OOST-BRABANT

VOORWOORD

Op woensdag 20 april vond aan de Noordkade in Veghel het Symposium Cyber Oost-Brabant plaats. Zo'n 200 gasten waren daar bijeen om te luisteren naar verhalen over Cybercrime. De sprekers, soms zelf slachtoffer, deden daar 'een boekje open over Cybercrime'. Door met elkaar verhalen te delen en in gesprek te gaan kunnen we vanuit de gezamenlijkheid werken aan een digitaal veiligere samenleving. Het Symposium werd u aangeboden door de gemeente Meierijstad (die dit jaar 5 jaar bestaat), de Programmaraad Cyber Oost-Brabant en het Regiobureau Integrale Veiligheid Oost-Brabant. Verschillende partners, zoals Het CCV en de VNG, hebben teruggeblikt op deze mooie middag.
Wij danken de sprekers en uiteraard u als gasten. Tijdens het Symposium hebben wij toegezegd dat we nog een mailing sturen met o.a. meer handelingsperspectieven. We willen u hiermee graag een eerste handvat bieden om met Cyber, ofwel Digitale Veiligheid, aan de slag te gaan. De Programmaraad Cyber Oost-Brabant wenst u hierbij veel succes. Mocht u vragen hebben, dan kunt u deze sturen naar info@rivob.nl

Kees van Rooij, burgemeester Meierijstad, Voorzitter Programmaraad Cyber Oost-Brabant.

VOOR GEMEENTEN IN OOST-BRABANT

Voor gemeenten is het van belang dat Digitale Veiligheid in de lokale coalitieakkoorden en Integrale Veiligheidsplannen een prominente plek krijgt. Hiertoe hebben burgemeester van Rooij (gemeente Meierijstad) en burgemeester Ubachs (gemeente Best), respectievelijk voorzitter en vicevoorzitter van de Programmaraad Cyber Oost-Brabant, recent een bericht gestuurd naar alle 32 burgemeesters in Oost-Brabant. Daarbij zijn ook de Lokale Cyberwegenkaart van het CCV, de Agenda Digitale Veiligheid en het Focusblad Digitale Veiligheid van de VNG t.b.v. het Integrale Veiligheidsplan meegestuurd. De VNG organiseert bestuurlijke gesprekken rondom het thema digitale veiligheid. Gemeenten die willen deelnemen kunnen hun interesse kenbaar maken door een mail te sturen naar teamadv@vng.nl. Aangezien de Programmaraad Oost-Brabant prioriteit geeft aan kwetsbare groepen zoals jeugd, ouderen en laaggeletterden en het MKB gaan we in deze nieuwsbrief wat specifieker in op een aantal projecten die de moeite waard zijn voor deze doelgroepen. Wilt u als gemeente van gedachten wisselen over Digitale Veiligheid, neem dan contact op met Frank Hustin of Ronny van Gerven van het Regiobureau Integrale Veiligheid Oost-Brabant (info@rivob.nl).

VOOR BEDRIJVEN IN OOST-BRABANT

Het Platform Veilig Ondernemen Oost Brabant en Zeeland West Brabant (PVO Brabant-Zeeland) is een Publiek-Private Samenwerking (PPS). Zij zetten zich in om veiligheidsmaatregelen te ontwikkelen en onder de aandacht te brengen in de strijd tegen onder andere ondermijnende criminaliteit, cybercrime, vastgoedfraude en High Impact Crimes. Hierbij zet het PVO Brabant-Zeeland in op voorlichting, instrumentontwikkeling en het aanjagen van samenwerking.

Het Digital Trust Center is er ook voor bedrijven. Naast preventieve adviezen delen zij ook dreigingsinformatie met bedrijven.

In Oost-Brabant is ook het Cyberweerbaarheidscentrum Brainport gevestigd. Zij bieden bedrijven een unieke kans om zich beter te wapenen tegen cyber criminaliteit. Hierover leest u meer verderop in deze nieuwsbrief.

