infosequre

know what you show

e-Learning programma's voor duurzame gedragsverandering

Overzicht e-Learningmodules

infosequre

Stel je toekomst veilig. Wapen je medewerkers tegen risico's met meer dan 30 security awareness onderwerpen.

Introductieprogramma

De belangrijkste security awareness onderwerpen worden op een interactieve, herkenbare en toegankelijke manier behandeld in onze introductieprogramma's. In slechts 20-30 minuten, leren je medewerkers de juiste manier van veilig werken. Een introductieprogramma is de perfecte start van een bewustwordingscampagne.

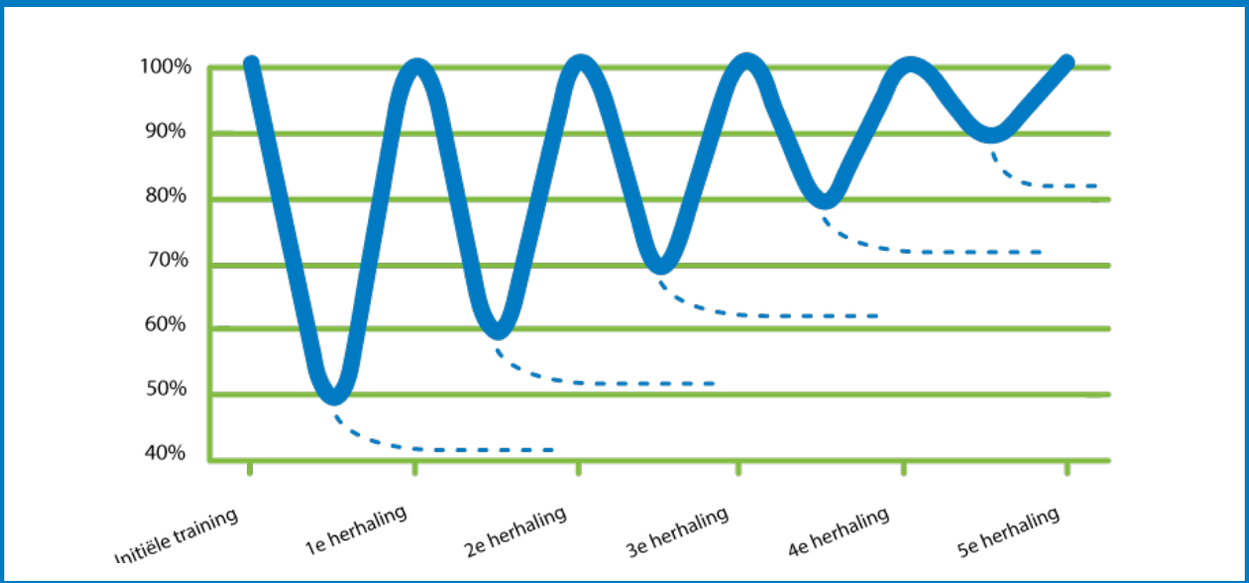
- Introductieprogramma Informatiebeveiliging in de frontlinie
- Informatiebeveiliging voor ziekenhuizen (geaccrediteerd door V&VN)
- security by design functionaliteit vs. veiligheid
- Cybersecurity voor directie en bestuur
- Informatiebeveiliging in de zorg
- Informatiebeveiliging voor gemeenten

In depth e-learning

De verdiepingmodules gaan dieper in op veilig gedrag tijdens de dagelijkse werkzaamheden. De modules duren 10-15 minuten en starten met een algemene introductie. De modules zijn interactief, bevatten boeiende video's en testvragen. In-depth modules kunnen ook worden ingezet voor specifieke doelgroepen.

- NIEUW: Ransomware
- Phishing
- Social engineering
- Mobiele apparatuur
- Cybersecurity
- Werken in de cloud
- Informatieclassificatie
- Malware
- Risicomanagement
- Fysieke beveiliging
- Algemene Verordening Gegevensbescherming (AVG)
- Algemene Verordening Gegevensbescherming (AVG) voor gemeenten

Vergeetcurve



Regelmatig herhalen helpt bij het onthouden van informatie. Met onze microlearning en security flashes fris je kennis in 1 tot 5 minuten weer op.

Microlearning

- NIEUW: Privacy en gegevensbescherming
- Gebruik van wachtwoorden
- Thuiswerken
- Shadow IT
- Werk veilig buiten kantoor
- Beveilig je mobiele apparaten
- Weet met wie je zaken doet
- Meld informatiebeveiligingsincidenten
- Hoe classificeer je informatie?
- Ransomware
- Internet of Things
- Privacy in de praktijk
- Privacy in het ziekenhuis
- Onrechtmatige toegang tot het EPD

Security flashes

- Bring your own device
- Clear desk, screen & office
- Phishing
- Meld security-incidenten
- Sterke wachtwoorden
- Werken in het openbaar
- Social engineering
- Toegangscontrole
- Social media & werken in de cloud
- Informatieclassificatie
- Malware

Baseline tests

Onze baseline tests geven een goed beeld van de kennis van de medewerkers op een bepaald moment of van de hiaten daarin.

- Algemene Verordening Gegevensbescher-ming (AVG)
- Cyber security
- Fysieke beveiliging
- Malware
- Phishing
- Risicomanagement

Introductieprogramma's

Introductieprogramma Informatiebeveiliging - In de frontlinie

Technische maatregelen zijn slechts een deel van de oplossing voor een effectief informatiebeveiligingsbeleid. De manier waarop medewerkers omgaan met bedrijfsinformatie is minstens zo belangrijk. Iedere werknemer kan doelwit zijn van cybercriminelen. In dit programma volg je 2 collega's tijdens een werkdag. Van 's ochtends vroeg tot 's avonds laat krijgen zij te maken met incidenten die we allemaal herkennen vanuit ons dagelijkse werk. Aan de hand van praktijkvoorbeelden leer je hoe je met deze situaties omgaat.

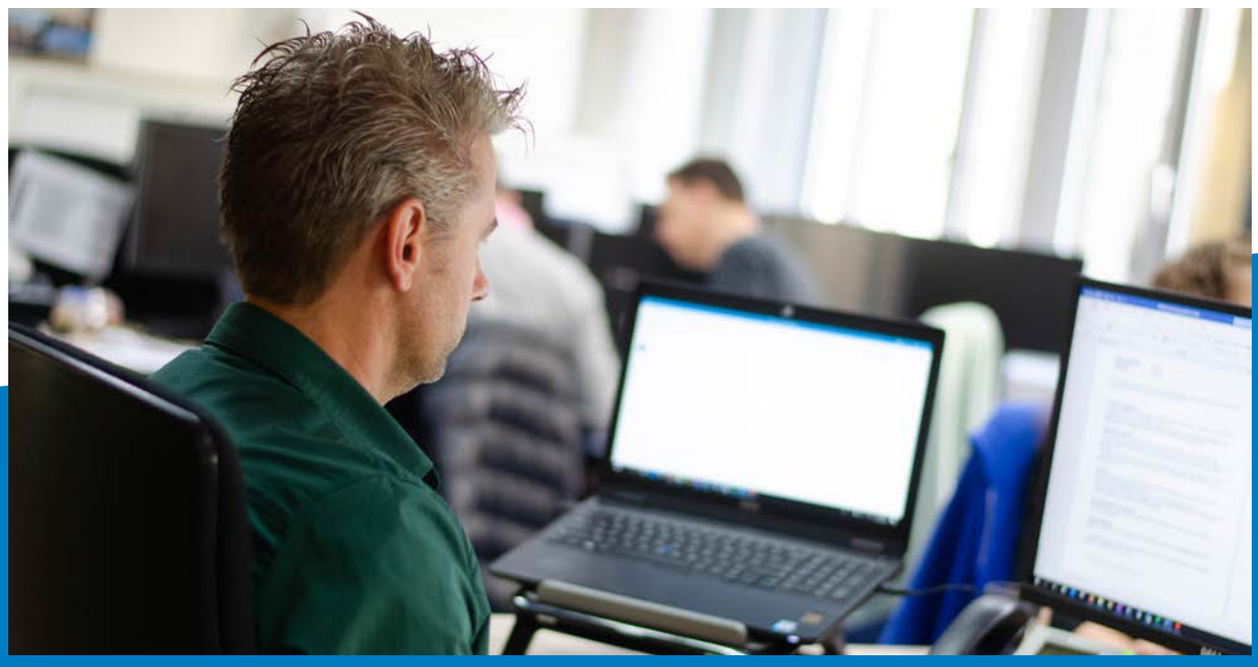
Na 15-20 minuten kun je de volgende vragen beantwoorden:

- Hoe behandel je informatie met zorg?
- Wat doe je als je een verdachte situatie ziet?
- Hoe ga je veilig met wachtwoorden om?
- Wat zijn de regels van clear desk, screen & office?
- Hoe ga je om met bezoekers?
- Waaraan herken je verdachte e-mails?
- Hoe print je veilig gevoelige informatie?
- Waarvoor gebruik je een Virtueel Privé Netwerk (VPN)?
- Hoe werk je veilig in het openbaar?

