BEVEILIGMIJ.NL
Security awareness

Security awareness Handboek

www.beveiligmij.nl

Dit handboek hoort bij de opleidingen van BeveiligMij.nl.
Je kunt hier alle tips nog eens rustig doorlezen.
Wil je nog meer tips of een uitgebreidere uitleg?
Kijk dan op ons informatieportaal:

https://beveiligmij.nl

BEVEILIGMIJ.NL
Security awareness

Wachtwoorden

Wachtwoorden gebruik je iedere dag. Bijvoorbeeld als je inlogt op je computer, je tablet of je telefoon. Wachtwoorden zijn de sleutel tot informatie en mogelijkheden die alleen voor jou beschikbaar zijn.

Aan de hand van een gebruikersnaam en wachtwoord controleert een systeem of jij wel diegene bent die je zegt dat je bent. Dit noemen we *authenticatie*. Als de inloggegevens kloppen bepaalt het systeem welke rechten jij binnen het systeem hebt. Welke informatie mag je zien? Welke bewerkingen mag je doen? Dit noemen we *autorisatie*.

Identiteitsdiefstal

Weet iemand anders jouw wachtwoord? Dan kan die persoon doen alsof hij jou is. Inloggen op Facebook en een statusupdate plaatsen bijvoorbeeld. Of inloggen op het bedrijfsnetwerk en documenten verwijderen. We noemen dit identiteitsdiefstal. En het erge is, dat jij verantwoordelijk gesteld wordt voor de daden van die ander.

Informatiediefstal

Kent iemand jouw gebruikersnaam en wachtwoord? Dan kan die persoon informatie inzien die alleen voor jou toegankelijk is. De ander kan daar misbruik van maken.

Tips

- **Stel veilige wachtwoorden samen:**
  - **Een goed wachtwoord:**
    - **bevat geen woorden, namen, of data;**
    - **bevat minimaal 12 karakters.**
  - **Wees creatief in het gebruik van karakters.**
  - **Stel een acroniem samen op basis van een gemakkelijk te onthouden gegeven.**
  - **Vervang letters of woorden door cijfers en symbolen.**
  - **Maak spelfouten.**
  - **Relateer je wachtwoord aan een favoriete hobby of sport.**
- **Schrijf wachtwoorden nooit op.**
- **Gebruik een wachtwoordmanager.**
- **Laat wachtwoorden genereren door een wachtwoordmanager.**
- **Gebruik 2-factor authenticatie.**
- **Gebruik voor elke dienst een unieke gebruikers naam-en-wachtwoordcombinatie.**
- **Beantwoord geheime vragen niet eerlijk.**

Veilig internetten

Surfen

Internetten doen we meestal op de automatische piloot. Dat is gevaarlijk, want cybercriminelen maken hier misbruik van.

Malware

Cybercriminelen gebruiken speciale software om bijvoorbeeld jouw identiteit te kopiëren of jouw bestanden te gijzelen (*ransomware*). Deze software noemen we malware. Ze verspreiden malware via bijvoorbeeld websites en advertenties. De malware infecteert je computer vaak zonder dat je het door hebt. De malware stuurt jouw persoonlijke gegevens dan terug naar de criminelen.

Identiteitsdiefstal

Weten cybercriminelen jouw gegevens? Dan kunnen ze zich voordoen als jou. We noemen dit identiteitsdiefstal.

Informatiediefstal

Met jouw identiteit kunnen criminelen nog meer van jouw informatie stelen. Zowel persoonlijke en zakelijke informatie, zoals foto's, e-mails en documenten.

Tips

- **Controleer links voordat je erop klikt.**
- **Analyseer de link voordat je erop klikt.**
- **Wees alert op veranderingen op de website.**
- **Wees alert op “typefouten” en lees nauwkeurig.**
- **Gebruik alleen veilige en vertrouwde netwerken.**
- **Een vreemde computer is nooit veilig.**
- **Sluit pop-ups af met**
  - **Alt+F4 op Microsoft Windows;**
  - **Cmd+Q op Apple macOS / OS X.**
- **Eerlijkheid duurt het langst, maar gaat ook ten koste van je privacy.**
- **Als het te mooi is om waar te zijn, dan is dat ook zo.**
- **Gebruik je gezonde verstand.**

Veilig internetten

Internetbankieren

Iedereen doet aan internetbankieren. En we zijn ons redelijk bewust van de gevaren. Maar hoe goed wij ook opletten... cybercriminelen zitten niet stil!