Wanneer er bij een gemeentelijke organisatie een cyberincident is waar spoed bij is, dan neemt u contact op met de Informatiebeveiligingsdienst (IBD): Home - Informatiebeveiligingsdienst

Bent u als ondernemer geraakt door een cyberincident, dan kan de Hackhelpdesk u mogelijk op weg helpen. Ook voor preventieve adviezen kunt u daar terecht: Hulp na hack | hackhelpdesk.nl

KIJK, LEES- EN LUISTERTIPS

'Inbraakpogingen zijn aan de orde van de dag' (binnenlandsbestuur.nl)
Digitale veiligheid chefsache (binnenlandsbestuur.nl)
Digitaal Beroofd - Veiligheidscoalitie
Cyber Sessies | RTL Nieuws
Hack Talk
Cyberhelden.nl – Podcast van Ronald Prins

INTERVENTIES VOOR GEMEENTEN

Er zijn verschillende interventies om mee aan de slag te gaan als het gaat om het bevorderen van de cyberweerbaarheid in uw gemeente. In Oost-Brabant zijn Jeugd, Ouderen en laaggeletterden en het MKB gedefinieerd als "kwetsbare" groepen als het gaat om digitale veiligheid. Voor Jeugd en Ouderen en laaggeletterden zijn er een aantal interventies die we hieronder toelichten. In de database van het CCV staan allerlei nuttige interventies die u als gemeente kunt inzetten om de digitale veiligheid van uw inwoners en ondernemers te vergroten: Database lokale cyberprojecten - Het CCV

Jeugd

HackShield was een hele energieke afsluiting van het symposium op 20 april! Begin 2022 is er een collectieve ambitie uitgesproken door de 32 gemeenten in Oost-Brabant om met HackShield (een interventie om 8-12 jarigen Cyberweerbaar te maken) aan de slag te gaan.
We willen zoveel mogelijk Junior cyber agents (8-12) gaan opleiden in alle gemeenten in Oost-Brabant. De aankomende weken zal HackShield starten met de groepsvorming voor gemeenten om aan te kunnen haken bij de maand van de cyber security en, week van de mediawijsheid.
HackShield zal gemeenten begeleiden in het opstarten van lokale campagnes en alle materialen ter beschikking stellen. Emily Jacometti en Wessel van Stiphout van HackShield coördineren het volgende instroommoment van 15 September. Om te zorgen dat de capaciteit goed kan worden verdeeld over alle gemeenten zullen zij contact opnemen met iedereen individueel om afspraken te maken over vervolg, contactpersoon en startmoment. Voor vragen kunnen gemeenten altijd direct contact opnemen met Emily Jacometti. (e.jacometti@joinhackshield.nl)

Ouderen en laaggeletterden

Voor ouderen en laaggeletterden is in Oost-Brabant een interventie ontwikkeld: Storytelling Cybercrime. In samenwerking met het KBO kunnen avonden worden georganiseerd waarop getrainde storytellers ouderen en laaggeletterden op een laagdrempelige manier vertellen over de risico's van de digitale wereld. Daarbij worden ook praktische tips meegegeven. Wit u meer weten over deze interventie of andere lokale interventies gericht op ouderen en laaggeletterden, neem dan contact op met het Regiobureau Integrale Veiligheid Oost-Brabant. Naast gerichte interventies is er ook landelijk materiaal beschikbaar om via uw gemeentelijke kanalen te verspreiden. Dit betreft de Campagne Senioren en Veiligheid 2022: Campagne Senioren en Veiligheid 2022 | Senioren en Veiligheid | Maak het ze niet te makkelijk

Cyber Weerbaarheidscentrum BRAINPORT

CYBER WEERBAARHEIDSCENTRUM BRAINPORT: SAMEN STERKER TEGEN CYBERCRIMINALITEIT

Hebben de verhalen van Xander Koppelmans, Gemeente Hof van Twente en Senzer u aan het denken gezet? En wilt u graag de volgende stap zetten om bedrijven in uw gemeente meer cyberweerbaar te maken? Of wilt u aan de slag met de cyberweerbaarheid van uw eigen bedrijf? Maar weet u niet zo goed waar te beginnen? Het Cyber Weerbaarheidscentrum Brainport (CWB) helpt u verder!

Voor bedrijven in de high-tech maakindustrie en hun toeleveranciers bestaat sinds 2019 de Stichting Cyber Weerbaarheidscentrum Brainport. Deze stichting zonder winstoogmerk biedt bedrijven in deze sector een unieke kans om zich samen beter te wapenen tegen cybercriminaliteit. De nadruk ligt op samen. Het doel van het CWB is cyberweerbaarheid in de hele keten van de high-tech maakindustrie te versterken. Dit kan alleen als bedrijven informatie en kennis met elkaar delen.