Security by design - Functionaliteit vs veiligheid

Wanneer je een nieuwe applicatie ontwerpt, een nieuwe software ontwikkelt of een systeem beheert, wil je dat het goed functioneert. Gebruiksvriendelijkheid en gebruikerservaring staan voorop. Maar wat is gebruiksvriendelijkheid waard als hackers deze kunnen omzeilen? Een stevige infrastructuur vraagt om een goede balans tussen functionaliteit en veiligheid.

Deze training biedt tools om de juiste balans te vinden in functionaliteit en veiligheid. Medewerkers krijgen advies en concrete tips van ethical hacker Tim om applicaties, software en systemen op een veilige manier te ontwerpen, ontwikkelen en beheren.



In 20-25 minuten geeft ethical hacker Tim antwoord op vragen als:

- Welke verschillende soorten security assessments kun je inzetten?
- Waarom is patch management belangrijk?
- Wat is Coordinated Vulnerability Disclosure en hoe helpt het bij het onderhoud van een systeem?
- Waarom is de OWASP zo waardevol?
- Hoe helpt het principe van 'defense in depth' bij het ontwikkelen van een veilige infrastructuur?

Cybersecurity for executives - Cyber security voor directie en bestuur

Directie en bestuur spelen een cruciale rol bij informatiebescherming. In deze introductietraining leren medewerkers niet alleen waarom cyber security belangrijk is en hoe je omgaat met cyberrisico's, ze krijgen ook praktische tips om de organisatie te beschermen tegen cyberdreigingen. Na het afronden van deze training kun je zelf een plan opstellen waarmee je direct aan de slag kunt.

Na de training kun je de volgende vragen beantwoorden:

- Wat is cyber security?
- Waarom is cyber security belangrijk?
- Welke cyberaanvallen zijn direct op directie en bestuur gericht?
- Hoe belangrijk is cyber security voor jouw organisatie?
- Welke maatregelen heeft jouw organisatie nodig?
- Hoe werk je binnen jouw organisatie aan cyber security?
- Wat doe je bij een incident?

Informatiebeveiliging in de zorg

In de zorg werken we veel met vertrouwelijke informatie. Als iedereen weet hoe je veilig met deze informatie omgaat, houd je samen de informatie van bewoners/cliënten en de organisatie veilig. In dit programma zie je mensen die in de zorg werken. Dit zijn mensen die werken met bewoners/cliënten, maar ook mensen die ondersteunende taken uitvoeren. Je ziet hoe zij met informatie omgaan en leert met uitleg, oefeningen, video's en dilemma's hoe je zelf veilig met informatie omgaat.

Na 15-20 minuten kun je de volgende vragen beantwoorden:

- Waarom is het belangrijk om informatie en privacy te beschermen?
- Wat is gevoelige informatie?
- Hoe bescherm je (gevoelige) informatie tegen fysieke bedreigingen?
- Hoe bescherm je (gevoelige) informatie tegen cyberdreigingen?
- Wat zijn incidenten?
- Wat zijn datalekken?
- Wat moet je doen bij een (mogelijk) incident?

Informatiebeveiliging voor gemeenten

Datalekken komen vaak voor. Om datalekken bij gemeenten te voorkomen, is de BIO (Baseline Informatiebeveiliging Overheid) bedacht. De BIO bestaat uit een aantal basisregels die je helpen om veilig met gevoelige informatie om te gaan. In dit programma leer je aan de hand van praktijkvoorbeelden hoe je de basisregels van de BIO tijdens je werkdag gebruikt om informatie te beschermen.

Na 15-20 minuten kun je de volgende vragen beantwoorden:

- Met wie mag je gevoelige informatie delen en waar moet je op letten als je informatie deelt?
- Wanneer en bij wie meld je informatiebeveiligingsincidenten?
- Hoe maak je sterke wachtwoorden en hoe ga je hier veilig mee om?
- Waaraan herken je verdachte e-mails en hoe ga je daarmee om?
- Hoe deel je gevoelige informatie?
- Wat zijn de regels van clear desk, screen & office?
- Hoe ga je om met bezoekers?
- Op welke risico's let je aan het einde van je werkdag?
- Hoe werk je veilig in het openbaar?
- Hoe werk je veilig met mobiele apparaten?

In-depth e-learning

NIEUW: Ransomware - Laag voor laag

Ransomware-aanvallen zijn de nachtmerrie van elke security officer. Iedereen denkt dat ze het vast beter weten dan de sukkels die in zo'n aanval trappen. Je hoeft echter maar ÉÉN phishingmail over het hoofd te zien of ÉÉN beheerdersaccount met een zwak wachtwoord beveiligd te hebben om de hoofdprijs te moeten betalen. Het gaat niet alleen om veel geld, maar ook om de tijd en het werk die het kost om het hele computersysteem weer te herstellen.

Peprico & partners doet er alles aan om de risico's zo klein mogelijk te houden en is een onderzoek gestart. Laten we met ze meekijken in hun zoektocht naar de antwoorden op hun vragen!

Na 15-20 minuten kun je de volgende vragen beantwoorden:

- Hoe krijgen hackers toegang tot onze computers en ons netwerk?
- Wat zijn de signalen dat een mogelijke ransomware-aanval plaatsvindt?
- Welke preventieve maatregelen kun je nemen om je te beschermen tegen ransomware-aanvallen?