Phishing: misleidende nep-e-mails

Vroeger kon je phishingberichten gemakkelijk herkennen: er zaten vaak taalfouten in de e-mails en de nepwebsites waar ze je heen leidden zaten amateuristisch in elkaar. Tegenwoordig zijn hun e-mails en websites niet van de echte te onderscheiden. Ook is de malware die de cybercriminelen gebruiken steeds geavanceerder geworden. Je hebt vaak niet of te laat door dat je computer is geïnfecteerd.

Telefoonscam

Cybercriminelen worden ook steeds brutaler. Aan de telefoon doen ze zich bijvoorbeeld voor als medewerker van een bank. Ze proberen je dan over te halen om jouw gegevens af te geven. Dit doen ze met de oude vertrouwde trucs: verleiding, angst aanjagen en onder tijdsdruk zetten.

Tips

- **Log alleen in via een beveiligde website (https://).**
- **Klik nooit op een link, maar type deze altijd zelf in.**
- **Controleer of het adres van de website klopt.**
- **Wees alert op afwijkingen op de site en tijdens de betalingsprocedure.**
- **Controleer regelmatig je bij- en afschrijvingen.**
- **Reageer niet op verzoeken om inloggegevens of pin-codes via de e-mail of telefoon.**
- **Geef geen inloggegevens aan andere websites.**
- **Zorg voor een goed beveiligde PC, tablet en telefoon.**
- **Maak geen gebruik van openbare netwerken.**
- **Controleer, controleer en blijf controleren.**
- **Log altijd uit.**
- **Gebruik alleen je Postvak In van je internetbankieren.**
- **Laat je niet bang maken!**
- **Gebruik alleen de officiële app.**

Veilig e-mailen

Phishing

Phishing is oplichting via e-mail. Je krijgt een e-mail die lijkt van jouw bank of een ander bedrijf dat je vertrouwd te zijn. Maar in de mails zitten links naar nepwebsites. Eenmaal daar infecteert de website je computer met malware, of probeert de site naar je persoonlijke (bank-) gegevens te 'vissen'.

Geld gestolen

Hebben criminelen jouw bankgegevens? Dan kunnen ze namens jou bankoverschrijvingen uitvoeren of aanpassen.

Identiteitsdiefstal

Criminelen kunnen ook jouw online identiteit overnemen. Bijvoorbeeld op LinkedIn, Twitter of Facebook. Maar ze kunnen ook online een bankrekening afsluiten. En zo via 'jouw' rekening geld doorsluizen.

Tips

- **Controleer op de volgende phishing-kenmerken:**
  - **De e-mail heeft een onpersoonlijke aanhef.**
  - **Phishing e-mails bevatten vaak nog steeds grammatica- en spelfouten.**
  - **In de e-mail wordt gevraagd om persoonlijke gegevens.**
  - **Phishing e-mails spelen vaak in op jouw angst.**
  - **Phishing e-mails zetten je soms onder tijdsdruk.**
  - **Er wordt vaak verwezen naar een eerdere gebeurtenis.**
  - **Uiteraard bevatten phishing e-mails onbetrouwbare links.**
- **Klik nooit op een link.**
- **Wil je toch klikken:**
  - **Controleer naar welke URL een link verwijst.**
  - **Lees de volledige link.**
  - **Type de link zelf in.**
- **Open geen bijlagen.**
- **Geef NOOIT persoonlijke informatie en logingegevens via e-mail of telefoon.**
- **Zorg voor een veilige PC, tablet en telefoon.**

Veilig e-mailen

Spear phishing

Bij phishing benaderen criminelen een grote groep mensen in de hoop dat een klein percentage in hun val trapt. Spear phishing is gericht op een specifieke organisatie, een zeer kleine groep personen of zelfs op een individu.

Moeilijk te herkennen

Criminelen maken gebruik van bestaande vertrouwensbanden. Ze doen zich bijvoorbeeld voor als één van je collega's. Hierdoor zijn hun e-mails moeilijk te herkennen als spear phishing.