Het CWB ondersteunt dit met diverse diensten. Zo biedt het CWB onder andere dreigingsinformatie met handelingsperspectief, netwerk monitoring, maandelijkse kennissessies, een kennisbank vol met best-practices & templates , informele uitwisseling van informatie tussen participanten en de mogelijkheid voor organisaties om zich te certificeren. Daarnaast kan het CWB doorverwijzen naar haar partners voor extra ondersteuning bij cybersecurity.

Wilt u ook uw steentje bijdragen aan een meer cyberveilige keten? Of wilt u meer weten over het CWB? Neem dan vrijblijvend contact op met Lisette Oosterbosch via info@cwbrainport.nl of kijk op onze website.

OPENBAAR MINISTERIE

Afgelopen jaar zagen wij het opnieuw: een schrikbarende toename van cyberincidenten. Ook de impact ervan is groter geworden. Denk alleen al aan de verschillende ransomware-aanvallen in binnen- en buitenland, die ook burgers en bedrijven in de regio Oost-Brabant raken. Wij willen het criminele organisaties moeilijker maken mensen en bedrijven op te lichten. Daarom werken wij onder andere samen met andere overheidsinstanties, bedrijven, wetenschappers, en ethisch hackers. Kennisdeling leidt tot een betere opsporing, maar ook tot een betere beveiliging van computers en andere devices. Naast opsporing en vervolging zetten politie en OM namelijk ook in op alternatieve interventies om cybercrime in de breedte te bestrijden, denk aan vormen van preventie, verstoring en notificeren van (potentiële) slachtoffers.

Hoe meer politie en OM weten van cybercriminaliteit, hoe meer kans er is de daders te pakken. Aangifte doen is daarom altijd belangrijk. Via de website van de politie kunt u aangifte doen. Daar en bijvoorbeeld via veiliginternetten.nl en fraudehelpdesk.nl vindt u adviezen hoe cybercrime en oplichting via de smartphone of computer is te voorkomen.

AVANS HOGESCHOOL ALS KENNISPARTNER VOOR VRAAGSTUKKEN ROND CYBERCRIME EN CYBERWEERBAARHEID

Cybercriminaliteit ontwikkelt zich snel qua verschijningsvormen en daarmee samenhangende dreiging en schade voor burgers en ondernemers. De corona-pandemie heeft een snelle groei laten zien van cybercrime (hoewel daarvoor al een stijging te zien was van de digitaliseerde criminaliteit). Het beperken van schade en vooral het vergroten van cyberweerbaarheid roepen kennisvragen op die om praktijkgerichte kennis vanuit verschillende disciplines vraagt.

Vanuit Avans zijn een groot aantal docenten, studenten en onderzoekers betrokken bij verschillende betekenisvolle projecten. Samen met bewonersorganisaties, ondernemers, ketenpartners, veiligheidsregio's en gemeenten wordt gewerkt aan praktische maatregelen. Vaak gaat het daarbij om samenwerking met specialisten op het gebied van ondermijning, maar ook op het terrein van sociale en technologische innovaties (zoals toepassingen van Artificial Intelligence).

Samen met collega's van Fontys wordt de komende jaren gewerkt aan een krachtenbundeling op het gebied van verantwoorde toepassingen van Artificial Intelligence voor het midden- en kleinbedrijf (mkb). Binnen Avans gaat het daarbij om de opleidingen Integrale Veiligheidskunde, Social Work, Rechten en Bestuurskunde, Bedrijfskunde en Innovatie en de lectoraten Ondermijning en Digitalisering en Veiligheid.

Contactpersonen voor verdere info:
Lector Digitalisering en Veiligheid, Ben Kokkeler bjm.kokkeler@avans.nl
Senior-onderzoeker Cybercriminaliteit, Roel de Beer rmg.debeer@avans.nl
Senior-onderzoeker Ondermijning, Jonas Stuurman jj.stuurman@avans.nl

INTERNATIONALE CYBERDREIGING:

Eind april verscheen het **Jaarverslag 2021 van de AIVD**. Daarin ook speciale aandacht voor cyberdreiging. Enkele belangrijke punten uit dit hoofdstuk:

- De Nederlandse overheid, vitale sectoren en bedrijven liepen in 2021 een grotere kans om te worden gehackt door landen met een offensief cyberprogramma.
- Nederland staat hoog op de lijst van landen waarvan de digitale infrastructuur wordt misbruikt bij cyberaanvallen. Ook worden cyberaanvallen om processen in een ander land te beïnvloeden of om desinformatie te verspreiden.
- Veel statelijke actoren met een offensief cyberprogramma voeren aanvallen bij voorkeur uit via Nederlandse verbindingen en via in Nederland gehuurde servers. Dat doen ze omdat die servers van goede kwaliteit zijn en de internetverbindingen snel en betrouwbaar zijn.