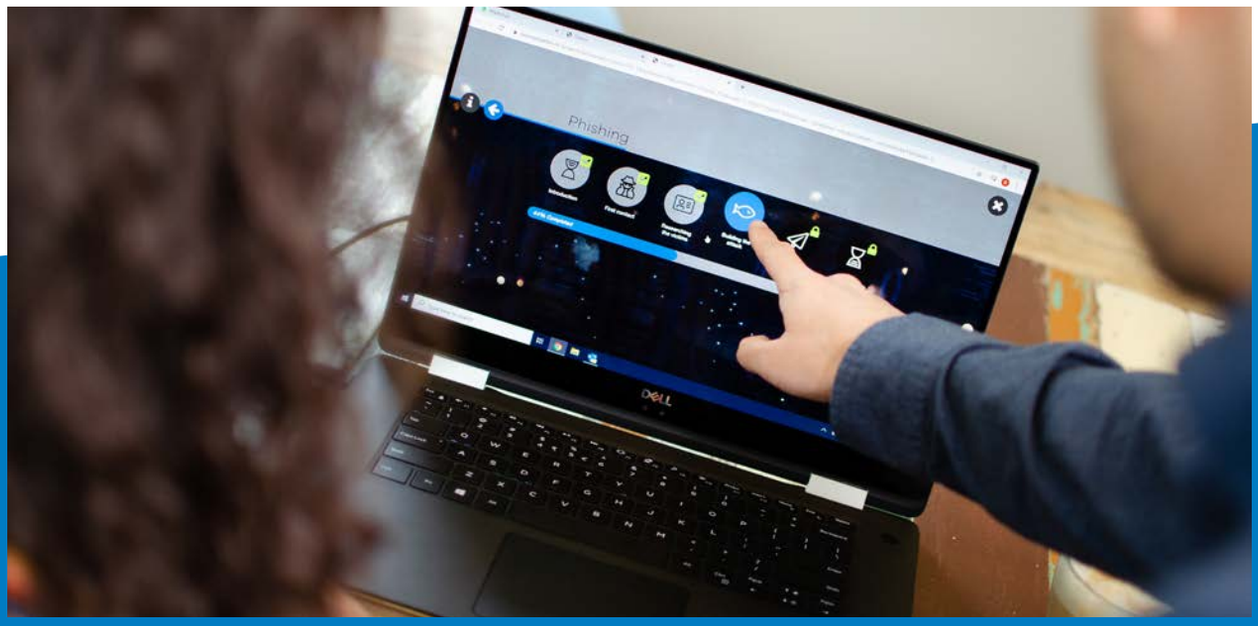
Phishing

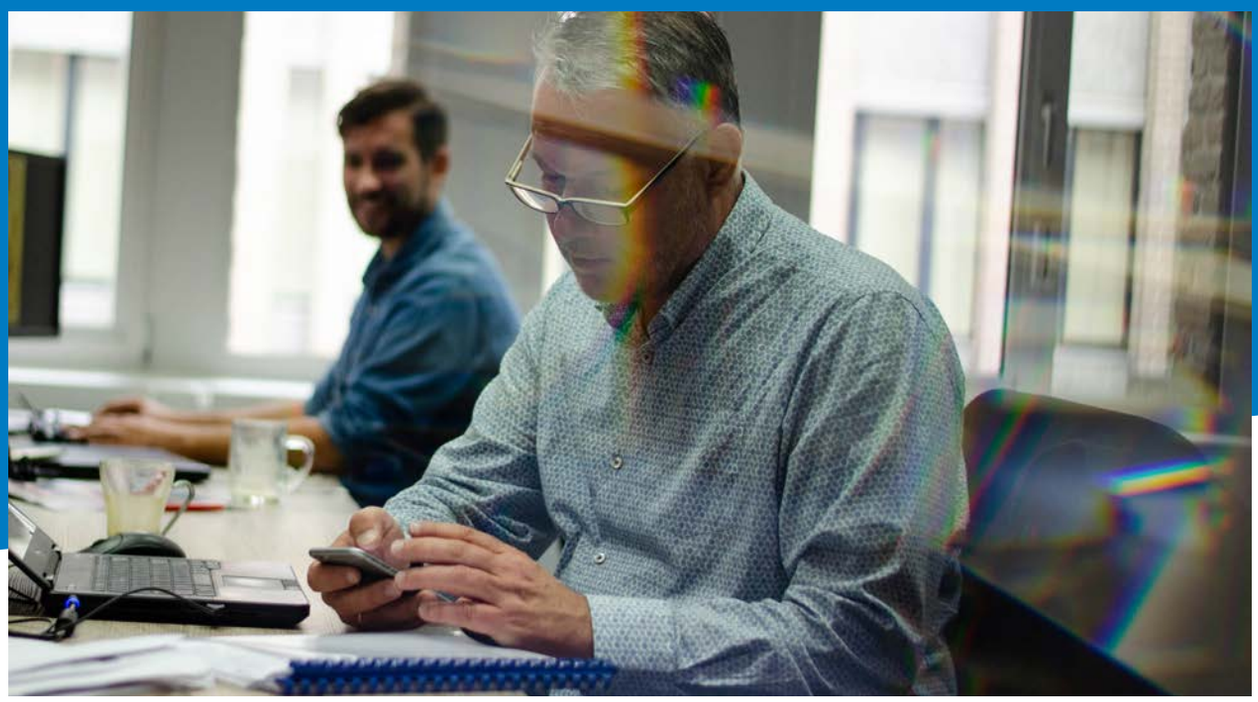
Tot een paar jaar terug waren phishingmails eenvoudig te herkennen. Ze stonden vol met taalfouten, slecht geplakte logo's en hadden onderwerpregels in hoofdletters. Tegenwoordig zijn phishingmails veel realistischer en lastiger te herkennen. Je hoeft geen programmeur te zijn om een phishing mail te sturen, dus steeds meer oplichters wagen een poging. Winst kan oplopen tot in de miljoenen euro's. Maar hoe maak je een phishingmail? Hoe denken phishers als ze een aanval voorbereiden?

Kruip in de huid van een phisher. Ben jij er klaar voor?

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Hoe herken je phishing?
- Hoe vinden phishers informatie over hun slachtoffers?
- Wat is het verschil tussen phishing via social media en phishing via e-mail?
- Hoe bescherm je jezelf tegen phishing?





Social engineering - The social dilemma

De tijd dat cybercriminelen alleen computers hacken, ligt achter ons. Er is een manier die misschien wel nog effectiever is: het hacken van mensen!
Manipuleren en beïnvloeden van mensen kan leiden tot enorme winsten. Social engineers versturen phishingmails, proberen informatie telefonisch te ontfutselen en de echte waaghalsen lopen zelfs fysieke kantoren binnen om gevoelige informatie te stelen. Medewerkers spelen een belangrijke rol in het beschermen van bedrijfsgegevens voor dit soort aanvallen. Volg de module en leer meer.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is social engineering?
- Welke tactieken gebruiken social engineers?
- Hoe herken je een social engineer?
- Hoe deal je met verdachte situaties?

Mobiele apparaten

Het is je eerste werkdag bij je nieuwe baan. Maar zodra je je nieuwe team ontmoet, blijkt er een probleem te zijn. Er is informatie gelekt over een nieuw project en alles is nu te vinden op het internet. Gelukkig valt de schade mee. Het is geen gevoelige informatie, maar het kan leiden tot een lek met veel consequenties. Het is aan jou om uit te zoeken waar het mis is gegaan.

Na 15-20 minuten kan je de volgende vragen beantwoorden:

- Waarom is het zo belangrijk om mobiele apparaten te beschermen?
- Wat zijn de gevaren van apps?
- Hoe bescherm je je mobiele apparatuur tegen de gevaren van openbare Wi-Fi netwerken?
- Hoe bescherm je informatie op je mobiele apparatuur, als deze gestolen is of je je device kwijt bent?

Cybersecurity

In deze training leer je over de betekenis, de risico's en het belang van cyber security. Je volgt Rosa onder werktijd en ziet hoe ze de veiligheid van digitale informatie beschermt. Je leert over maatregelen die je kunt nemen tijdens het dagelijkse werk om de veiligheid van digitale informatie te beschermen.

In 15-20 minuten krijg je antwoord op de volgende vragen:

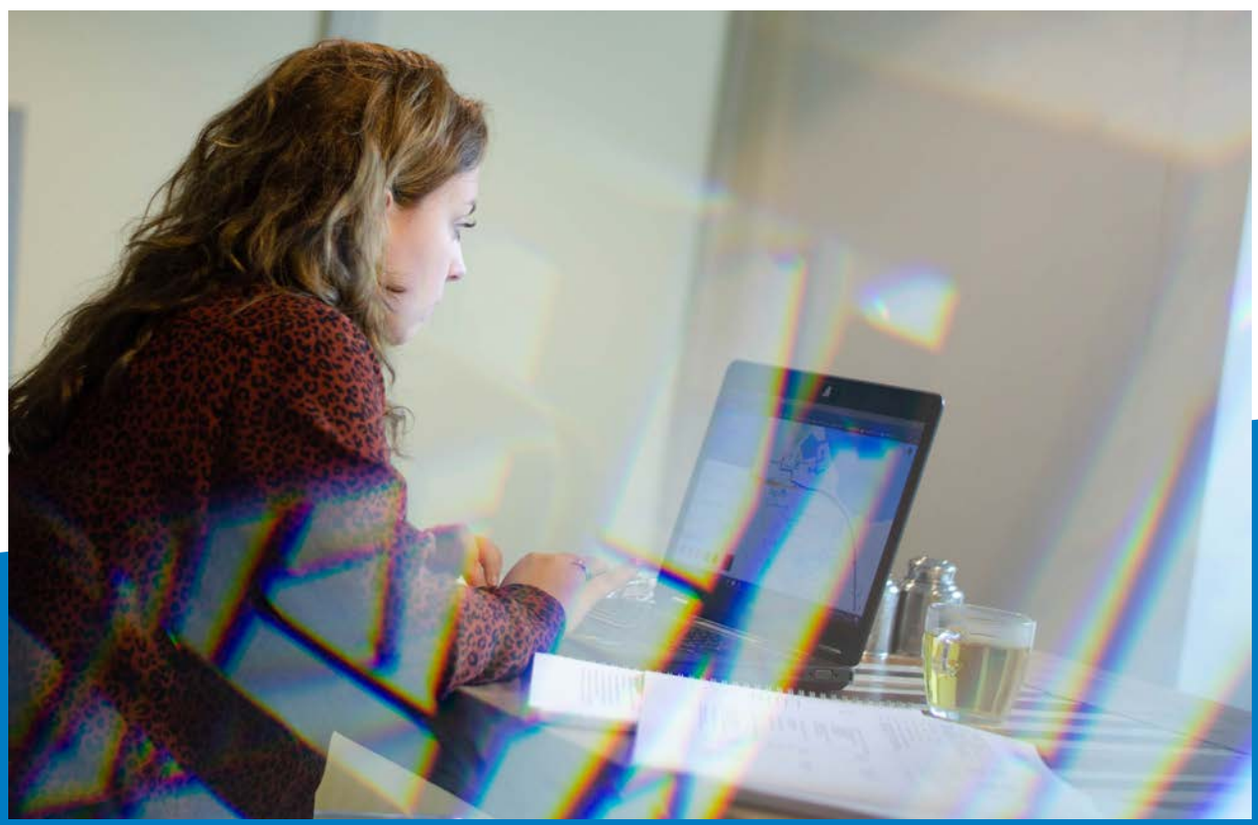
- Wat is cyber security?
- Waaraan herken je een phishingmail en hoe reageer je hierop?
- Hoe bescherm je inloggegevens en accounts?
- Hoe sla je informatie veilig op?
- Wat is het Internet of Things en hoe ga je er veilig mee om?
- Hoe maak je veilig gebruik maken van het internet?
- Hoe voorkom je dat je slachtoffer wordt van social engineering?

Werken in de cloud

Met de cloud heb je altijd en overal toegang tot informatie. Dit biedt grote mogelijkheden, maar heeft ook risico's. Als je weet hoe je veilig werkt in de cloud, kun je de voordelen ervan optimaal benutten. In deze training leer je alles wat je moet weten om veilig in de cloud te werken.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is werken in de cloud?
- Wat is een publieke clouddienst en wat zijn de voor- en nadelen?
- Wat is een privé clouddienst en wat zijn de voor- en nadelen?
- Hoe werk je veilig in de cloud?