Goed voorbereid

Criminelen bereiden hun aanvallen goed voor. Ze selecteren hun slachtoffers en gaan op zoek naar specifieke informatie over hen. Hiervoor gebruiken ze vooral social media. Daar vinden ze namelijk veel persoonlijke informatie.

Tips

- **Blijf altijd alert.**
- **Verwacht je de ontvangen e-mail?**
- **Eén telefoontje kan alle twijfel wegnemen.**
- **Verwacht je geen bijlagen en links? Open deze dan niet.**
- **Controleer de volledige link.**

Veilig e-mailen

Spam

Spam is mail die je ongevraagd ontvangt. Criminelen versturen spam in grote hoeveelheden tegelijk. In de hoop dat iemand de mail opent.

Spamberichten zijn niet alleen irritant, ze zijn ook gevaarlijk.

Spam verspreidt malware...

Klik je op een link in een spambericht? Dan kunnen criminelen malware op je computer installeren.

... en malware verspreidt spam

Sommige malware kan via jouw computer spam versturen. Jouw computer is dan ongevraagd onderdeel van een groter spamnetwerk.

Onoplettendheid

Spam werkt alleen als we niet goed opletten. We ontvangen iedere dag veel e-mails en willen deze snel verwerken. In de haast kun je dan sneller op een verkeerde, onveilige link klikken.

Tips

- **Wees zuinig met je e-mailadres. Vul het niet zomaar overal in.**
- **Gebruik meerdere e-mailadressen.**
- **Maak gebruik van wegwerp e-mailadressen.**
- **Vermom je e-mailadres.**
- **Let op opties in formulieren van websites.**
- **Gebruik een lang e-mailadres.**
- **Gebruik nooit de unsubscribe-optie in een spambericht.**
- **Gebruik de Afwezigheidsassistent bewust.**
- **Gebruik de Voorbeeldweergave-optie niet.**
- **Open geen NDR berichten.**
- **Nieuwsbrieven zijn meestal geen spamberichten.**
- **Gebruik de *Dit is spam*-optie.**
- **Laat spamberichten niet automatisch verwijderen.**
- **Spammers liegen.**
- **Koop nooit iets wat aangeboden wordt in spamberichten.**
- **Mails van onbekende afzenders is spam.**
- **Klik nooit op links.**

Wifi-netwerken

Een onbeveiligd draadloos netwerk is als een handtas die open en bloot op straat ligt. Iedereen die dat wil kan door je spulletjes graaien, geld uit je portemonnee halen, je foto's bekijken en schade toebrengen.

Informatiediefstal / installatie van malware

Gebruik je een onbeveiligd netwerk? Dan hebben anderen toegang tot jouw apparaten. Ze kunnen dan bij je persoonlijke gegevens. En criminelen kunnen ook malware installeren op jouw computer.

Identiteitsdiefstal

Criminelen kunnen via een onbeveiligd netwerk ongemerkt al het netwerkverkeer onderscheppen. Dus ook jouw inloggegevens en andere persoonlijke informatie. Zo kunnen ze jouw identiteit kopiëren en misbruiken.

Misbruik van jouw internetverbinding

Heb je thuis of op het werk een onbeveiligd wifi-netwerk? Dan kan iedereen hier vrij gebruik van maken. En als dit gebeurt voor illegale praktijken, dan gebeurt dit dus onder jouw naam.

Tips

Tips voor het gebruik van openbare wifi-netwerken:

- **Controleer de naam van het netwerk met de locatie.**
- **Schakel automatisch verbinding maken uit.**
- **Vermijd websites waar je je moet aanmelden wanneer je verbonden bent via een wifi-netwerk.**
- **Gebruik altijd een VPN, zeker bij openbare netwerken.**
- **Schakel wifi alleen in wanneer je het ook daadwerkelijk gebruikt.**
- **Gebruik buitenshuis het mobiele 3G/4G netwerk.**

Tips voor het beheren van je wifi-netwerk thuis:

- **Verander het standaard beheerderswachtwoord en de standaard loginnaam.**
- **Verander de naam van het netwerk (SSID).**
- **Gebruik minimaal WPA2 voor de beveiliging.**
- **Schakel UPnP uit.**
- **Inventariseer alle aangesloten apparaten.**
- **Stel jezelf de vraag “Moeten deze apparaten (altijd) toegang hebben tot internet?”.**
- **Stel jezelf de vraag “Moeten apparaten echt en altijd bereikbaar zijn vanaf het internet?”.**
- **Sta geen nieuwe apparaten toe in jouw netwerk.**
- **Activeer een gastennetwerk voor bezoekers.**

Veilig mobiel

Onze smartphones bevatten veel persoonlijke informatie. Daarom moeten we bewust omgaan met de gegevens in onze broekzak.

