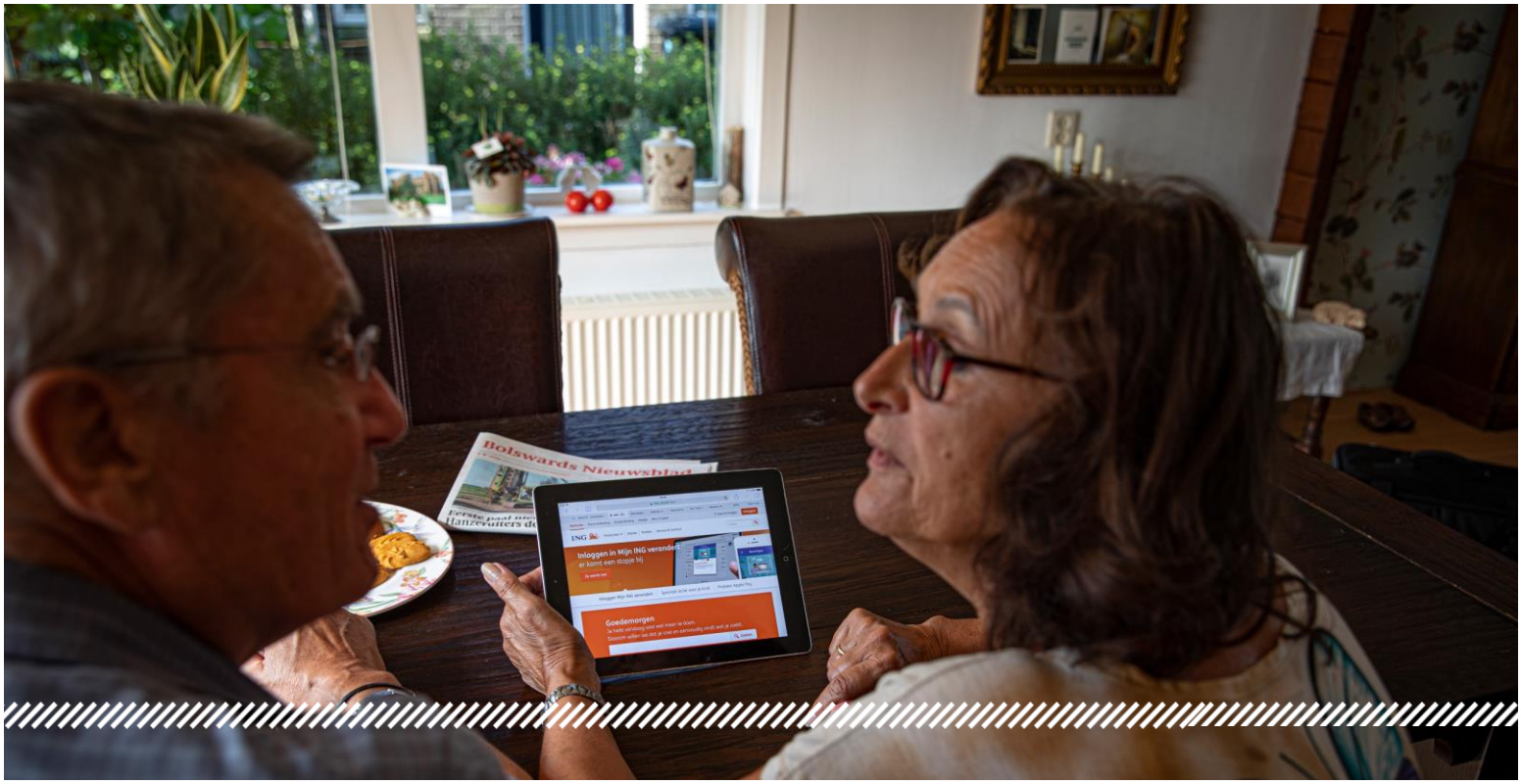
01 /23



BEWEGEN INWONERS VAN FRYSLÂN ZICH VEILIG ONLINE?

VEEL WINST TE HALEN DOOR IN TE ZETTEN OP KENNIS EN GEDRAG

// Bewegen inwoners van Fryslân zich veilig online?

Een kwart van de inwoners van Fryslân maakt geen gebruik van de top 3 van noodzakelijke beveiligingstools: virusscanning, het maken van back-ups en het uitvoeren van updates. Dit maakt hen extra kwetsbaar voor computercriminelen.

Eén op de vijf (21%) inwoners van Fryslân kreeg ooit te maken met online criminaliteit, 13 procent werd daadwérkelijk slachtoffer. Gemiddeld ontbreekt het vooral lager opgeleiden, lage inkomensgroepen en 65-plussers aan kennis en vaardigheden om zich voldoende te kunnen beschermen tegen computercriminelen. Dit rapport brengt in beeld hoe inwoners van Fryslân hun kennis over online veiligheid inschatten, wat zij doen op het gebied van beveiliging, wat hun ervaringen zijn met computercriminaliteit, welke ondersteuning ze graag willen hebben en wie die zou moeten geven.

// *Online (on)veiligheid*

Sinds de start van het internet in 1969 en de invoering van het Wereld Wijde Web bij het grote publiek in 1991, is het onlineverkeer enorm toegenomen. In 2000 waren wereldwijd 70 miljoen personal computers aangesloten op 'het net'. In 2009 gebruikte een kwart van de wereldbevolking internet, en waren er zo'n 58 miljard websites actief. Bij de laatste meting door het CBS heeft het merendeel (97%) van de inwoners van Nederland *thuis* toegang tot het internet (CBS, 2021). De groep die thuis geen internet heeft bestaat voor twee derde uit 75-plussers, vooral vrouwen met een lage opleiding.

In diverse kaders worden definities gegeven van onderwijsniveaus, inkomensgroepen en vormen van computercriminaliteit.

