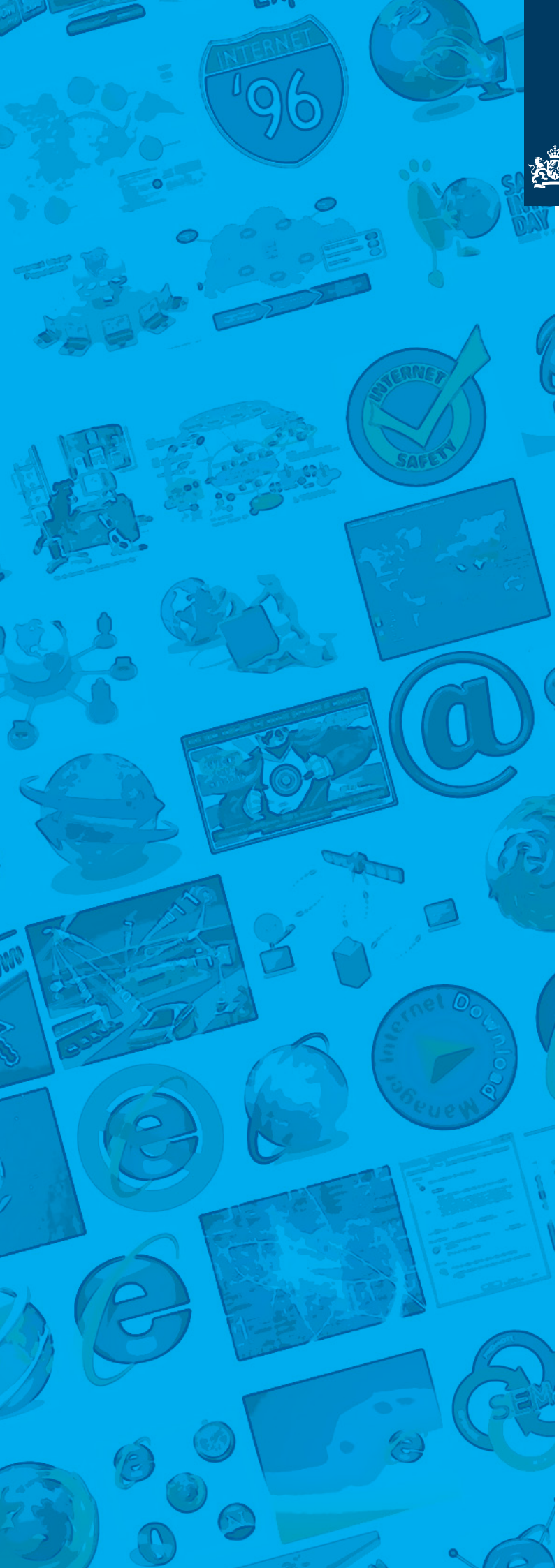

Ministerie van Veiligheid en Justitie

Je bent zichtbaarder dan je denkt

Een programma over cyber security awareness

Informatie voor medewerkers


Mobile Web Initiative
Google
JOIN US ON
facebook
http://www
http://com

Inleiding

Iedereen maakt steeds meer gebruik van internet. Niet alleen privé, maar zeker ook zakelijk. Nederland heeft één van de hoogste percentages computers met internettoegang. En telefoneren doen we ook bijna allemaal mobiel. Dat heeft hele grote voordelen: het maakt ons bereikbaar, flexibel en efficiënt. Maar er is ook een andere kant. Bij het gebruik van deze apparaten laten we sporen na en zijn we traceerbaar. Lang niet iedereen is zich ervan bewust dat kwaadwillenden gebruik kunnen maken van die sporen voor ongewenste activiteiten. Incidenten laten zien dat er kwaadwillenden zijn die gebruikmaken van ons onbewuste onveilige handelen op het internet en bij mobiele communicatie.

Om je bewust te maken van waar je sporen achterlaat, hoe kwaadwillenden daarvan gebruik maken en hoe je veiliger kunt handelen, hebben het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) een Cyber Security Awareness-programma ontwikkeld: 'Je bent zichtbaarder dan je denkt'.


DRUNK
PARTY

Het programma

Het programma bestaat uit: een film van ongeveer 15 minuten, een factsheet en een e-learning-module van ongeveer 30 minuten.
De film kan worden ingezet bij het werkoverleg. De e-learning-module kun je zelfstandig doorlopen op een moment dat het je schikt.

In deze factsheet vind je de belangrijkste onderwerpen van het programma en tips hoe je veilig kunt handelen.