Verlies

Ben je je telefoon verloren? Dan ben je veel informatie kwijt. Privégegevens, zoals foto's en contacten. Maar ook zakelijke e-mails, notities en je agenda.

Diefstal

Is je telefoon gestolen? Dan ben je ook belangrijke gegevens kwijt. Maar er is nog een ander gevaar. Het kan namelijk ook een gerichte diefstal zijn. Misschien zoeken criminelen naar specifieke informatie. Of willen ze toegang tot jouw zakelijke e-mail via jouw smartphone.

Lekken van informatie

Veel apps vragen toegang tot enorm veel informatie. Is dit echt noodzakelijk? Hoe gaan de app-eigenaren om met hun rechten? En met de eventueel verzamelde informatie?

Tips

- **Beveilig mobiele apparaten altijd met een wachtwoord of pincode.**
- **Wees voorbereid op diefstal en verlies.**
- **Gebruik openbare wifi-netwerken zo min mogelijk.**
- **Schakel bestandsoverdracht via Bluetooth en internet uit.**
- **Let goed op bij onverwachte berichten.**
- **Geef geen vertrouwelijke informatie door aan onbekenden.**
- **Controleer je telefoonrekening.**
- **Pas standaard-handtekeningen aan.**

PC beveiliging

De beveiliging van je PC is een van de belangrijkste schakels in je algemene online beveiliging. Voor alles wat je online met de PC doet is het de basisbeveiliging.

Malware geeft toegang tot jouw computer

De belangrijkste bedreiging voor je computer is malware. Cybercriminelen willen malware op jouw PC installeren. Zo krijgen ze volledige controle over jouw computer. De cybercrimineel kan er dan alles mee doen wat hij wil. De schade die ze aanrichten kan enorm zijn.

Jouw computer ongevraagd onderdeel van netwerk

Criminelen kunnen jouw geïnfecteerde computer uitlenen aan andere cybercriminelen. Je computer is dan onderdeel van een zogenaamd *botnet*. Dit is een netwerk van geïnfecteerde computers die wachten op instructies. Zo gebruiken criminelen jouw computer voor criminele activiteiten.

Tips

- **Installeer een up-to-date antimalwarepakket.**
- **Installeer en activeer een firewall.**
- **Weet welke beveiliging je hebt. Dan weet je waar de waarschuwingen vandaan kunnen komen.**
- **Maak een gebruikersaccount aan voor beheerstaken.**
- **Update het besturingssysteem regelmatig.**
- **Update je browser regelmatig.**
- **Installeer updates van programma's zodra deze beschikbaar zijn.**
- **Zorg voor een goed spamfilter.**
- **Plak je camera af wanneer je deze niet gebruikt.**
- **Zorg regelmatig voor een goede offline back-up.**
- **Versleutel belangrijke gegevens.**
- **Gebruik uiteraard goede wachtwoorden voor alles wat met je computer te maken heeft.**
- **Installeer geen software die ongevraagd wordt aangeboden!**
- **Wees sceptisch met het installeren van gratis software.**
- **Scan gedownloade software voordat je deze installeert.**
- **Gebruik een privacyfilter om meekijken te voorkomen.**

Informatievernietiging

Informatie die we niet meer nodig hebben gooien we weg. Papieren of digitale documenten. Onze prullenbakken zijn een walhalla voor criminelen. Ze zijn immers continu en overal op zoek naar informatie.

Informatie is geld waard

Criminelen verkopen onze informatie. Er is een levendige handel in bijvoorbeeld creditcardgegevens, persoonsinformatie, paspoorten (en kopieën ervan) en logingegevens.