De beschikbaarheid van internet geeft een scala aan mogelijkheden: van mailverkeer tot het opzoeken van informatie, van internetbankieren tot het verrichten van online boekingen. Het uitgebreide internetverkeer biedt echter ook kansen aan computercriminelen, om op slinkse wijze data, geld en persoonsgegevens te ontfutselen aan argeloze internetgebruikers, of hen te chanteren met een dreigende online publicatie van bijvoorbeeld foto's of filmpjes. Veel gebruikers hebben het meteen door als een bericht of linkje 'niet klopt', waardoor computercriminelen geen kans bij hen maken. Anderen worden het slachtoffer door onwetendheid, onoplettendheid, goedgelovigheid of onvoldoende of verouderde beveiliging van hun computer, gegevens of wachtwoorden.

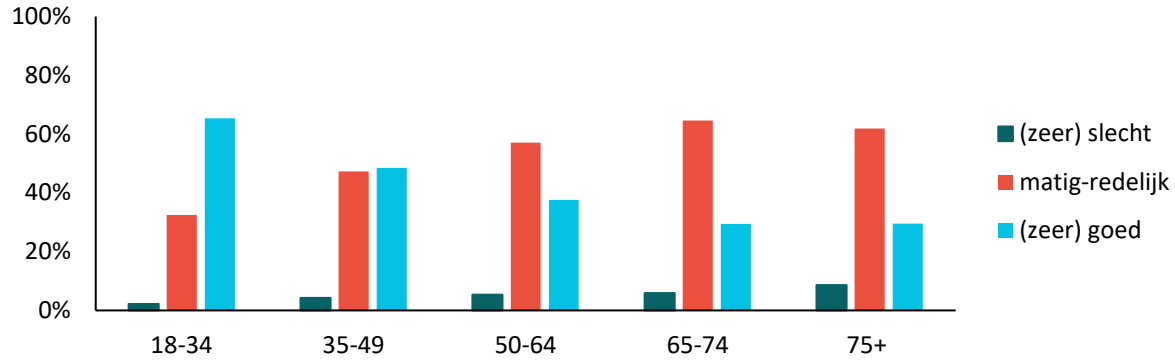
***Cursist computer-basiscursus**: Je móet wel online. Altijd hoor je: "Ga naar www..." Waardeloos vind ik dat. Waar is het contact? En je moet de kennis steeds bijhouden, die is snel verouderd.*

// *Vooral jongeren waarderen hun kennis als (zeer) goed*

De inschatting van eigen kennis over online veiligheid laat grote verschillen zien. Jongeren van 18-34 jaar (65%) omschrijven hun kennis aanzienlijk vaker als (zeer) goed dan 65-plussers (30%). Lager opgeleiden (28%) noemen hun kennis minder vaak als (zeer) goed dan middelbaar (39%) en hoger opgeleiden (38%). Mensen met een laag inkomen (31%) noemen minder vaak (zeer) goed dan mensen met een midden (35%) of hoog inkomen (42%).

Definitie inkomensniveau (bruto per jaar):
***Laag inkomen**: < € 24.700*
***Midden inkomen**: € 24.700 - € 48.000*
***Hoog inkomen**: > € 48.000*

Omschrijving eigen kennisniveau van online veiligheid per leeftijdsgroep



// *Online criminaliteit recentelijk gestegen*

Het CBS meldt recent (2022) dat slachtofferschap van computercriminaliteit sinds 2012 met 22 procent is toegenomen. Vooral in de laatste jaren is er een stijgende lijn. In 2019 werden landelijk 5.000 aangiftes gedaan van online oplichting, in 2020 ging het om 10.000.

Vormen van computercriminaliteit:
***Aankoopfraude**: u hebt voor een product of dienst betaald, maar niet ontvangen.*
***Verkoopfraude**: u hebt een product of dienst geleverd, maar de koper betaalt niet.*
***Fraude betalingsverkeer**: er is geld van uw rekening afgeschreven zonder dat u of uw mederekeninghouder daar toestemming voor heeft gegeven, bijv. door de installatie van geïnfecteerde software.*
***Hacking**: iemand logt of breekt zonder uw toestemming en met kwade bedoelingen in in uw computer, account, telefoon of apparaat, of installeert schadelijke software.*
***Identiteitsfraude**: iemand maakt illegaal gebruik van uw persoonsgegevens (online-account of ID, rijbewijs, paspoort).*
***Ransomware**: criminelen installeren (na hacking) schadelijke software die computers en bestanden gijzelt. Ze geven deze pas vrij nadat de getroffene 'losgeld' heeft betaald.*
***Phishing**: criminelen doen zich voor als een bekende of instantie, en beweren dat u een loterij hebt gewonnen, een boete moet betalen, of een dierbare in geldnood moet helpen. Ze vragen uw gegevens, waarna er wordt ingebroken in uw computer.*
***Shamesexting**: iemand chanteert u met het online verspreiden van naaktfoto's of filmpjes. De chanteur geeft aan niet tot actie over te gaan als u betaalt.*

Door de coronamaatregelen werkten veel mensen vanaf maart 2020 online vanuit huis. Ook werd er meer online geregeld, verliepen contacten meer online en werden er meer online aankopen gedaan. Maar er was ook een toename in aan- en verkoopfraude en online pesten. Want niet alleen burgers, maar ook computercriminelen brachten meer tijd door achter hun computer. De daders zijn vaak jonge mannen, opgegroeid met computer en internet. Het is eenvoudig om aan schadelijke software komen. Online criminaliteit is 'gemakkelijker' voor hen omdat het leed van hun slachtoffers (meestal) onzichtbaar is.
Vanwege deze recente ontwikkelingen is in de zomer van 2022 aan Panel Fryslân gevraagd hoe zij omgaan met online veiligheid. Aanvullend op de uitvraag werden gesprekken gevoerd met een digitaal wijkagent, Rabobank, cursisten van een basis-computercursus en met bibliotheekmedewerkers.
Het panel-project kon rekenen op de gedegen en inspirerende kennis van een expertgroep bij het samenstellen van de vragenlijst en de beschouwing van de antwoorden.

