de 10 deelnemers het afgelopen jaar slachtoffer is geworden van online dreigingen. Meer dan 1 op de 5 ervaart hiervan negatieve gevolgen in termen van tijd en moeite.



Figuur 2: Het percentage deelnemers dat slachtoffer is geworden van een online dreiging in het afgelopen jaar.

- Meer dan 3 op de 4 deelnemers is slachtoffer geworden van phishing. Bij phishing wordt geprobeerd via misleidende e-mails vertrouwelijke informatie, zoals een bsn-nummer of het wachtwoord van internetbankieren, binnen te hengelen. Hiermee kan iemands rekening worden geplunderd.
- 3 op de 5 deelnemers is slachtoffer van geworden doordat gebeld werd door een onbekend nummer en dat terugbelden.
- 1 op de 7 deelnemers is slachtoffer geworden van computervirussen of andere malware. Dit is kwaadaardige software die gebruikt wordt om een computer te verstoren of gevoelige informatie te verzamelen.
- 1 op de 20 deelnemers is slachtoffer geworden van ransomware. Bij ransomware worden bestanden versleuteld en daardoor ontoegankelijk gemaakt. Dit kan grote gevolgen hebben voor het slachtoffer, zoals het verlies van toegang tot de mail en documenten zoals persoonlijke foto's. Na betaling van de ransom (=losgeld) wordt er in principe weer toegang gegeven.
- 1 op de 20 deelnemers is slachtoffer geworden van hacking, ook wel bekend als computervredebreuk. Dit is een inbraak of insluiping op een computer via het internet. Zo kunnen waardevolle gegevens in verkeerde handen vallen en worden doorverkocht aan derden. Ook kunnen gegevens worden aangepast of gebruikt om geld weg te sluizen.
- 1 op de 6 deelnemers heeft gemerkt dat iemand bij hun aan het social engineeren was. Onder social engineering vallen de technieken die ingezet worden om gevoelige informatie, zoals bijvoorbeeld een wachtwoord, te bemachtigen. Dit kan op verschillende manieren plaatsvinden, zoals meekijken over iemands schouder, of via de telefoon door zich als iemand anders voor te doen, bijvoorbeeld een medewerker van de belastingdienst of Microsoft.
- Cyberpesten is weinig gemeld in het onderzoek. Dit is toe te schrijven aan het feit dat weinig jongeren deelnamen aan het onderzoek, terwijl juist bij die groep cyberpesten relatief veel voorkomt.

Het is van belang dat burgers zich online veilig gedragen om zich weerbaar te maken tegen online dreigingen. Om maatregelen te kunnen treffen, is kennis nodig over dergelijke maatregelen. In het onderzoek is gekeken naar het kennisniveau van de deelnemers op het gebied van online veiligheid. Uit de resultaten blijkt dat het matig gesteld is met deze kennis. Van de 11 kennisvragen heeft geen enkele deelnemer 10 of 11 vragen correct. De gemiddelde score blijft steken op 6 correcte antwoorden.



Figuur 3: Het percentage deelnemers dat een bepaalde kennisvraag correct beantwoord heeft.

- Vrijwel iedereen weet dat je verschillende wachtwoorden moet gebruiken. Ook is een groot deel zich ervan bewust dat wachtwoorden, ook sterke wachtwoorden, af en toe gewijzigd dienen te worden. 7 op de 10 deelnemers weet een sterker wachtwoord van een minder sterk wachtwoord te onderscheiden. Als mensen hier geen kennis van hebben zijn ze kwetsbaarder om slachtoffer van online dreigingen te worden.
- Meer dan 2 op de 3 deelnemers is op de hoogte van wat de locatiedienst op de smartphone of laptop doet. Als mensen dit niet weten, dat is 1 op de 3 deelnemers, betekent dit meestal dat de locatiedienst automatisch aanstaat, omdat dit veelal de default stand is. Zo wordt er standaard informatie verzameld en bewaard over alle plekken die met de smartphone of laptop zijn bezocht. Aanbieders van diensten kunnen deze informatie misbruiken.
- Ongeveer de helft van de deelnemers weet wat een VPN is. Een VPN wordt gebruikt om een afgeschermde verbinding te maken met het internet. Als mensen geen VPN gebruiken, omdat ze er geen kennis van hebben, dan kunnen anderen zien waarvandaan de betreffende persoon op het internet aan het werken is.
- Minder dan 1 op de 10 deelnemers weet dat de camera en de microfoon van een smartphone of laptop niet uitgeschakeld kunnen worden, zodat een hacker in de smartphone of laptop de hele tijd mee kan kijken en mee kan luisteren. Wanneer mensen dit niet weten, schermen zij hun