Informatieclassificatie

Het werken met informatie is een belangrijk en groot onderdeel van een organisatie. Het is daarom belangrijk dat je informatie op de juiste manier classificeert. Hiermee geef je aan welk beschermingsniveau nodig is. Iedereen weet dan welke niveaus van vertrouwelijkheid, integriteit en beschikbaarheid ze moeten toepassen als ze met de informatie werken. Het doel hiervan is dat informatie niet kwijtraakt of in verkeerde handen komt.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is informatieclassificatie?
- Waarom is het belangrijk?
- Hoe classificeer je informatie?
- Hoe ga je om met geclassificeerde informatie?

Malware

Malware staat voor 'malicious software', of kwaadaardige software. Het is een verzamelnaam voor verschillende soorten schadelijke software. Ransomware is een bekende vorm van malware.
Malware kan tot veel schade in een organisatie leiden. Zo kunnen persoonsgegevens gestolen worden of gevoelige informatie op straat komen te liggen. Deze training zorgt ervoor dat je op de hoogte bent van de gevaren van de verschillende vormen van malware. Je leert malware herkennen en besmettingen voorkomen.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is malware?
- Welke vormen van malware bestaan er?
- Wat doet malware?
- Hoe kun je malware herkennen?
- Hoe kun je malware voorkomen?

Risicomanagement

In deze training leer je wat risicomanagement is, met welke risico's je te maken kunt krijgen en wat jouw rol hierin is. De training is ontwikkeld voor (project) managers, maar andere medewerkers kunnen de training ook volgen om beter met risico's te leren omgaan. Je ontdekt wat de rol van de risicomanager is binnen de organisatie, je leert risico's in kaart brengen door middel van een zelfaudit en je leert wanneer je de risicomanager inschakelt voor advies of ondersteuning.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is het doel van risicomanagement?
- Wat is de rol van de risicomanager?
- Wat is een risico?
- Hoe breng je risico's in kaart?
- Wat zijn de gevolgen van risico's?
- Welke beheersmaatregelen kun je nemen?
- Wanneer benader je de risicomanager voor advies of ondersteuning?

Fysieke beveiliging

Fysieke beveiliging beschermt mensen en bezittingen van een organisatie, maar ook de informatie. Informatie heeft, naast technische beveiliging, ook fysieke beveiliging nodig. De belangrijkste bedreigingen waar fysieke beveiliging een organisatie tegen beschermt, zijn opzettelijke bedreigingen door mensen. Denk hierbij aan diefstal en onbedoelde toegang. In deze training leer je welke maatregelen een organisatie kan treffen voor de fysieke beveiliging en wat jouw rol hierin is.

In 15-20 minuten krijg je antwoord op de volgende vragen:

- Wat is fysieke beveiliging?
- Waarom is fysieke beveiliging belangrijk?
- Hoe draag je zelf bij aan fysieke beveiliging?

Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensbescherming, of AVG in het kort, geldt sinds 25 mei 2018. Sindsdien mag iedereen organisaties op de naleving van deze nieuwe Europese privacywetgeving aanspreken. In deze training leer je over de hoofdlijnen van de AVG en de juiste manier van beschermen, verwerken en opslaan van persoonsgegevens.

In 15-20 minuten krijg je antwoord op de volgende vragen:

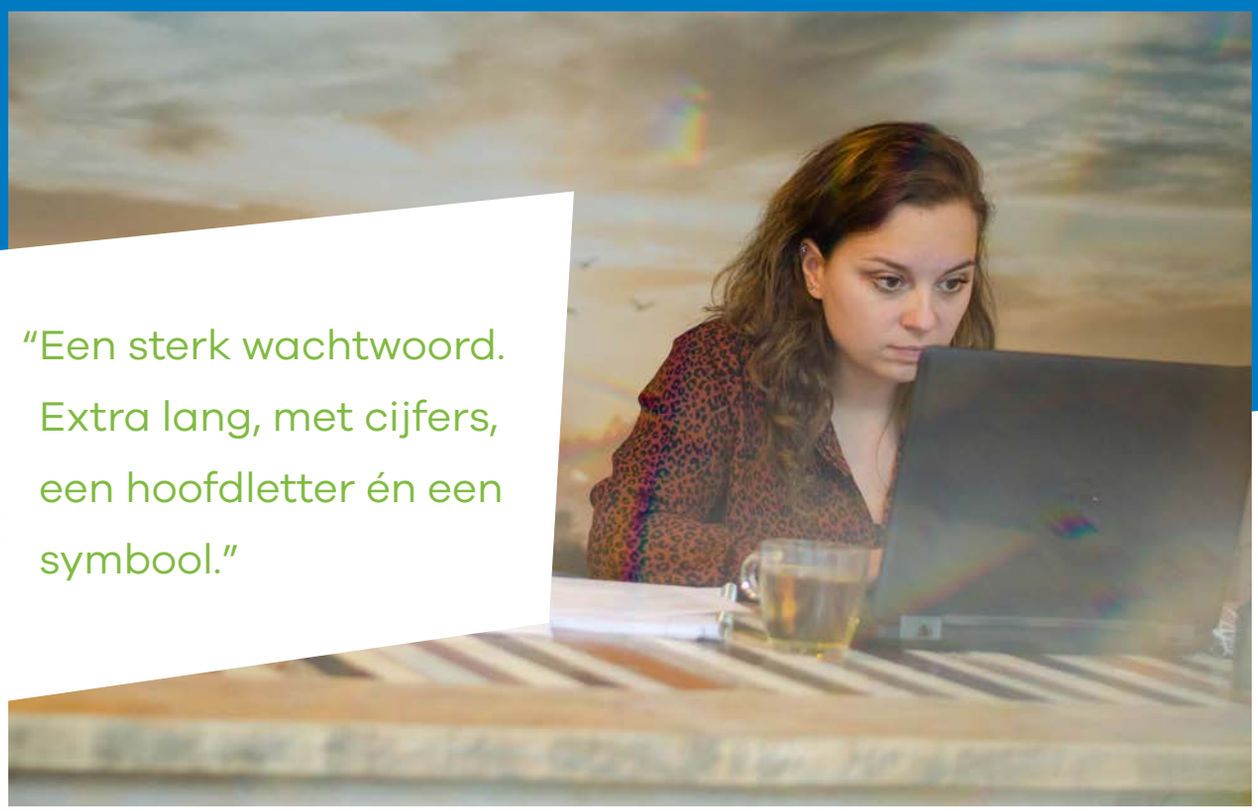
- Wat is de AVG?
- Wat zijn persoonsgegevens?
- Wat houdt de verwerking van persoonsgegevens in?
- Waarom is een goede bescherming van persoonsgegevens belangrijk?
- Wat zijn de basisregels van de AVG?
- Wat zijn de rechten van betrokkenen?
- Wat zijn de taken en verantwoordelijkheden bij verwerking?
- Wat moet je doen om persoonsgegevens te beschermen?

Algemene Verordening Gegevensbescherming (AVG) voor gemeenten

De Algemene Verordening Gegevensbescherming, of AVG in het kort, geldt sinds 25 mei 2018. Sindsdien mag iedereen organisaties op de naleving van deze nieuwe Europese privacywetgeving aanspreken. In deze training leer je over de hoofdlijnen van de AVG en de juiste manier van beschermen, verwerken en opslaan van persoonsgegevens.

Na de training kun je de volgende vragen beantwoorden:

- Wat is de AVG?
- Wat zijn persoonsgegevens?
- Wat houdt de verwerking van persoonsgegevens in?
- Waarom is een goede bescherming van persoonsgegevens belangrijk?
- Wat zijn de basisregels en grondslagen van de AVG?
- Wat zijn de rechten van betrokkenen?
- Wat zijn de taken en verantwoordelijkheden bij verwerking?
- Wat moet je doen om persoonsgegevens te beschermen?



Microlearning

NIEUW: Privacy en gegevensbescherming

Hecht jij waarde aan privacy? Het is goed om te weten dat je persoonsgegevens worden beschermd door verschillende wetten. Maar hoe pak je dit aan in de praktijk? In deze microlearning help je Oliver en Eveline om de juiste keuzes te maken.

Na 5 minuten kun je vragen beantwoorden als:

- Wat zijn (gevoelige) persoonsgegevens?
- Hoe zorg je dat persoonlijke data veilig blijft?
- Wat kun je doen als het toch misgaat en je een datalek veroorzaakt?

Gebruik van wachtwoorden

Je weet waarschijnlijk wel hoe je een sterk wachtwoord maakt. Maar er is meer. Als je goed omgaat met wachtwoorden is informatie veiliger. Ga er dus even voor zitten. Pak een kop koffie en ontdek hoe je slim met wachtwoorden omgaat.

Na 5 minuten kan je de volgende vragen beantwoorden:

- Welke accounts bescherm je als eerste?
- Hoe maak je een sterk wachtwoord?
- Wat is tweefactorauthenticatie?
- Hoe check je of je wachtwoorden zijn gelekt?
- Wat zijn de voordelen van een passwordmanager?