Lees meer op aivd.nl/cyberdreiging

Weten hoe de AIVD cyberdreigingen onderzoekt?
Luister naar het tweede seizoen van de podcastserie De Dienst (aivd.nl/podcast).
Een teamhoofd, een bewerker, een analist en een cryptoloog vertellen daar wat zij doen om Nederland tegen cyberaanvallen te beschermen.

VEILIGHEIDSREGIO BRABANT-NOORD
VeiligheidsRegio Brabant + Zuidoost

Binnen de veiligheidsregio's worden twee soorten vormen van cybergevolgbestrijding voorzien: extern en intern.
Voor beide zijn aparte trajecten gestart, welke volop in ontwikkeling zijn.

Enerzijds richt de veiligheidsregio zich op grootschalige externe cyberincidenten in de regio. Hierbij ligt de focus niet op de bronbestrijding of technische oplossingen bij externe bedrijven, maar voornamelijk op het beperken en bestrijden van fysieke gevolgen van de cybercrisis. Denk hierbij onder andere aan uitval van elektriciteit, verstoring van de drinkwatervoorziening of het vrijkomen van gevaarlijke stoffen bij een BRZO bedrijf. Hiernaast kunnen ook cascade effecten ontstaan, welke moeilijk te voorspellen zijn. Daarom zijn bouwstenen ontwikkeld, die kunnen helpen bij een goed beeld en inzicht in de ernst van de situatie.

Daarnaast kan de veiligheidsregio ook intern worden geraakt door een cyber-incident. Om dit te voorkomen is er een groeiende aandacht voor de cyber-veiligheid waarbij toegankelijke preventiemaatregelen worden aangereikt aan alle medewerkers. Dit wordt gedaan door onder meer maandelijkse stukjes met informatie op het intranet en waarschuwingsbalken bij e-mails welke afkomstig zijn van buiten de veiligheidsregio. Ook is er ontwikkeling op het gebied van cyberweerbaarheid door de opzet van een intern team. Dit team kan snel worden ingeschakeld bij mogelijk interne cyberincidenten.

Voor zowel de externe als interne cyberbestrijding is duidelijke communicatie en een goed netwerk van groot belang.

POLITIE OOST-BRABANT

Trends en ontwikkelingen:
Steeds meer criminaliteit vindt plaats in een digitaal jasje. De politie is vanzelfsprekend een belangrijke partij bij de bestrijding van digitale criminaliteit. Hierbij wordt een onderscheid gemaakt tussen enerzijds Cybercrime en anderzijds Gedigitaliseerde criminaliteit.

Cybercrime
Cybercrime is criminaliteit waarbij ICT zowel doelwit als middel is. Voorbeelden zijn computervredebreuk/ hacken,
DDoS aanvallen en ransomware. Het bestrijden van dergelijke fenomenen is de kerntaak van het cybercrimeteam.

Gedigitaliseerde criminaliteit
Naast Cybercrime zien we Gedigitaliseerde criminaliteit. Dit is criminaliteit waarbij ICT-middelen als ondersteunend middel ingezet worden om 'traditionele' criminaliteit te plegen. Denk hierbij aan het plegen van oplichting of diefstal via het internet. Het plegen van online identiteitsfraude, phishing of het online uiten van bedreigingen. In de politiecijfers is online oplichting veelal terug te vinden onder de term: 'Horizontale fraude'.

Voor een effectieve aanpak en een goede informatiepositie wordt er zowel landelijk als regionaal samengewerkt. De eenheid Oost-Brabant bestaat uit 3 districten die zijn onderverdeeld in 9 basisteams die in de aanpak van gedigitaliseerde criminaliteit worden gecoacht door het regionale cybercrimeteam. De aanpak van Gedigitaliseerde criminaliteit ligt bij de reguliere politieorganisatie, het cybercrimeteam focust zich op het bestrijden van cybercriminele fenomenen zoals ransomware.