Criminelen gebruiken onze informatie ook voor gerichte aanvallen. Hoe onbelangrijk deze informatie voor ons ook lijkt. Door gegevens te koppelen kunnen alle puzzelstukjes voor een crimineel in elkaar vallen. Zo kunnen ze een gerichte aanval uitvoeren.

Wil je zeker weten dat criminelen niet bij jouw informatie kunnen? Zorg er dan voor dat je informatie zorgvuldig vernietigt.

Tips

- **Neem kennis van de DIN-norm 66399.**
- **Berg te verwijderen informatie goed op.**

Elektronische informatie vernietiging
- **Informatiedragers vernietigen**
  - **Laat gecertificeerde bedrijven vernietigen.**
  - **Zelf vernietigen: doorboor de drager.**
- **Informatiedragers behouden**
  - **Laat gecertificeerde bedrijven verwijderen.**
  - **Zelf verwijderen: gebruik speciale software.**

Papiervernietiging
- **Versnipper papier met waardevolle informatie altijd.**

Mobiele apparaten
- **Informeer de IT-afdeling over buitengebruikstelling.**
- **Verwijder het apparaat uit jouw wifi-netwerk.**
- **Overschrijf alle wachtwoorden, PIN-/ toegangscodes.**
- **Verwijder persoonlijke informatie.**
- **Verwijder instellingen van randapparatuur.**
- **Verwijder SIM en eventuele SD-kaarten.**
- **Gebruik een wipe-app.**
- **Zet het apparaat terug naar fabrieksinstellingen.**

Multifunctionals

Multifunctionals zijn alles-in-éénapparaten waarmee je kunt kopiëren, printen, scannen, e-mailen en vaak ook nog faxen. Heel handig, maar er zijn ook risico's in het gebruik ervan.

Documenten blijven opgeslagen in een geheugen

De meeste multifunctionals kunnen opdrachten onthouden. Handig als je je computer al hebt afgesloten, maar je dat ene document nog een keer wilt uitprinten. Of je wilt dezelfde scan nog een keer e-mailen.

Maar let op: opgeslagen documenten kunnen toegankelijk zijn voor anderen. Bijvoorbeeld voor collega's, maar ook voor schoonmakers, bezoekers, onderhoudsmedewerkers enzovoort.

De apparaten zijn voor anderen toegankelijk

Multifunctionals staan vaak in algemene ruimtes zonder toezicht waar iedereen mag komen. Let daarom goed op welke informatie je achterlaat. Zowel op papier als in het geheugen van het apparaat.

Tips

- **Laat geen documenten onbeheerd achter op het apparaat.**
- **Laat je niet afleiden tijdens het printen.**
- **Gebruik een beveiligingscode of token.**
- **Weet met welke apparaten je werkt.**
- **Geef geen informatie over gebruikte apparatuur aan derden.**

Veilige werkplek

Een veilige PC is een must. Een veilige werkplek ook. Vanaf je werkplek heb je toegang tot (bijna) alle informatie die je nodig hebt om je werkzaamheden uit te voeren.

Vergrendel je computer

Verlaat je je werkplek? En vergrendel je de computer niet? Dat is hetzelfde als je voordeur open laten staan als je boodschappen gaat doen. Iedereen kan onopvallend naar binnen sluipen. Of het nu een professionele inbreker is of je joviale buurman van wie je het niet verwacht.

Veilig mobiel werken

Flexwerken is populair. Er komen steeds meer flexplekken op kantoor. En personeel werkt vanuit huis, de trein, restaurant, of op een vliegveld.

Deze tijdelijke werkplekken moeten natuurlijk veilig zijn. Onderweg heb je bijvoorbeeld te maken met meekijkers. Mensen die het scherm van je laptop kunnen zien. Bewust of onbewust. Ze deel je ongewild informatie die niet voor anderen bestemd is.

Tips

- **Berg informatie zo op dat alleen bevoegde personen erbij kunnen.**
- **Sluit kasten met een slot ook altijd af.**
- **Berg ook persoonlijke spullen goed op.**
- **Laat geen sleutels en toegangskaarten slingeren.**
- **Neem je telefoon altijd mee.**
- **Laat geen logingegevens achter.**
- **Pak documenten direct van de printer.**
- **Wees je bewust van meekijkers zowel op kantoor als onderweg.**
- **Laat geen informatie op een whiteboard achter.**
- **Vergrendel je PC altijd als je die achterlaat.**
- **Vertrouw niet op de schermbeveiliging, activeer deze zelf.**

Identiteitsbewijzen

Op je paspoort, rijbewijs en identiteitskaart staan belangrijke persoonsgegevens. Je volledige naam, geboortedatum, woonplaats en je Burgerservicenummer (BSN).