***Digitaal Wijkagent**: Bij computercriminelen moeten we beslist niet alleen denken aan doorgewinterde nerds die op het foute pad zijn geraakt. Ook leken kunnen heel veel schade berokkenen. Uit verveling of uit interesse, gewoon omdat het kán. In mijn werk zie ik dat er vooral misbruik wordt gemaakt met financieel gewin als doel. Zo komen er veel aangiftes binnen over helpdeskfraude, vriend-in-nood-fraude, misbruik van een account, aan- en verkoopfraude, en als uitschieter: fraude van bankgegevens (internetbankieren).*

***Expertgroep**: Bibliotheek Mar en Fean, Politie Súdwest-Fryslân, Sociaal Collectief Súdwest-Fryslân, FERS, Veiligheidsregio Fryslân, NHL-Stenden Hogeschool, Rabobank, en de gemeenten Súdwest-Fryslân en Leeuwarden.*

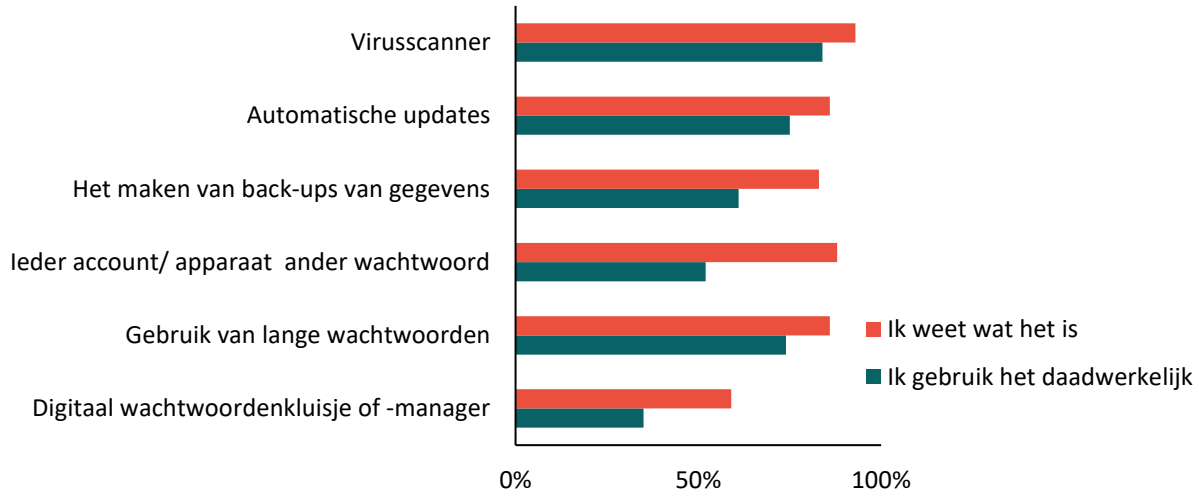
// *Kennis en gebruik van beveiligingstools*

Virusscanning, het maken van back-ups en het uitvoeren van updates worden over het algemeen als de drie sterkste acties gezien om gegevens te beschermen en zwakke plekken in computers tijdig te repareren.

***Rabobank**: Kennis houdt niet automatisch veilig gedrag in. Wat wéét je en wat dóe je? Kennis kan je juist ook achtetoos maken...*

De virusscanner is het bekendst bij de inwoners van Fryslân. Bijna iedere inwoner (93%) kent deze beveiliging. Ook het beschermen van elk account en apparaat met een ander wachtwoord (88%) en het gebruiken van lange wachtwoorden (86%) scoren hoog qua kennis. Tot slot maakt het uitvoeren van automatische updates (86%) en het maken van back-ups (83%) deel uit van de top 5 aan kennis over het beschermen van digitale gegevens.
Maar het hebben van kennis over manieren van beveiliging betekent nog niet dat deze ook daadwerkelijk worden gebruikt. De virusscanner (84%) scoort het hoogst qua gebruik, gevolgd door het uitvoeren van automatische updates (75%), het gebruik van lange wachtwoorden (74%), en het maken van back-ups van gegevens (61%).

Kennis en daadwerkelijk gebruik van online beveiligingstools



// *Acties bij verdachte mails of berichtjes*

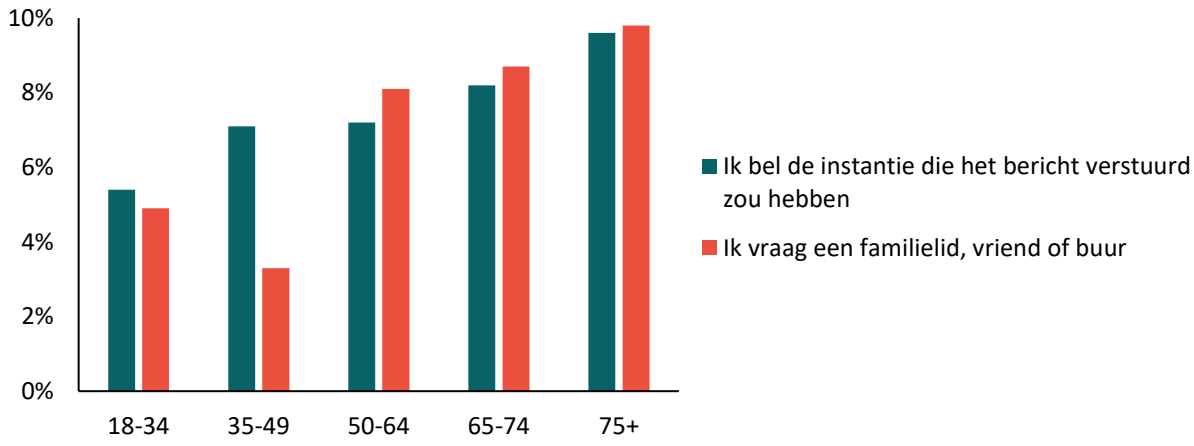
Aan de panelleden werden enkele afbeeldingen voorgelegd met de vraag hoe ze hierop zouden reageren. Het betrof vier schadelijke en twee veilige berichten. Alle berichten werden unaniem benaderd als 'onveilig'. Verklaarbaar, de vragenlijst ging immers over online veiligheid, en de eerste afbeelding was dubieus... De expertgroep-leden vroegen zich bij de beschouwing van de antwoorden af: "*Schiep het eerste bericht een sfeer van 'alles is vast nep', of maakt aandacht voor het thema misschien extra alert?"* Dit rapport moet het antwoord schuldig blijven.