Thuiswerken

Als je thuiswerkt is er geen collega in de buurt om je te wijzen op de veiligheid. Dit betekent dat jij verantwoordelijk bent voor veilig werken. In deze microlearning volg je onze collega Mina. Zij laat de security-basics zien zodat je veilig thuis aan de slag kan.

Na 5 minuten weet je de antwoorden op de volgende vragen.

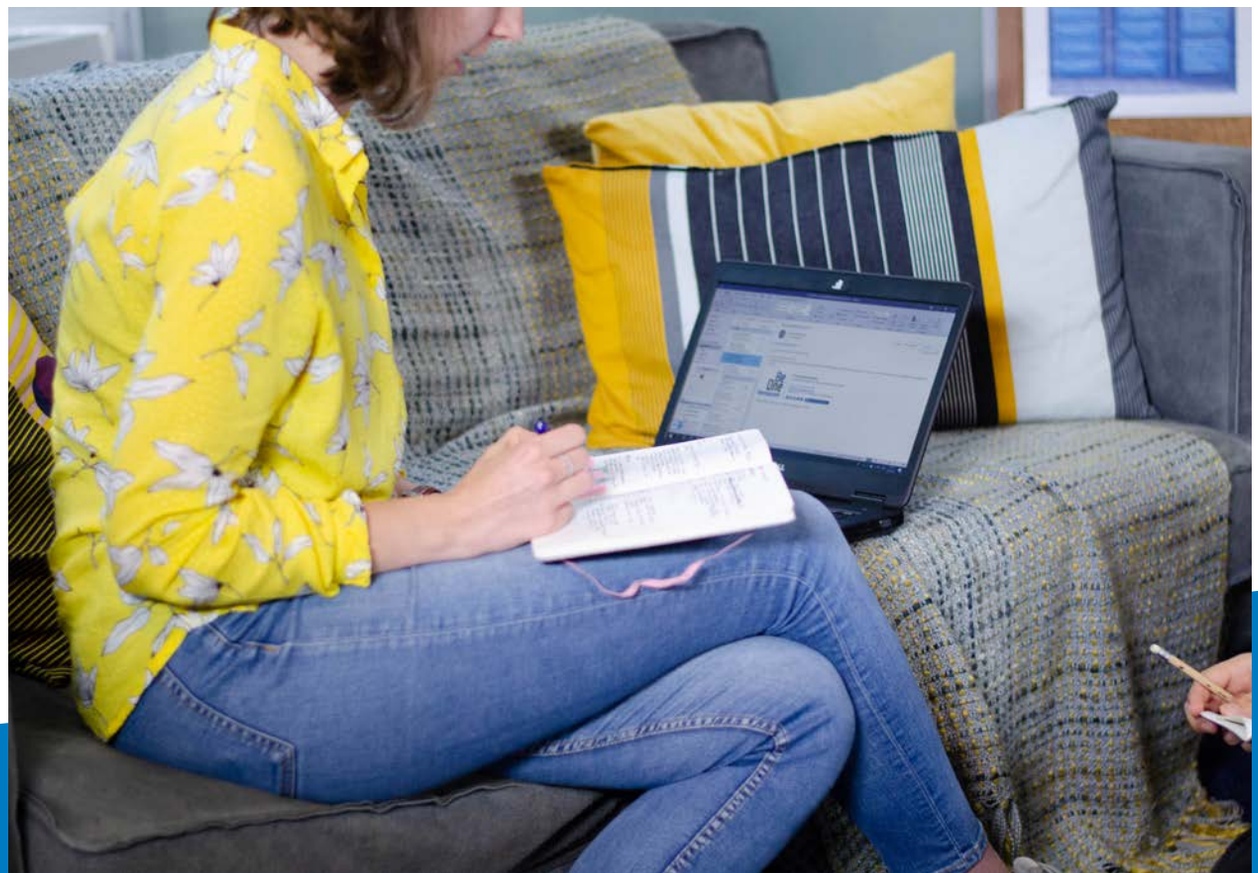
- Hoe verzeker je je ervan dat je niet meer informatie deelt dan je wilt tijdens een online meeting?
- Wat doe je met zakelijke documenten en apparatuur als je werkdag is afgelopen?

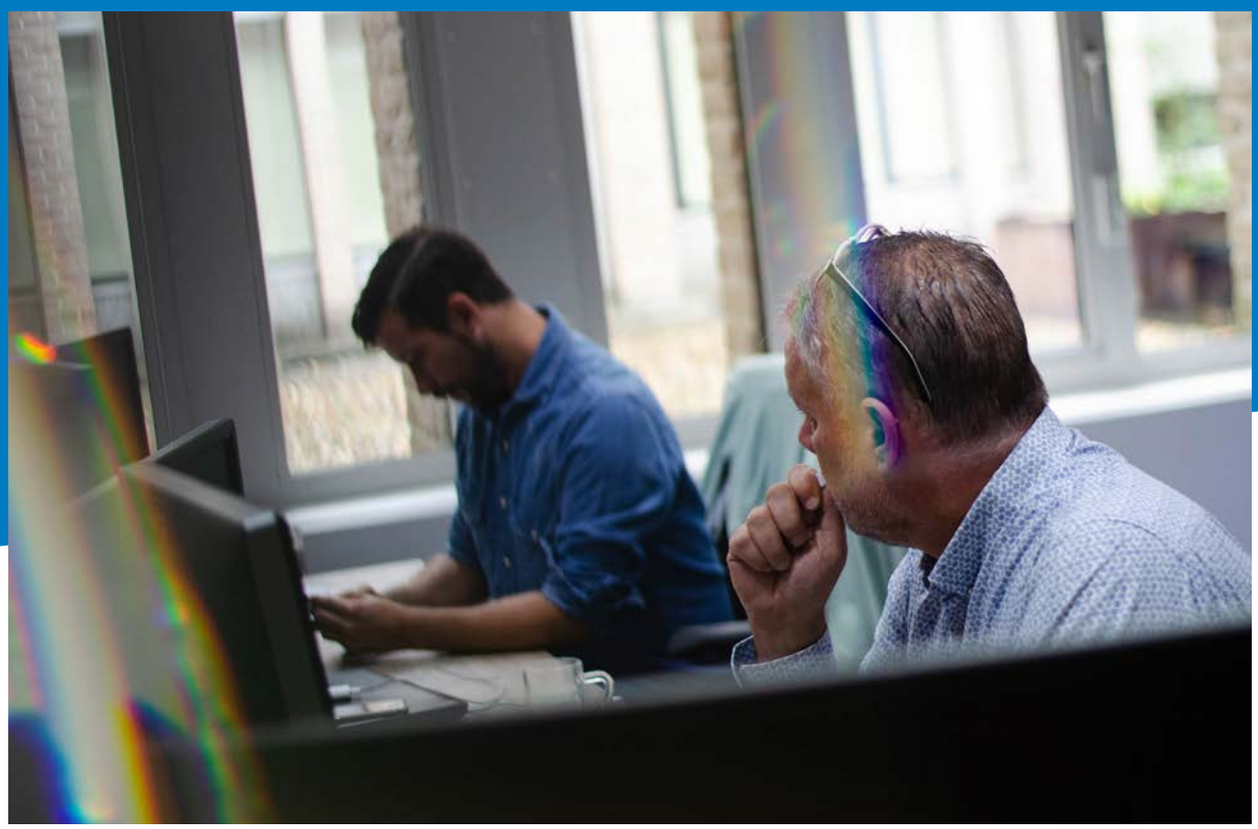
Shadow IT

We doen het allemaal wel eens: Even snel een bestand delen via een gratis applicatie of aan een belangrijk document werken op je privételefoon. Heel makkelijk en handig, maar er is ook een keerzijde aan het gebruik van deze oplossingen waar je misschien niet zo 1, 2, 3 aan denkt...

Na 5 minuten kan je de volgende vragen beantwoorden:

- Wat is Shadow IT?
- Wat zijn de risico's van Shadow IT?





Beveilig je mobiele apparaten

Mobiele apparaten zijn altijd binnen handbereik. Er zijn veel voordelen aan verbonden, maar sommige van deze voordelen brengen risico's met zich mee. Ben je je bewust van deze risico's? Dan weet je ook hoe je je ertegen beschermt. Deze microlearning legt uit waarom het beveiligen van mobiele apparatuur belangrijk is.

Na 5 minuten kun je de volgende vragen beantwoorden:

- Hoe beveilig je al je mobiele apparatuur op de juiste manier?
- Wat zijn de risico's die zich voordoen bij het gebruik van mobiele apparatuur?

Weet met wie je zaken doet

Social engineers doen zich voor als iemand anders. Ze doen dit via e-mail, tijdens telefoongesprekken of zelfs face-to-face. Maar hoe kom je erachter met wie je te maken hebt? Hoe voorkom je dat je het slachtoffer wordt van social engineering? Als je een social engineer herkent, voorkom je dat je gevoelige informatie vrijgeeft. Deze microlearning laat in een paar minuten zien hoe je erachter komt met wie je te maken hebt en leert je hoe je met verdachte situaties omgaat.