Wie mogen een kopie van je identiteitsbewijs maken?

Overheden, financiële instellingen, notarissen, casino's en jouw huidige werkgever mogen een kopie van je identiteitsbewijs maken. Alle andere bedrijven en organisaties mogen dat niet. In de wet staat ook, dat de gegevens alleen onder strikte voorwaarden opgeslagen mogen worden.

Identiteitsdiefstal

Hebben andere bedrijven en organisaties toch een kopie van je identiteitsbewijs? Dan weet je niet zeker wat zij met de gegevens doen. Ook kunnen deze bedrijven slachtoffer worden van gegevensdiefstal, jouw gegevens welteverstaan. De kans bestaat dat je slachtoffer wordt van identiteitsfraude.

Tips

- **Een kopie maken is verboden, behalve voor:**
  - **Overheden.**
  - **Banken en creditcardmaatschappijen.**
  - **Verzekeraars.**
  - **Notarissen.**
  - **Casino's.**
  - **Je werkgever (gedurende je dienstverband)**
- **Verder zijn er geen instanties die jouw identiteitsgegevens mogen kopiëren!**
- **Er zijn nog wel instanties die alleen jouw Burgerservicenummer mogen opslaan:**
  - **Scholen**
  - **Zorgverleners**
  - **Zorgverzekeraars**
  - **Kinderopvangorganisaties**
- **Laat nooit je paspoort ergens achter.**
- **Laat geen kopie maken zonder ID-cover.**
- **Maak zelf een kopie, waarbij je**
  - **vermeldt voor wie de kopie is gemaakt;**
  - **het Burgerservicenummer doorstreept;**
  - **je foto afschermt;**
  - **achteraf de kopie terugvraagt.**

Social media

We delen veel persoonlijke informatie via social media. Twitter, Facebook of LinkedIn, bijna iedereen heeft wel ergens een profiel.

Puzzelen met jouw gegevens

Cybercriminelen vinden allerlei informatie over ons op social media. En ze gebruiken deze puzzelstukjes bij een gerichte aanval op jou of het bedrijf waar je werkt.

“Maar hoe interessant ben ik nou voor cybercriminelen?” vraag je je misschien af. Héél interessant! Meestal ben jij een middel om het uiteindelijke doel te bereiken.

Identiteitsdiefstal

Criminelen kunnen jouw identiteit overnemen, als ze de juiste informatie over jou hebben. En als deze puzzelstukjes in elkaar vallen gebruiken ze jouw identiteit voor criminele activiteiten.

Tips

- **Denk rustig na voordat je iets plaatst op social media.**
- **Wees kritisch met het plaatsen van persoonlijke informatie.**
- **Bedenk goed met wie je berichten deelt.**
- **Wees terughoudend met foto's van je kinderen.**
- **Zorg dat foto's geen verborgen informatie bevatten.**
- **Schakel de locatievoorzieningen uit.**
- **Iets wat geplaatst is op social media is permanent.**
- **Controleer regelmatig de privacy instellingen.**
- **Bekijk berichten van vrienden en relaties kritisch.**
- **Niet alles is wat het lijkt.**
- **Houd privénetwerken en zakelijke netwerken gescheiden.**
- **Wees kritisch met het accepteren van "vrienden" en "relaties".**
- **Type zelf de adressen van social media sites in.**
- **Controleer ingekorte links.**

Notities

Hier geen wachtwoorden noteren!

Notities

En ook hier geen wachtwoorden noteren!

Notities

Dus ook hier geen wachtwoorden noteren!

Voor vragen kun je contact opnemen met:

BEVEILIGMIJ.NL
Security awareness

Fahrenheitstraat 18
6662 PZ Elst
0481 - 46 38 19
info@beveiligmij.nl
www.beveiligmij.nl

BEVEILIGMIJ.NL
Security awareness