De reacties van de respondenten zijn als volgt: Verreweg de meesten (91%) verwijderen de mail of het bericht onmiddellijk. Ruim een kwart (26%) kijkt op internet of er iets bekend is over het bericht. Middelbaar (29%) en hoog opgeleiden (27%) en mensen met hogere inkomens (26%) checken het bericht vaker op internet dan laag opgeleiden (20%) en lagere inkomensgroepen (22%).

***Bibliotheekmedewerker**: Kennis is wéten van beveiliging. Gedrag is hándelen vanuit die kennis. Dus tools gebruiken, maar ook alertheid, oplettendheid, gezonde argwaan, hulp vragen bij twijfel.*

Vrouwen (13%) vragen vaker dan mannen (5%) aan een familielid, vriend of buur om mee te kijken naar het mogelijk verdachte bericht. Hetzelfde geldt voor laag opgeleiden (12%) en lagere inkomensgroepen (9%) ten opzichte van hoog opgeleiden (6%) en hogere inkomensgroepen (6%). Vooral 50-plussers bellen de instantie die het bericht gestuurd zou hebben, of vragen een familielid, vriend of buur om raad.

Acties bij verdachte mails of berichten, naar leeftijdsgroep



Een aantal inwoners wijst in een toelichting op valse-email@fraudehelpdesk.nl waar ontvangers verdachte mails naar toe kunnen sturen. Ook instanties beschikken over zo'n meldfunctie, bijvoorbeeld valse-email@rabobank.nl of valse-email@belastingdienst.nl. Ook geven ze aan naasten vooral bij te staan met adviezen, waarschuwingen en het installeren van beveiligingssoftware.

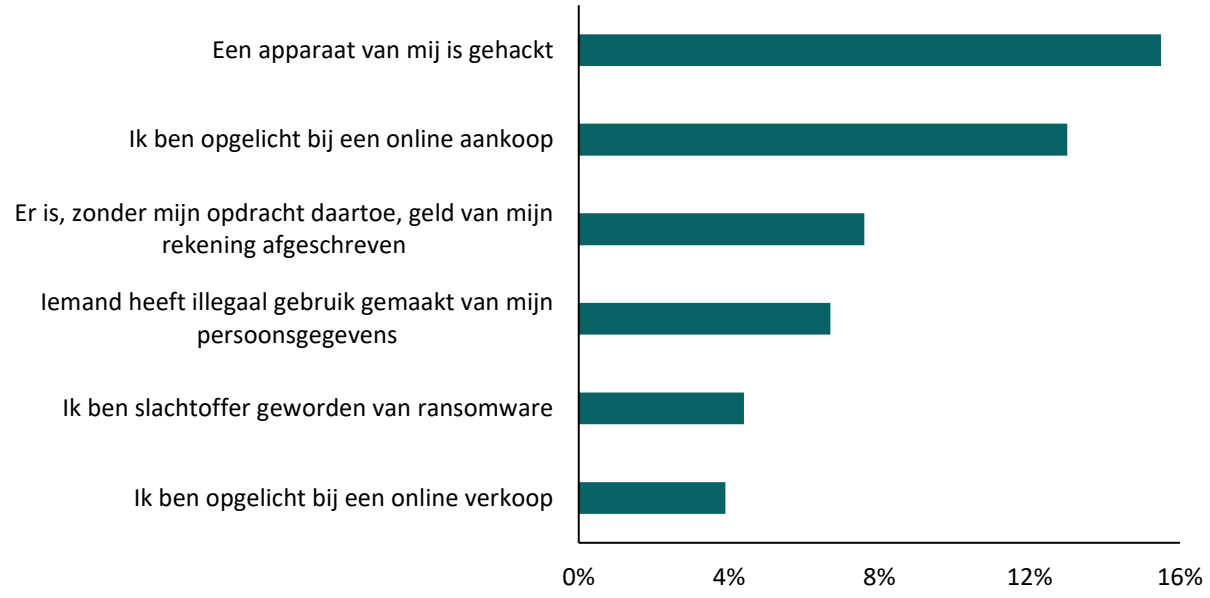
***Digitaal Wijkagent**: Zélf kun je al zoveel doen op het gebied van online veiligheid, vooral door het installeren van een virusscanner, het tijdig uitvoeren van updates en het voortdurend maken van back-ups. Daarnaast draagt 'gezonde argwaan' bij aan veiligheid. Kijk naar je eigen gedrag door de ogen van computercriminelen. Haastig even je mail checken, vlug op het linkje klikken? Het kwaad is snel geschied. Een Facebookberichtje dat je op vakantie gaat? Computercriminelen zien dat ook. Kijk dus uit wat je op sociale media plaatst. Computercriminelen lezen mee, en weten veel van je als ze je een appje sturen met 'Hoi mam, ik heb een nieuw telefoonnummer, sla je het even op?' En bij het opslaan gaat het mis: je hebt niet met een bekende te maken maar met een crimineel.*

// Hacking vaakst genoemde ervaring met online oplichting

Een op de acht (13%) inwoners van Fryslân werd ooit slachtoffer van online criminaliteit. Het vaakst werd een apparaat gehackt (16%) of werden mensen opgelicht bij een online aankoop (13%). Ook werd genoemd dat er geld van de bankrekening werd afgeschreven, zonder dat daartoe opdracht was gegeven (8%), of dat er illegaal gebruik is gemaakt van persoonsgegevens (7%). Eén op de vijfentwintig inwoners (4%) werd het slachtoffer van ransomware. Door middelbaar opgeleiden werd oplichting bij online aankoop (16%) het vaakst genoemd, door lager (14%) en hoger opgeleiden (16%) het hacken van een apparaat.