> *Het is van belang dat mensen naast kennis over online veilig gedrag, ook de urgentie ervan inzien*

Uit het bovenstaande blijkt het belang van kennis over dreigingen en maatregelen met betrekking tot de online veiligheid. Maar zelfs mensen die deze kennis in voldoende mate hebben, treffen niet altijd de benodigde maatregelen. Iemand kan namelijk kennis over bepaalde dreigingen en maatregelen hebben, maar hier niet de urgentie van inzien. Zo blijkt uit de gedragsliteratuur dat naast kennis, ook houding een belangrijke factor is voor veilig gedrag.
De resultaten uit het onderzoek illustreren dit. Meer dan 9 op de 10 deelnemers weet dat verschillende wachtwoorden voor verschillende accounts de online veiligheid bevordert. Maar als we kijken in hoeverre deelnemers in hun dagelijks leven verschillende wachtwoorden gebruiken, dan zien we dat ongeveer 4 op de 10 deelnemers dit doet. Het idee dat met het verbeteren van kennis over online veiligheid het gewenste gedrag vanzelf volgt, is dan ook te rooskleurig. Het is van belang dat mensen naast kennis over online veilig gedrag, ook de urgentie ervan inzien. Dit vergt andere interventies dan het verbeteren van kennis.

Aandacht voor kwetsbare groepen

Aan de deelnemers is gevraagd wie volgens hun de aangewezen partij is voor het verbeteren van hun online veiligheid. Het blijkt dat de deelnemers in eerste instantie naar zichzelf kijken en vinden dat hun eigen aandeel hierin het grootst is. 1 op de 5 deelnemers ziet daarnaast ook een rol weggelegd voor de gemeente, met name gericht op kwetsbare groepen. Onder kwetsbare groepen vallen bijvoorbeeld digibeten en ouderen. Voor niet-kwetsbare groepen zien de deelnemers slechts een bescheiden rol voor de gemeente.

> *Stel een alarmnummer in of zet een informatiepunt op in de wijk.*

Met betrekking tot kwetsbare groepen, zoals digibeten en ouderen, is het van belang dat de gemeente voldoende middelen beschikbaar stelt om de online veiligheid van deze groepen te verbeteren. Dit kan door het lesaanbod over online veiligheid, van bijvoorbeeld de Stichting Lezen en Schrijven, toegankelijk te maken voor deze groepen om zo de kennis te vergroten en de basisvaardigheden te verbeteren. Door de kennis te vergroten, weten kwetsbare burgers beter hoe ze zich tegen online dreigingen kunnen beschermen. En als het gevoel van urgentie nog onvoldoende is dan kan het verbeteren hiervan direct meegenomen worden. Om de nieuwe kennis in praktijk te brengen is het goed als digibeten en ouderen, onder begeleiding, in aanraking komen met echte online dreigingen, zoals bijvoorbeeld phishing, en leren hoe ze hiermee om moeten gaan. Het buurthuis of de bibliotheek kan wellicht een geschikte plek zijn voor de begeleiding van de kwetsbare burgers op hun weg naar betere online veiligheid.

ontvangen. De gemeente zou dit kunnen faciliteren. Daarnaast zien zij voor de gemeente ook een rol bij het bieden van hulp aan slachtoffers van cybercriminaliteit. Dit kan bijvoorbeeld door het instellen van een alarmnummer of het opzetten van een informatiepunt in de wijk.

Céline Kreffer is onderzoeker en Marcel Spruit is professor Cyber Security bij het Kenniscentrum Cybersecurity, de Haagse Hogeschool

Meer iBestuur

iBestuur artikelen

Nieuws

Blogs

Podium

Artikelen

Persberichten

Praktijk

Personalia

Service & Contact

Contact

Algemene Voorwaarden

Klantenservice

Abonnement iBestuur Magazine

Adverteren

Colofon

Nieuwsbrief

iBestuur