Wat zagen we de afgelopen jaren?
Als we kijken naar de registraties zien we dat de categorie fraude / oplichting in de jaren 2019, 2020 en 2021 veruit dominant was. Wanneer wordt gekeken naar de ontwikkeling van de grootste subcategorie (fraude met bankgegevens / internetbankieren) is te zien dat deze categorie ieder opeenvolgend jaar flink toeneemt. De toename in 2021 t.o.v. 2020 is echter minder groot dan de toename in 2020 t.o.v. 2019. De stijging in 2021 heeft mogelijk deels te maken met de intrede van het delict bankhelpdeskfraude.

Daarnaast valt op dat het aantal registraties op het gebied van afpersing / chantage voor het tweede achtereenvolgende jaar gestegen is. Dit is voornamelijk te wijten aan een stijging op het gebied van sextortion. Mogelijk is deze stijging deels te wijten aan het feit dat het gebruik van social media onder jongeren sterk gestegen is tijdens corona.

Ook is er een stijging waar te nemen van het aantal registraties dat betrekking heeft op diefstal van cryptomunten.
Het fenomeen "vriend-in-nood-fraude" is afgenomen t.o.v. vorig jaar. Er zijn echter wel nog meer registraties dan in 2019. Ditzelfde beeld is te zien voor misbruik van accounts voor bestellingen.

Welke vormen van digitale criminaliteit komen het meest voor?

Top 5 delicten 2021

Fraude met bankgegevens/internetbankieren	49,6%
Aan- en verkoopfraude	10,0%
Helpdeskfraude	8,8%
Misbruik accounts voor bestellingen	7,4%
Vriend-in-noodfraude	5,2%

Top 5 delicten 2020

Fraude met bankgegevens/internetbankieren	45,9%
Vriend-in-noodfraude	12,9%
Misbruik accounts voor bestellingen	12,8%
Aan- en verkoopfraude	11,8%
Helpdeskfraude	8,5%

UITGELICHT: BANKHELPDESKFRAUDE

Gezien het feit dat bijna de helft van de geregistreerde incidenten bij de politie Oost-Brabant 2021 Fraude met bankgegevens/internetbankieren betrof, lichten we deze vorm van digitale criminaliteit er uit.

Bij bankhelpdeskfraude worden slachtoffers gebeld door iemand die zich voordoet als zogenaamde bankmedewerker. Dit kan met een anoniem nummer of met een zogenaamd 'gespoofd' nummer. Bij een gespoofd telefoonnummer is het telefoonnummer vervalst, waardoor het nummer in je scherm overeenkomt met het nummer van de bank (terwijl je niet echt met de bank belt).
Het slachtoffer wordt de volgende mededelingen gedaan:

- De nepbankmedewerker zegt dat er verdachte activiteiten zijn op je rekening (terwijl dat in werkelijkheid nog niet het geval is);
- Vervolgens wordt het slachtoffer wijsgemaakt dat hij of zij zijn of haar geld moet veiligstellen en/of dat de pinpas vervangen moet worden. In sommige gevallen wordt er gezegd dat er iemand aan huis komt om te 'helpen' of om de oude pinpas op te halen. Daarnaast kunnen de criminelen ook aanbieden op afstand te 'helpen' door de pc over te nemen.
- Ten slotte vindt de "cash out" plaats. De rekening van het slachtoffer wordt gekoppeld aan de telefoon van de dader en de telefoon waarmee het slachtoffer toegang heeft tot zijn haar rekening wordt ontkoppeld. Vervolgens wordt het geld van de rekening gepind of doorgesluisd naar een andere rekening en het slachtoffer kan niet meer bij het geld en / of de rekening. Ook komt het voor dat de daders zowel de pinpas en de pincode op komen halen en vervolgens naar de pinautomaat gaan om daar geld te pinnen.

"Via een 06-nummer werd ik gebeld door een man die zich voordeed als medewerker van ABN AMRO. Hij vroeg me mijn geld tijdelijk op een ander rekeningnummer te zetten, omdat Mexicanen wilden inbreken op mijn spaar- en privérekening. De man, die perfect Nederlands sprak, wist alles van me. Mijn naam, mijn adres, de laatste transacties. Ik dacht: 'Die gegevens heeft toch alleen de bank?'. Daardoor liet ik me, ondanks mijn twijfels, toch overhalen en maakte ik ruim 5.000 euro over."