Definitie opleidingsniveau (CBS):
***Lager opgeleid**: Bo, Vmbo, Havo-onderbouw, Vwo-onderbouw, Mbo1*
***Middelbaar opgeleid**: Havo, Vwo, Mbo2-3-4*
***Hoger opgeleid**: Hbo, Wo*

Meest gemelde ervaringen met online oplichting



// Schade grootst bij shamesexting, phishing en bedreiging

De CBS Veiligheidsmonitor (2022) meldt dat slachtoffers van online criminaliteit aangeven schade te ondervinden op emotioneel, psychisch of financieel gebied. Zo ervaart 15 procent emotionele en psychische schade, 7% financiële schade als gevolg van de online criminaliteit. Emotionele en psychische schade wordt vooral opgelopen bij pesten, stalken en shamesexting (44%). De dader is meestal een bekende. De meeste financiële schade wordt opgelopen bij phishing en verkoopfraude (15%).

// *Slachtoffers buiten beeld*

Het CBS (2022) meldt dat landelijk minder dan de helft (47%) van de getroffenen melding maakte van het feit dat ze in 2021 slachtoffer waren geworden van computercriminelen. Het vaakst werd melding gemaakt van fraude in het betalingsverkeer (77%) en phishing (71%), maar slechts 19% deed daadwerkelijk aangifte. Van phishing (55%) werd het vaakst aangifte gedaan.

***Digitaal Wijkagent**: Veel slachtoffers blijven buiten beeld. Ze schamen zich, of gaan ervan uit dat het hun eigen schuld is. Of ze weten niet wat ze moeten doen. Ik hamer er op om het wél te melden of aangifte te doen. Om het voor iedereen wat overzichtelijker te maken is www.meldknop.nl een handig middel. Via deze site weet je aan de hand van een stappenplan hoe, wat en waar je iets kunt melden, en of je eventueel aangifte kunt doen bij de politie.*

// *Onderlinge hulp bij online veiligheid*

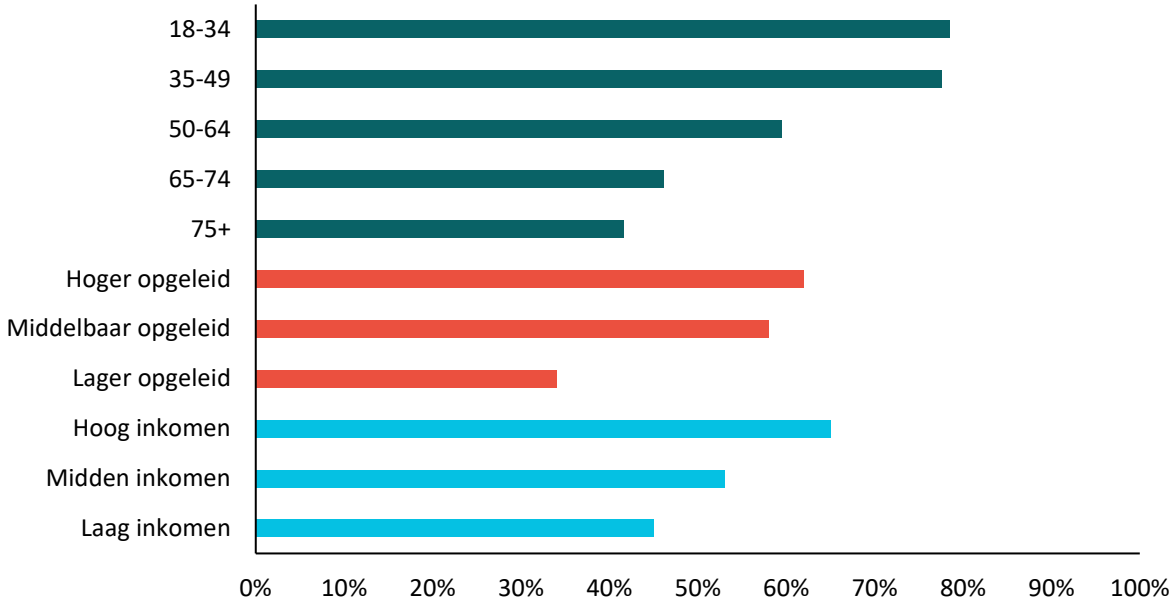
Een kleine helft (44%) van de inwoners Van Fryslân wordt door anderen aangespoord om back-ups van bestanden te maken, ruim de helft (54%) wordt gewezen op het belang van online veiligheid. Een derde (36%) van de tien inwoners wordt geholpen om veiliger online te zijn doordat er bijvoorbeeld beveiliging voor hen wordt geïnstalleerd. Driekwart (77%) kan op anderen rekenen wanneer ze een telefoontje, mail of ander bericht niet vertrouwen. Tweederde (66%) geeft aan dat anderen op hén kunnen rekenen. Ze helpen anderen om veiliger online te zijn.