TIPS

wachtwoorden

1. Gebruik altijd een wachtwoord van minimaal 8 karakters.
2. Maak altijd een combinatie van hoofdletters en kleine letters, cijfers en speciale (lees)tekens.
3. Gebruik nooit al te voor de hand liggende wachtwoorden, zoals (achter)namen of geboortedata.
4. Gebruik verschillende wachtwoorden, in ieder geval voor je zakelijke digitale verkeer, privé e-mail en online-bankieren.
5. Gebruik nooit alleen een woord uit het woordenboek, maakt niet uit welke taal. Tenzij je een woord uit het woordenboek combineert met een 'woord' dat niet voorkomt in een woordenboek.
   Bijvoorbeeld:
   - Bedenk een zin die je makkelijk kunt onthouden en gebruik de eerste of laatste letter van ieder woord. Bijvoorbeeld: 'Ik heb twee zussen en koekjes zijn lekker.' Als wachtwoord krijg je dan: Ih2z&kzl
   - Je kunt dit wachtwoord aanvullen met een woord of omschrijving dat past bij het programma waarvoor je inlogt. Bijvoorbeeld: Ih2z&kzl+Centjes of Ih2z&kzlBrieven voor respectievelijk je online-bankieren en e-mail-account
6. Pas het standaardwachtwoord van een (nieuwe) account meteen aan.
7. Houd je wachtwoorden geheim. Wanneer je ze toch wilt vastleggen, bewaar ze dan in een digitale wachtwoordkluis of in een echte kluis.
8. Wijzig je wachtwoord regelmatig. Wijzig je wachtwoord in ieder geval nadat je hebt ingelogd op een publieke computer of op een openbaar WiFi-netwerk, zoals in de trein, in het café en/of tijdens je vakantie.
9. Als je wachtwoord is gekraakt, meld dat dan binnen je organisatie.
10. Als je privé wordt gekraakt, neem dan contact op met de organisatie van het account dat is gekraakt. Als een strafbaar feit is gepleegd en de persoonlijk geleden schade groot is, neem dan contact op met de politie.

(spear)phishing

1. Vertrouw nooit blindelings afzendergegevens in e-mailberichten.
2. Denk na over de context van het bericht: 'Klopt het dat ik dit bericht ontvang van deze organisatie?'
3. Klik in ieder geval nooit op onbekende links en download of open geen onbekende bijlagen bij een e-mailbericht van een onbekende afzender.
4. Het komt ook voor dat kwaadwillenden berichten van bekende afzenders gebruiken om je door te linken naar malafide websites. Dus wees hier ook voorzichtig mee. Bij twijfel, neem (telefonisch) contact op met de afzender van het bericht.
5. Je kunt een link tekstueel controleren door deze in een Word-document te kopiëren. Bevat de link een rare website of tekst die je niet verwacht, bewaar de e-mail en meld de situatie binnen je organisatie.
6. Kopieer de link nooit in je browser want dan kan je alsnog besmet raken.
7. Wees voorzichtig met het plaatsen en uitwisselen van gevoelige gegevens via e-mail en mobiele dragers, zoals een USB-stick. E-mail-accounts kunnen worden gekraakt en mobile dragers kun je verliezen.
8. Controleer de gebruikersvoorwaarden én privacy-instellingen van de social media waarop je actief bent.
9. Alle gegevens die je via social media plaatst, lijk je te kunnen verwijderen. Realiseer je dat al deze berichten worden bewaard.
10. Realiseer je ook: hoe meer je deelt, hoe vollediger je profiel kan worden ingevuld.

cloud

1. Lees altijd goed de gebruikersvoorwaarden van clouddiensten. Vaak zijn deze zo opgesteld dat de aanbieder van de opslagdienst rechten verkrijgt over jouw informatie.

2. Voor (bedrijfs)vertrouwelijke documenten zijn clouddiensten daarom minder geschikt. Bekijk het beleid van je organisatie voor het gebruik van clouddiensten.
3. Indien er toch gebruik gemaakt moet worden van een clouddienst zorg er dan voor dat de gegevens zijn versleuteld.