Het komt voor dat nepbankmedewerker het slachtoffer precies weet te vertellen wat het huidige banksaldo is en wat de laatste transacties waren. In dat geval hebben de oplichters zichzelf waarschijnlijk reeds toegang verschaft tot de bankrekening (bijvoorbeeld middels phishing via een nep-betaallink). Ook is het mogelijke dat (bijvoorbeeld via een link of bijlage in een valse e-mail) software (malware) op de computer van het slachtoffer is geplaatst. Die maakt een schermafbeelding op het moment dat internetbankieren wordt afgesloten. Zo weten ze precies wat er op dat moment op de bankrekening van het slachtoffer staat. Doordat de oplichter veel van het slachtoffer lijkt te weten, komt helpdeskfraude erg geloofwaardig over

Bankhelpdeskfraude is opgekomen in 2020 en in 2021 flink toegenomen ten opzichte van 2020. Hoewel er een daling is waar te nemen in november en december 2021, is er in januari 2022 weer een stijging te zien.

Spoofing wordt door criminelen overigens breder ingezet en wordt onder criminelen steeds populairder. Spoofing kan worden gedaan met een e-mailadres, telefoonnummer, website of IP-adres. Via spoofing is het dus mogelijk dat het telefoonscherm een ander nummer laat zien dan het nummer waarmee een beller eigenlijk belt. Op die manier kunnen oplichters het nummer van de bank laten zien, zodat het net lijkt alsof men echt door uw bank gebeld wordt. Ook helpdeskfraude is een bekend voorbeeld van spoofing. Oplichters doen zich voor als de helpdesk van een groot bedrijf, zoals Microsoft. Zo bellen ze met een Nederlands telefoonnummer terwijl ze helemaal niet in Nederland zitten. Ze proberen via een handig praatje toegang te krijgen tot de computer en het slachtoffer te bewegen om geld over te maken.

Tips om geen slachtoffer te worden van digitale criminaliteit:

Tot slot zijn we zelf ook allemaal gebruikers van ICT. Hieronder een paar praktische tips voor u:

Algemeen

- Installeer een anti-virusprogramma en houd dat up-to-date. Scan bijvoorbeeld uw computer regelmatig.
- Installeer een softwarematige firewall. Of nog beter: zet de firewall in uw router aan.
- Gebruik geen open WiFi-netwerken waarop u zonder wachtwoord kunt inloggen. Als het niet anders kan, gebruik dan een VPN-verbinding.
- Klik niet op links die u niet vertrouwt of verwacht, bijvoorbeeld in e-mails of pop-ups. Ga met uw muis boven een link staan (niet klikken!) en kijk onder in het scherm waar de link echt naartoe verwijst.
- Uw bank of bedrijven als Microsoft, Google en Apple bellen u nooit omdat er zogenaamd problemen zijn met uw computer. Trap dus niet in deze digitale babbeltrucs van criminelen.

Software

- Installeer alleen software van een betrouwbare afzender, bijvoorbeeld de website van de fabrikant.
- Houd geïnstalleerde software up-to-date.
- Gebruikt u bepaalde software niet meer, verwijder die dan.

Wachtwoorden

- Heeft u veel wachtwoorden, gebruik dan een digitale wachtwoordmanager als Lastpass, 1password, Dashlane of Keepas.
- Gebruik sterke wachtwoorden met een combinatie van hoofdletters, kleine letters, cijfers en leestekens.
- Gebruik nooit hetzelfde wachtwoord voor meerdere accounts.
- Bewaar uw wachtwoorden nooit bij uw computer, in een bestand op uw computer of in uw e-mailaccount.
- Geef uw wachtwoorden of inlogcodes aan niemand af (dus ook niet aan een helpdeskmedewerker binnen uw bedrijf of organisatie).
- Gebruik als extra beveiliging een zogenaamde two-factor-authentication. Via een sms of een app als Google Authenticator ontvangt u dan een extra inlogcode.
- Wijzig de standaard wachtwoorden van soft- of hardware altijd.
- Beveilig uw laptop, smartphone of computeraccount minimaal met een wachtwoord of pincode.

Websites met tips:

- Veiligbankieren.nl
- Veiliginternetten.nl
- Veiligzakelijkinternetten.nl
- 123cybersecurity.nl
- Politie.nl/themas/cybercrime.html
- Toolbox.bof.nl/
- Fraudehelpdesk.nl
- Internetsporen.nl
- Pasopjepas.nl
- Alertonline.nl
- Security.nl
- Laatjeniethackmaken.nl
- Checklistdigitaalveilig.nl

5 JAAR MEIERIJSTAD

MEIERIJSTAD

Regiobureau Integrale Veiligheid Oost-Brabant