*Aan **Panel Fryslân** werd gevraagd óf en hóe ze anderen hielpen veiliger online te zijn. Een samenvatting van de open antwoorden: Advies geven over de aanschaf van een virusscanner, het instellen van firewalls, het up-to-date houden van software, het gebruik van sterkere wachtwoorden of ww-kluis. Waarschuwen voor gevaren van online criminaliteit, behoeden voor oplichting. Adviseren om wantrouwig te zijn in het reageren op zaken online.*

// *Vooral jongeren maken zich zorgen over onlinegedrag door naasten*

Vier van de tien inwoners van Fryslân maakt zich soms zorgen over online gedrag van naasten, één op de tien maakt zich zelfs váák zorgen. Het zijn vooral de middelbaar opgeleiden (7%), de 18-34-jarigen (12%) en 35-49-jarigen (12%) die zich vaak tot altijd zorgen maken over het onlinegedrag van naasten.

"Ik ondersteun anderen op het gebied van online veiligheid" naar leeftijdsgroep



Ondersteuning op het gebied van online veiligheid wordt vooral gegeven door hoger opgeleiden (62%) en hoge inkomensgroepen (65%). Ook binnen leeftijdsgroepen zijn verschillen te zien als het gaan om de daadwerkelijke ondersteuning van anderen op het gebied van online veiligheid. De meeste ondersteuning wordt gegeven door de 18-34-jarigen (79%) en 35-49-jarigen (78%), maar ook vier van de tien 75-plussers ondersteunen anderen.

***Digitaal Wijkagent**: Naast het feit dat jongeren zich het meest zorgen maken, zijn ze ook het vaakst slachtoffer van twee specifieke vormen van computercriminaliteit: shamesexting en misbruikt worden als geldezel. Shamesexting kom ik, naast aan- en verkoopfraude veel tegen in mijn werk. Voorkomen is beter dan genezen: stuur nooit online intieme foto's of filmpjes naar vrienden of vriendinnen, en al helemaal niet naar iemand die je alleen online kent. Bezitters kunnen dreigen de foto's te publiceren, en op die manier geld eisen. Betaal nooit, want daarmee geef je het signaal af dat er meer te halen is. Doe aangifte. De politie kan een 'stop-gesprek' met de dader voeren, mede met het doel om het beeldmateriaal te laten verdwijnen. Jongeren kunnen gemakkelijk geronseld worden als geldezel. Ze lenen tegen een kleine vergoeding hun rekeningnummer uit aan 'een kennis' die daar vervolgens verkoopfraude mee pleegt. De actie levert slachtoffers op, maar ook een strafblad voor de geldezel."*

// Helft inwoners voert acties uit op het gebied van online veiligheid

Inwoners van Fryslân voeren verschillende acties uit om zo veilig mogelijk online te zijn, anderen doen dat, om wat voor reden ook, soms of nooit. Zo installeert driekwart (75%) van de inwoners vaak tot altijd updates van besturingssystemen, software en apps zodra die beschikbaar zijn, een kwart soms tot nooit. Tweederde (66%) laat vaak tot altijd apparaten door beveiligingssoftware scannen op virussen of andere nadelige software, een derde soms tot nooit. De helft (51%) maakt vaak tot altijd back-ups van belangrijke bestanden, de helft soms tot nooit.

Een kwart (26%) controleert vaak tot altijd de privacy-instellingen van zijn of haar apparaten, apps of sociale media, driekwart soms tot nooit. Driekwart (71%) gebruikt nooit of zelden simpele korte wachtwoorden, 19% doet dat soms, 9% vaak of altijd. Een elfde (9%) van de inwoners maakt vaak tot altijd gebruik van openbare WiFi, een derde (34%) soms, ruim de helft (57%) nooit. Al met al voert de helft van de inwoners van Fryslân acties uit die bijdragen aan het beschermen van hun apparaten en gegevens, de andere helft niet.

Enkele minder bekende vormen van online-beveiliging:
***VPN-verbinding**: versleutelde, veilige toegang tussen uw computer, smartphone of tablet en het internet.*
***Wachtwoordenkluisje**: een programma op uw computer (of smartphone-app) dat sterke en unieke wachtwoorden maakt, bewaart en invult wanneer dit nodig is.*
***Web tracking blocker**: deze blokkeert 'volgers' tijdens het surfen op internet, zodat u kunt surfen en online winkelen zonder dat gerichte advertenties op het internet u volgen.*
***Biometrische authenticatie**: instelling op uw apparaat of account die de toegang ervan alleen mogelijk maakt via uw vingerafdruk, iris- of gezichtsscan.*
***Ad-blocker**: en programma dat het weergeven van advertenties in de browser van uw computer, smartphone of tablet blokkeert of filtert.*
***Open source hard- en software**: een voordeel van 'open' is dat iedereen er naar kan kijken, zwakheden kan opsporen en repareren, en niet 'stiekem' iets kan inbouwen.*

// Moeite met acties op het gebied van online veiligheid

Een op de zeven (15%) inwoners geeft aan dat het up-to-date houden van software hen moeite kost. Het gaat vooral om vrouwen (20%), lager opgeleiden (18%), lage- en middeninkomens-groepen (17%) en 65-plussers (17%). Daarnaast geeft 16% aan dat het tijdrovend is om na te gaan of ze zich in een veilige online omgeving bevinden. Dit geldt voor met name lager opgeleiden (23%), lage inkomensgroepen (19%), 65-74-jarigen (17%) en 75-plussers (25%).

// Behoefte aan ondersteuning

Eén op de acht (12%) inwoners van Fryslân heeft behoefte aan ondersteuning op het gebied van online veiligheid. Het gaat vooral om informatie over online veiligheid (13%), een cursus of training om kennis over onlineveiligheid te vergroten (9%) en een telefonische of inloophelpdesk op het moment dat een probleem wordt ervaren of iets niet wordt vertrouwd.