Na 5 minuten kun je de volgende vragen beantwoorden:

- Hoe komen mensen met kwade bedoelingen aan gevoelige informatie?
- Hoe zorg je ervoor dat je informatie alleen deelt met de juiste personen?

Meld informatiebeveiligingsincidenten

Iedereen in een organisatie kan te maken krijgen met een informatiebeveiligingsincident. Onderneem altijd direct actie als je het gevoel hebt dat er iets niet klopt en meld incidenten. Zo zorg je ervoor dat je organisatie snel actie kan ondernemen. Deze microlearning laat zien wat een informatiebeveiligingsincident is en hoe je op zo'n incident reageert.

Na 5 minuten kun je de volgende vragen beantwoorden:

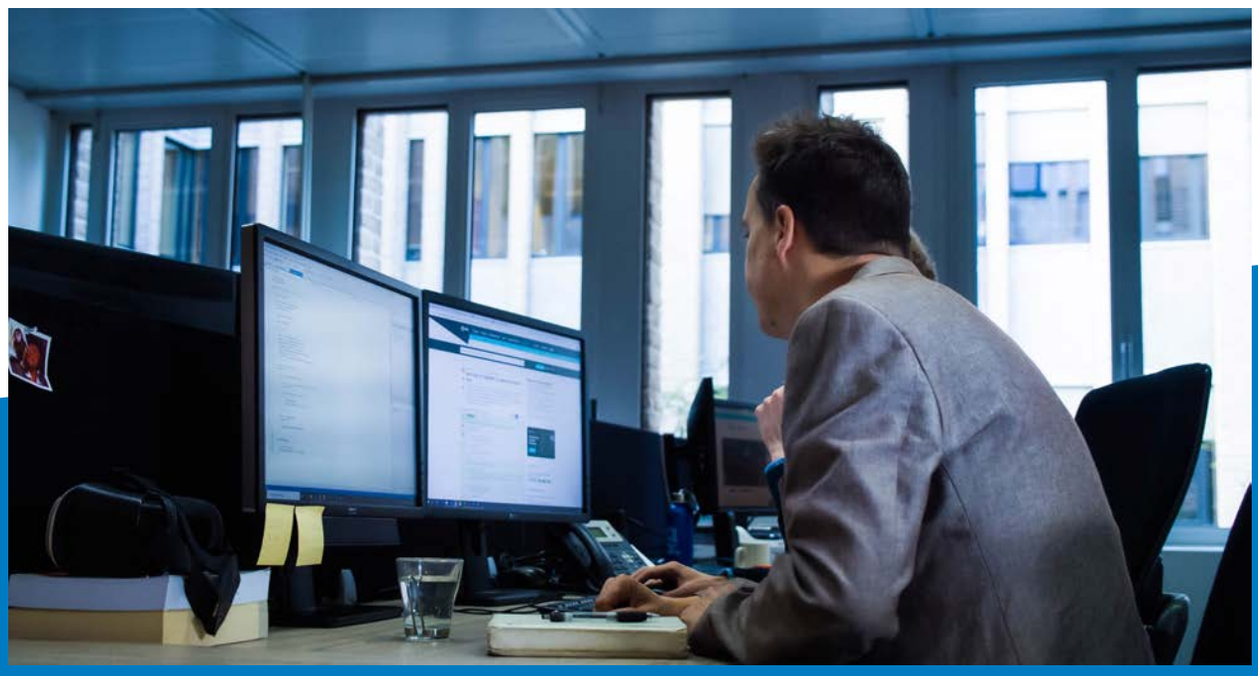
- Wat moet je doen als je iets eigenaardigs opvalt?
- Wat moet je doen als je ziet dat er bedrijfsmiddelen zijn verdwenen?
- Hoe voorkom je informatiebeveiligingsincidenten?

Hoe classificeer je informatie?

Het werken met informatie is een belangrijk onderdeel van een organisatie. Door informatie op de juiste manier te classificeren, geef je aan welk beschermingsniveau nodig is. Iedereen weet dan welke niveaus van vertrouwelijkheid, integriteit en beschikbaarheid ze moeten toepassen als ze met de informatie werken. Het doel hiervan is dat informatie niet kwijt raakt of in verkeerde handen komt. In deze microlearning leer je waarom het classificeren van informatie belangrijk is voor je organisatie.

Na de training kun je de volgende vragen beantwoorden:

- Waarom is het belangrijk om informatie juist te classificeren?
- Wat zijn de meest voorkomende classificatietypes?
- Wat zijn de risico's van het verliezen van bepaalde geclassificeerde informatie?
- Hoe handel je als mensen om gevoelige informatie vragen?



Ransomware

Ransomware is een bekende vorm van malware en is vaak in het nieuws. Ransomware vraagt om losgeld om een blokkade van een computer of computersysteem te verwijderen. Je weet alleen nooit zeker of de blokkade ook weggaat als je betaalt. Het is beter om de kans op ransomware te verkleinen. In deze training leer je over de manieren om de kans op ransomware zo klein mogelijk te maken.

Na 5 minuten kun je de volgende vragen beantwoorden:

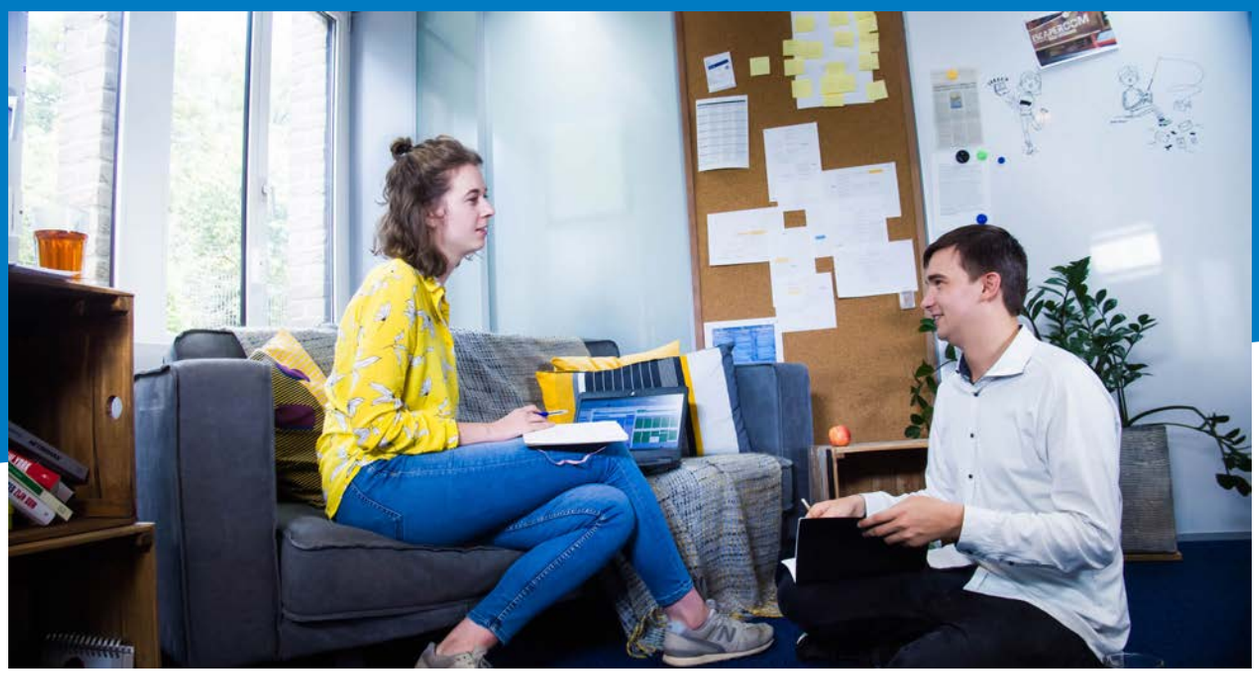
- Wat is ransomware?
- Hoe verklein je de kans op ransomware?

Internet of things (IoT)

Er komen steeds meer slimme apparaten die via het internet een netwerk vormen. Denk aan: smartwatches en externe harde schijven. Veel van deze apparaten zijn niet goed beveiligd. Gehackte of besmette 'slimme' apparaten zijn een bedreiging voor bedrijfsapparaten. Het is vaak onduidelijk wie binnen de organisatie verantwoordelijk is voor het beveiligen van deze 'slimme' apparaten. In deze microlearning leer je hoe je als medewerker zo veilig mogelijk met IoT-apparaten werkt.

Na 5 minuten kun je de volgende vragen beantwoorden:

- Wat is het IoT?
- Hoe besmetten IoT-apparaten bedrijfsapparatuur?
- Wat zijn de risico's van het IoT?
- Hoe ga je om met de zwakke plekken van het IoT?



Privacy in practice

De Algemene Verordening Gegevensbescherming, of AVG in het kort, geldt sinds 25 mei 2018. Sindsdien mag iedereen organisaties op de naleving van deze nieuwe Europese privacywetgeving aanspreken. In deze training leer je aan de hand van herkenbare praktijksituaties hoe je de AVG toepast.