metatags

1. Alle online activiteiten laten sporen na. Sommige sporen zijn onvermijdelijk voor het gebruik van een bepaalde dienst. Beperk daarom het privégebruik van diensten met je zakelijke computer.
2. Cookies kun je zelf op jouw computer verwijderen, maar de gegevens over jouw surfgedrag bevinden zich ook op andere computers die je niet meer kunt verwijderen. Zo blijven gegevens als 'welke websites je bezoekt, wanneer, hoe vaak en welke onderwerpen je interessant vindt' altijd beschikbaar. Wees je hiervan bewust.
3. Zet indien mogelijk de locatiegegevens van de apps op je mobiele telefoon uit. Soms kun je de app niet gebruiken zonder dat 'locatiegegevens' aanstaat, maar wees je daar in ieder geval van bewust.
4. Ook foto's en films bevatten deze gegevens in de vorm van GPS-informatie. Het is mogelijk om te bepalen waar de foto is gemaakt en bij direct delen op social media is te bepalen waar je jezelf bevindt. Realiseer je dit.
5. Ook al heb je zelf je locatie-instellingen uitgezet op al je mobiele apparaten, als je familie en vrienden dat niet hebben gedaan, is een locatie via sociale media alsnog heel snel te achterhalen. Wees je hiervan bewust.
6. Alle inhoud, ook overschreven teksten, kan worden opgeslagen in Word-documenten. Afhankelijk van de instellingen is te achterhalen wie, wanneer, wat heeft gewijzigd. Dit kan leiden tot reputatieschade van een organisatie of van een persoon. Ook andere documenten en bestanden (zoals PDF, Powerpoint, Excel) slaan extra gegevens op. Realiseer je dit.

thuiswerken

1. Bij gebruik van je zakelijke computer thuis, gebruik een VPN-verbinding. Zonder deze bescherming is de kans groter dat jouw computer besmet raakt met malware.
2. Zorg bij je privécomputer voor een 'gelaagde' beveiliging, d.w.z. installeer een virusscanner, een firewall, een spamfilter en de laatste software updates, zowel van je virusscanner als van de overige software die je thuis gebruikt.
3. Plak je webcam af als je deze niet gebruikt. Sommige malware is in staat mee te kijken via je webcam zonder dat je dat weet.
4. Laat eventuele huisgenoten geen gebruik maken van je zakelijke computer. Gebruik je zakelijke computer niet voor privédoeleinden.
5. Hoe meer poorten (d.w.z. toegang voor bijvoorbeeld gebruik van e-mail, games etc.) je op je computer open hebt staan hoe meer risico je loopt. Als je een router en/of firewall aanschaft, staan de poorten veelal standaard ingesteld. Controleer dit voor jouw computergebruik. Als je bijvoorbeeld geen gebruik maakt van games, laat de poorten hiervoor niet (automatisch) openen.
6. Raadpleeg altijd het beleid van jouw organisatie voor thuiswerken en houd je aan de regels. Ze zijn er om jou en je organisatie te beschermen.
7. Besef goed dat wanneer je al deze maatregelen neemt een 100% beveiliging onmogelijk is als je computer op het internet is aangesloten. Het is dus essentieel dat je ervoor zorgt dat er zo weinig mogelijk digitale 'buit' te halen valt.

WiFi / BYOD

1. Zet automatisch verbinden met WiFi-netwerken alleen aan voor eigen netwerken, dus je bedrijfsnetwerk via VPN of je thuisnetwerk. Andere netwerken, zoals in de trein of op je vakantieadres zijn onbeveiligd en daardoor onveilig(er).
2. Zet WiFi en bluetooth uit wanneer je er niet mee werkt. Mobiele apparaten met een actieve WiFi en bluetooth verbinding (die aanstaat) kunnen door kwaadwillenden worden misbruikt.
3. Zorg ervoor dat je (bedrijfs)vertrouwelijke en financiële gegevens alleen met SSL websites uitwisselt. SSL (Secure Sockets Layer) is een manier om verbindingen tussen webbrowser en webserver te beveiligen. SSL versleutelt de gegevens voordat ze worden verstuurd. Je herkent in je webbrowser een SSL-verbinding aan het webadres in de browser: wanneer de verbinding is beveiligd met SSL, begint het webadres met 'https' (secure). Ook de kleur van de balk waarin https staat is van belang. Als deze blauw of beter nog groen is, is deze beter beveiligd dan een normale 'witte' balk. Controleer tevens of je het veiligheidsslotje op het scherm ziet staan. Een beveiligde pagina is te herkennen aan de aanwezigheid van zo'n slotje.
4. Zorg ervoor dat al je mobiele apparaten een beveiligingscode hebben.
5. Zorg ervoor dat je jouw apparaten een 'remote wipe' functie geeft. Hiermee kun je op afstand gegevens van het apparaat wissen. Een 'remote locate' is ook handig. Hiermee kun je op afstand de locatie van het apparaat achterhalen.
6. Controleer altijd de privacy-instellingen van de app op jouw mobiele telefoon. Hier kun je zien waar je de app allemaal toegang tot geeft. Indien nodig, pas deze instellingen aan.
7. Raadpleeg het beleid van jouw organisatie voor het gebruik van je eigen mobiele apparaten, zoals smartphone en tablet.


Mobile Web Initiative
JOIN US ON facebook
Google
http://www
http://www.com