***Cursist computer-basiscursus**: Wij hebben een keer wat besteld op een site en dachten dat dat veilig was. Dat bleek niet het geval. Ik wil hier meer over leren zodat ik weet dat het goed is.*

***Cursist computer-basiscursus**: Vooral internetbankieren is moeilijk. En gevaarlijk. Ik ben naar een andere bank overgestapt. Hier kan ik binnen lopen. Ze leggen me alles stap voor stap uit.*

Mannen (14%) geven vaker dan vrouwen (12%) aan behoefte te hebben aan informatie over online veiligheid. Meer lager opgeleiden (15%) dan mensen met een midden (13%) of hoger (12%) onderwijsniveau hebben behoefte aan deze informatie. Hetzelfde geldt voor lagere inkomensgroepen (16%) ten opzichte van midden- (14%) en hogere inkomensgroepen (12%). Meer 65-plussers (16%) dan 65-minners (10%) hebben behoefte aan informatie over online veiligheid.

***Cursist computer-basiscursus**: Mijn man deed de computerzaken altijd. Nu moet ik dat zelf doen. En eigenlijk vind ik het wel leuk. Maar je moet steeds oefenen, anders is de kennis weer weg.*

***Cursist computer-basiscursus**: Ik dacht dat ik veel wist maar ik weet eigenlijk niks. Ik moest steeds mijn kinderen vragen en dat wil ik niet meer.*

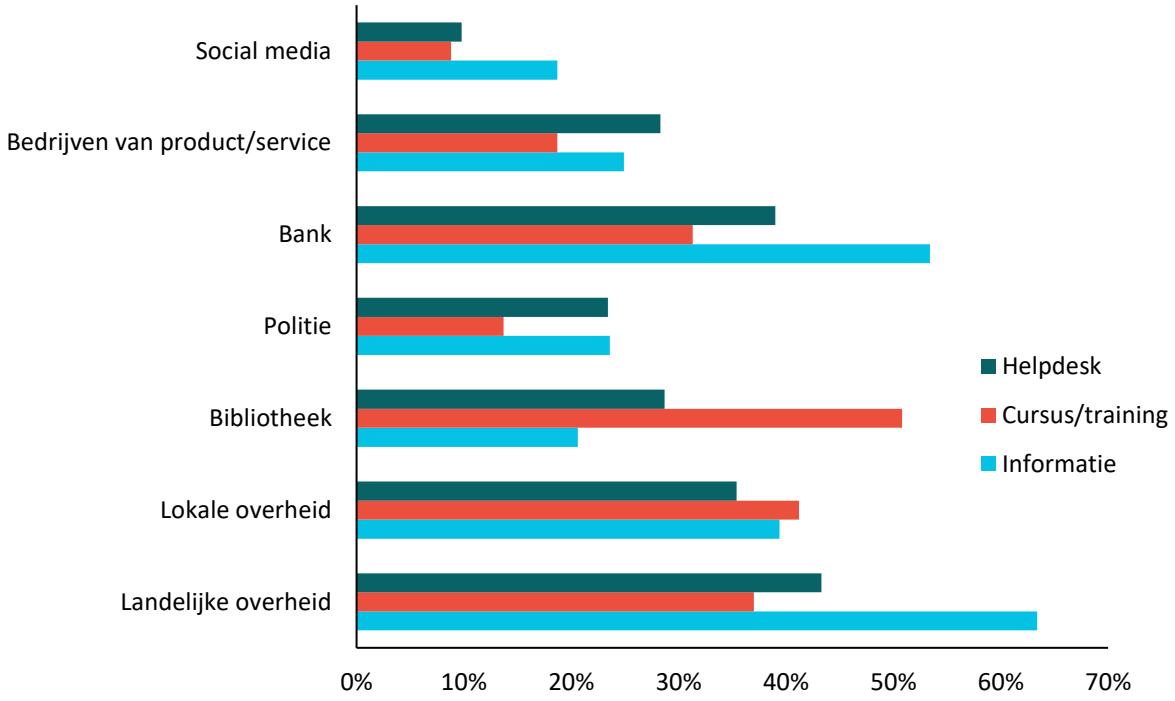
Als het gaat om een cursus of training om kennis over online veiligheid te vergroten, dan geven meer vrouwen (11%) dan mannen (9%) aan hier behoefte aan te hebben. Qua opleidings- en inkomensniveau is deze behoefte vrijwel gelijk. Gaat het om leeftijdsgroepen, dan zijn het vooral de 65-plussers (12%) die aangeven behoefte te hebben aan een cursus of training op het gebied van online veiligheid. Bij 18-34-jarigen leeft deze behoefte onder 2%, bij 35-49-jarigen onder 6% en bij 50-64-jarigen onder 11%.

Meer vrouwen (16%) dan mannen (11%) geven aan ondersteund te willen worden door een helpdesk. Ook hoger opgeleiden (15%) geven vaker aan behoefte te hebben aan een helpdesk dan middelbaar (12%) of lager opgeleiden (11%). Hetzelfde geldt voor midden-inkomensgroepen (16%) ten opzichte van mensen met een laag (12%) en hoog inkomen (12%). Meer 65-plussers (15%) dan 35-49-jarigen (12%) en 34-minners (7%) geven aan behoefte te hebben aan een helpdesk die hen kan ondersteunen als ze een probleem ervaren of iets niet vertrouwen op het gebied van online(on)veiligheid.

// *Hulp verwacht van overheden, banken en bibliotheken*

Jongeren kunnen doorgaans rekenen op hun onderwijsinstelling als het gaat om hulp bij, en voorlichting over digitale veiligheid. De panel-uitvraag richtte zich op de andere diensten. De inwoners van Fryslân geven in de panel-uitvraag aan dat het vooral de landelijke overheden en banken zijn die informatie moeten verstrekken over online veiligheid. Voor hen is ook de helpdeskfunctie weggelegd, aldus de inwoners. Bibliotheken worden vooral genoemd als het gaat om cursussen op het gebied van online veiligheid.

Wie zou informatie, cursus of helpdesk m.b.t. online veiligheid moeten verstrekken?



// Tot slot: Bewegen inwoners van Fryslân zich veilig online?