Na 5 minuten kun je de volgende vragen beantwoorden:

- Wat zijn (bijzondere) persoonsgegevens?
- Waarom is bescherming van persoonsgegevens belangrijk?
- Hoe ga je in de praktijk om met privacy?

Privacy in het ziekenhuis

De Algemene Verordening Gegevensbescherming, of AVG in het kort, geldt sinds 25 mei 2018. Ook in het ziekenhuis moeten wij ons aan deze regelgeving houden. In deze training leer je aan de hand van herkenbare praktijksituaties hoe je goed met de privacyregels omgaat.

Na 5 minuten kun je de volgende vragen beantwoorden:

- Wat zijn (bijzondere) persoonsgegevens?
- Waarom is bescherming van persoonsgegevens belangrijk?
- Hoe ga je in de praktijk om met privacy?

bepaalde geclassificeerde informatie?

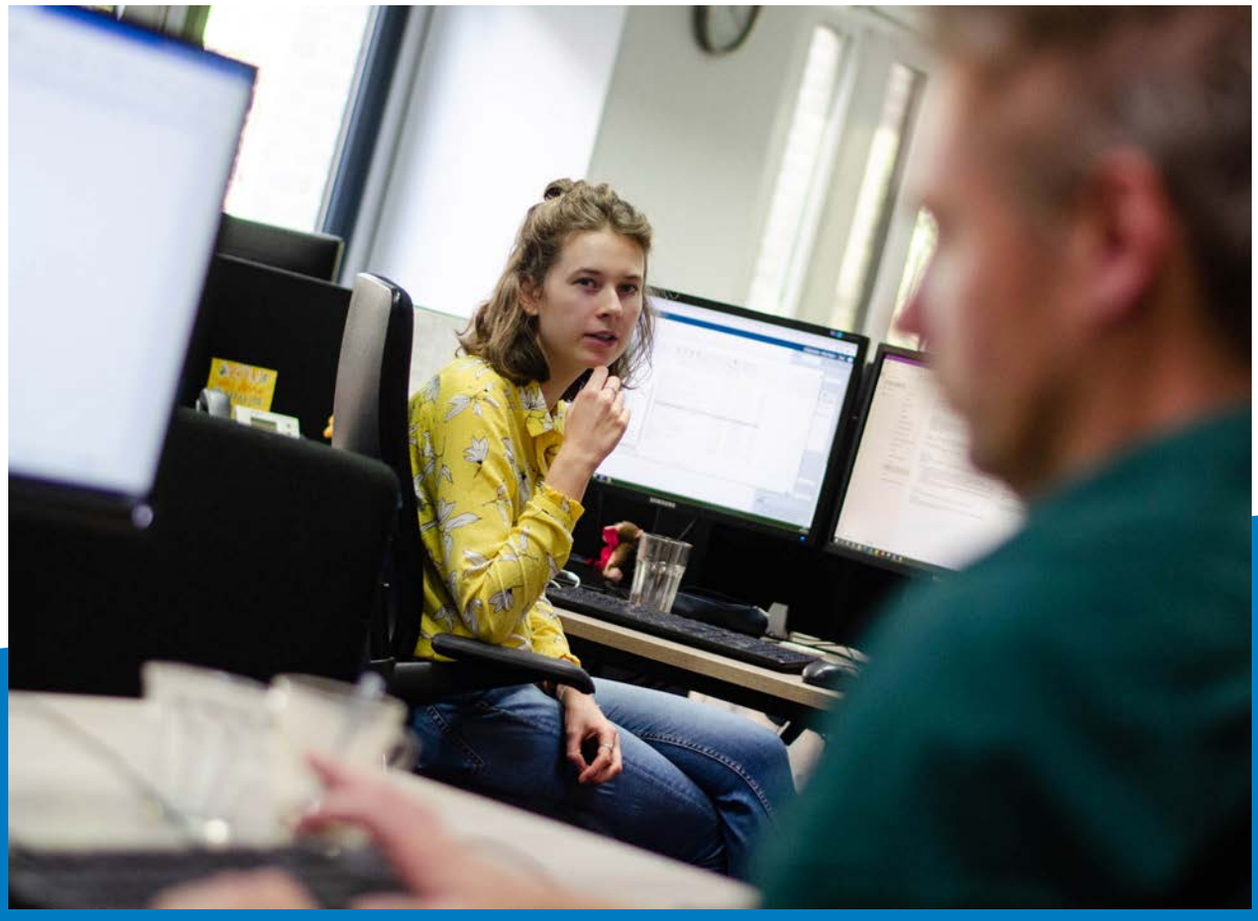
- Hoe handel je als mensen om gevoelige informatie vragen?

Onrechtmatige toegang tot het EPD

Onze patiënten vertrouwen op onze deskundigheid, niet alleen in de operatiekamer en aan hun bed, maar ook als het gaat om hun persoonlijke gegevens. Of het nu uit nieuwsgierigheid is of met de beste bedoelingen: we willen onrechtmatige toegang tot het EPD voorkomen. Zo beschermen we de gegevens en privacy van onze patiënten.

Weet jij wie er meekijkt in de dossiers van onze patiënten?

In de komende 5 tot 10 minuten ontdek je hoe wij allemaal ons steentje bijdragen aan het veilig houden van het EPD.



Security flashes

Bring your own device

Als medewerkers hun eigen mobiele apparatuur kunnen gebruiken voor zakelijke doeleinden, profiteert je organisatie hier zelf ook van. Bijvoorbeeld door lagere service- en hardwarekosten. Daarbij hebben medewerkers vaak telefoons, tablets en laptops die slimmer, beter en sneller zijn dan de bedrijfsapparatuur. Deze bewustwordingsvideo leert je hoe je eigen apparatuur voor je werk gebruikt, wat hiervan de gevaren zijn en hoe je met incidenten omgaat.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

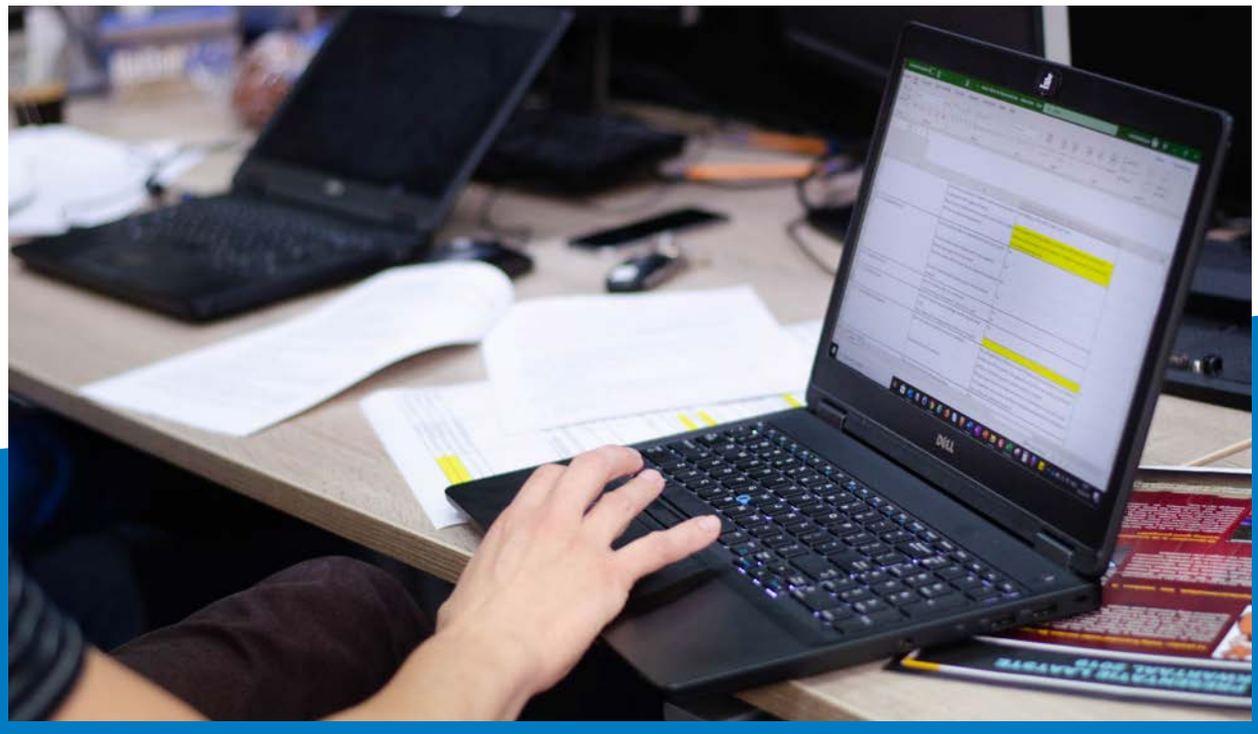
- Hoe kun je je eigen apparaat zakelijk gebruiken?
- Wat zijn de gevaren van het werken met je eigen apparatuur?
- Hoe kun je deze gevaren voor zijn?
- Wat te doen in geval van een security incident?