Er is er nog veel winst te halen op het gebied van onlineveiligheid. Gemiddeld een kwart van de inwoners maakt geen gebruik van de top 3 tools die als onmisbaar worden gezien als het gaat om online veiligheid: de virusscanner, het tijdig uitvoeren van updates en het maken van back-ups. Al met al voert gemiddeld de helft van de inwoners van Fryslân acties uit die bijdragen aan het beschermen van hun apparaten en gegevens, de andere helft niet. Ook zijn er tools die bijdragen aan online veiligheid, zoals biometrische authenticatie, nog niet bekend bij het grote publiek in Fryslân. Bij online veiligheid is zowel kennis als gedrag essentieel.

***Bibliotheekmedewerker**: een computer-cursist heeft zélf al bedacht: 'Hier moet ik iets mee'. Maar hoe zit het met die vele anderen die ook met de handen in het haar zitten als het om computers en online veiligheid gaat?*

Bij *kennis* gaat het om het op de hoogte zijn van tools die bijdragen aan online veiligheid en het kunnen gebruiken ervan. Zwakke of ontbrekende tools bieden computercriminelen een open deur. Kennis gaat ook om het herkennen van schadelijke mails en berichten. Wat staat er? Klopt het taalgebruik wel? Staat er een website in het bericht, of een adres? Kennis heeft daarnaast betrekking op het weten van wegen naar informatie, hulp en ondersteuning.

Bij *gedrag* gaat het om het adequaat handelen vanuit die kennis, dus het installeren van tools en het uitvoeren van acties die bijdragen aan online veiligheid. Gedrag gaat ook om alertheid, 'gezond wantrouwen', concentratie, check. Wát wordt er over het hoofd gezien? Welk signaal wordt gemist, en hoe komt dat? Vermoeidheid, argeloosheid, goedgelovigheid, haast en onoplettendheid vormen zwakke deuren waardoor computercriminelen gemakkelijk digitaal naar binnen kunnen sluipen. Gedrag heeft daarnaast betrekking op het inschakelen van informatie, hulp en ondersteuning als dat nodig is.

Voorlichting over, en hulp bij online veiligheid moet zich daarom niet alleen richten op kennis, maar ook op gedrag. En niet alleen gericht op ‘de computer’, maar op het gebruik ervan op de vele terreinen van de samenleving: van internetbankieren tot wonen, van online winkelen tot een zorg-aanvraag. Integraal dus.

De onderlinge bereidheid om elkaar te helpen bij digitale veiligheid is groot. Daarnaast kunnen politie en fraudehelpdesks signalen afgeven over recente en veel gepleegde vormen van onlinecriminaliteit, en adviezen geven over passende voorlichting. Overheden en banken kunnen veel soelaas bieden met voorlichting en helpdesks, net als bibliotheken met gerichte cursussen. Niet alleen voor de zwakkere groepen, dus mensen met een laag opleidings- en inkomensniveau en oudere leeftijdsgroepen, maar ook voor de sterkeren (let wel: ook uit bovengenoemde groepen) die hen bijstaan.

Er is werk aan de winkel. Het Fries Sociaal Planbureau en de expertgroep hopen dan ook dat álle inwoners van Fryslân hun kennis en gedrag bij online veiligheid tijdens een volgende panel-uitvraag, nadat er veel ‘werk in de winkel is verzet’, waarderen met een ‘zeer goed’.

*Het FSP realiseert zich dat **een groep inwoners van Fryslân niet wordt bereikt**, omdat zij thuis niet beschikken over computer en internet, of omdat het hen ontbreekt aan voldoende digitale kennis en vaardigheden. Deze wetenschap maakt de aanbevelingen nog urgenter.*

// Bronnen

Akkerman, M., Kloosterman, R., Moons, E., Reep, C. & Tummers-van der Aa (2022). *Veiligheidsmonitor 2021*. Den Haag: Centraal Bureau voor de Statistiek (CBS).

CBS: *Internettoegang en internetactiviteiten, persoonskenmerken*. Geraadpleegd op 15 november 2022 op: https://www.cbs.nl/nl-nl/cijfers/detail/84888NED

CBS: *435 duizend mensen hadden in 2019 thuis geen internet*. Geraadpleegd op 15 november 2022 op: https://www.cbs.nl/nl-nl/nieuws/2020/14/453-duizend-nederlanders-hadden-in-2019-thuis-geen-internet

CBS: *2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit.* Geraadpleegd op 15 november 2022 op: https://www.cbs.nl/nl-nl/nieuws/2022/09/2-5-miljoen-nederlanders-in-2021-slachtoffer-van-online-criminaliteit

// *Verantwoording Panel Fryslân*

Panel Fryslân bestaat uit een representatieve mix van inwoners van heel Fryslân van 18 jaar en ouder, met verschillende inkomens- en opleidingsniveaus. Deze groep deelt (anoniem) haar ervaringen en geeft meningen over wat er speelt in Fryslân. Door panelonderzoeken kan het FSP trends en ontwikkelingen in Fryslân in kaart brengen, analyseren en duiden. Daarmee krijgen beleidsmakers, politici, overheden, media en belangstellenden goede en betrouwbare informatie over hedendaagse, sociale en maatschappelijke onderwerpen https://www.fsp.nl/panelfryslan/

COLOFON

‘BEWEGEN INWONERS VAN FRYSLAN ZICH VEILIG ONLINE?’ is een uitgave van het Fries Sociaal Planbureau.

Auteurs
Truus de Witte
Jesse David Marinus
Chaïm la Roi

Vormgeving
Fries Sociaal Planbureau

Uitgave
Fries Sociaal Planbureau
Doelestraat 8a, 8911 DX Leeuwarden

Fries Sociaal Planbureau
Doelestraat 8a
8911 DX Leeuwarden
(058) 234 85 00
info@fsp.nl

Het Fries Sociaal Planbureau wordt gesubsidieerd door de provincie Fryslân.