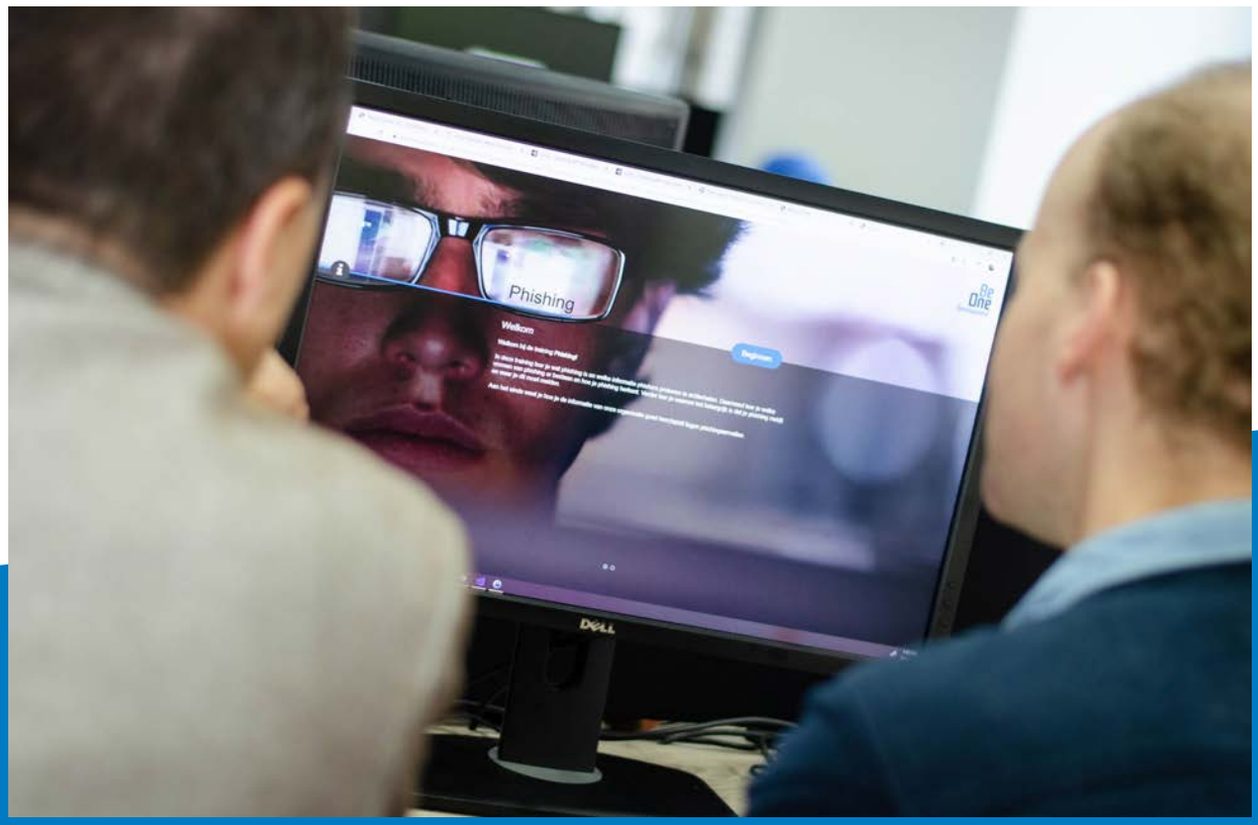
Clear desk, screen & office

Je weet nooit wie er langs je bureau loopt als je er niet bent. Laat daarom geen gevoelige informatie onbeheerd achter. Dit geldt zowel voor de informatie op je beeldscherm als op je bureau. Vergrendel je computer en laat geen gevoelige informatie achter als je je werkplek verlaat. Zelfs niet als je maar heel even weg bent. In iets meer dan een minuut leer je waarom een clear desk, screen en office policy bijdraagt aan een veilige organisatie.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Waarom moet je je werkplek schoon en opgeruimd houden?
- Wat zijn de gevaren als je dit niet doet?
- Hoe voorkom je deze gevaren?





Phishing

Phishing is één van de grootste cybercrimebedreigingen op dit moment. Er zijn veel vormen van social engineering, maar phishing is veruit het meest bekend en succesvol. Het idee is simpel: nadat je klikt op een valse link of een bijlage opent, heeft de cybercrimineel toegang tot je gegevens. Deze bewustwordingsvideo leert je hoe je verdachte e-mails herkent, wat hiervan de gevaren zijn en wat je moet doen als het misgaat.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Waar zijn phishingcriminelen naar op zoek?
- Hoe herken je een phishingmail?
- Wat doe je als je een link of bijlage niet vertrouwt?

Meld security-incidenten

Veiligheidsrisico's doen zich dagelijks voor binnen je organisatie. Op het eerste gezicht lijken ze onschuldig, maar deze risico's kunnen leiden tot incidenten. Als je denkt dat er sprake is van een incident of verdacht gedrag, is het belangrijk dat je actie onderneemt. Je organisatie neemt dan de juiste veiligheidsmaatregelen. Deze bewustwordingsvideo leert je incidenten te voorkomen en juist om te gaan met verdachte situaties.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Wat is een security-incident precies?
- Wat moet je precies doen als je te maken krijgt met een incident?
- Wat kun je nog meer doen om de veiligheid van informatie te waarborgen?

Sterke wachtwoorden

We weten allemaal dat we sterke wachtwoorden moeten gebruiken, omdat zwakke wachtwoorden makkelijk te hacken zijn. Heeft een cybercrimineel een wachtwoord in handen? Dan heeft hij toegang tot vertrouwelijke informatie. Deze bewustwordingsvideo leert je hoe je sterke wachtwoorden maakt, wat de gevaren van een zwak wachtwoord zijn en hoe je op een veilige manier met je wachtwoorden omgaat.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

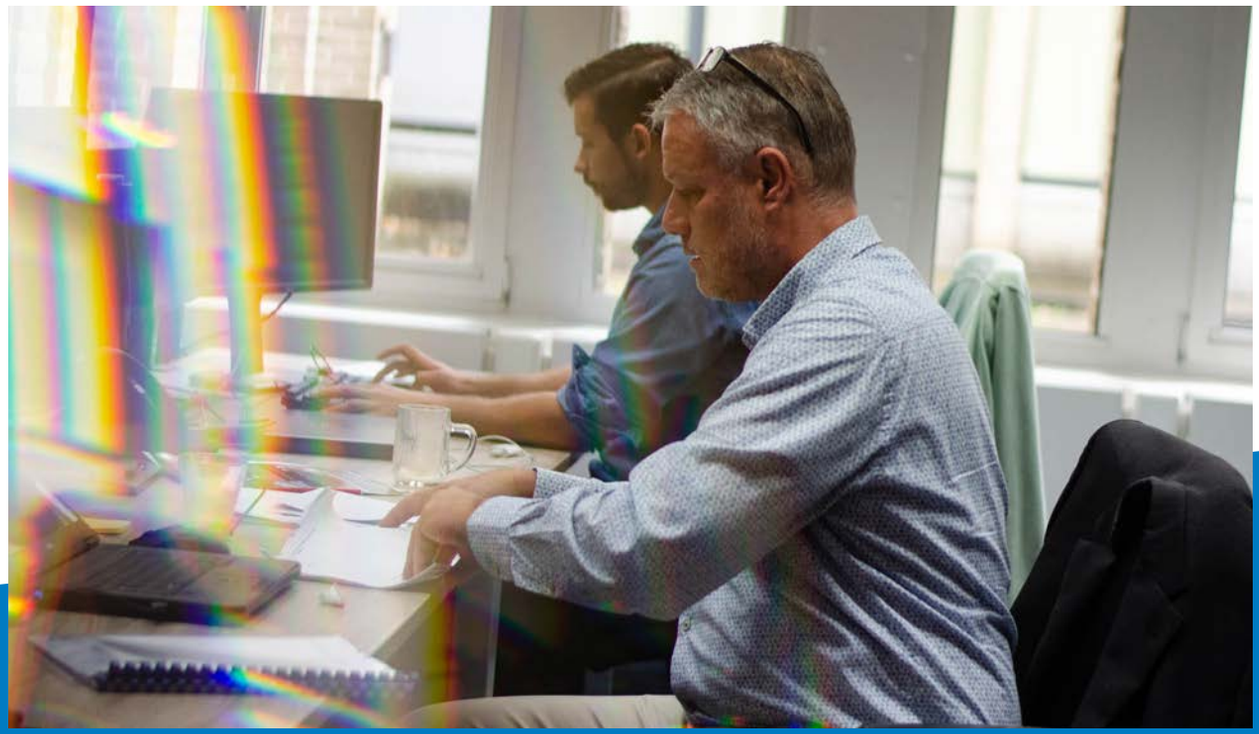
- Wat is een sterk wachtwoord?
- Hoe zorg je ervoor dat je wachtwoord makkelijk te onthouden is, maar moeilijk te raden?

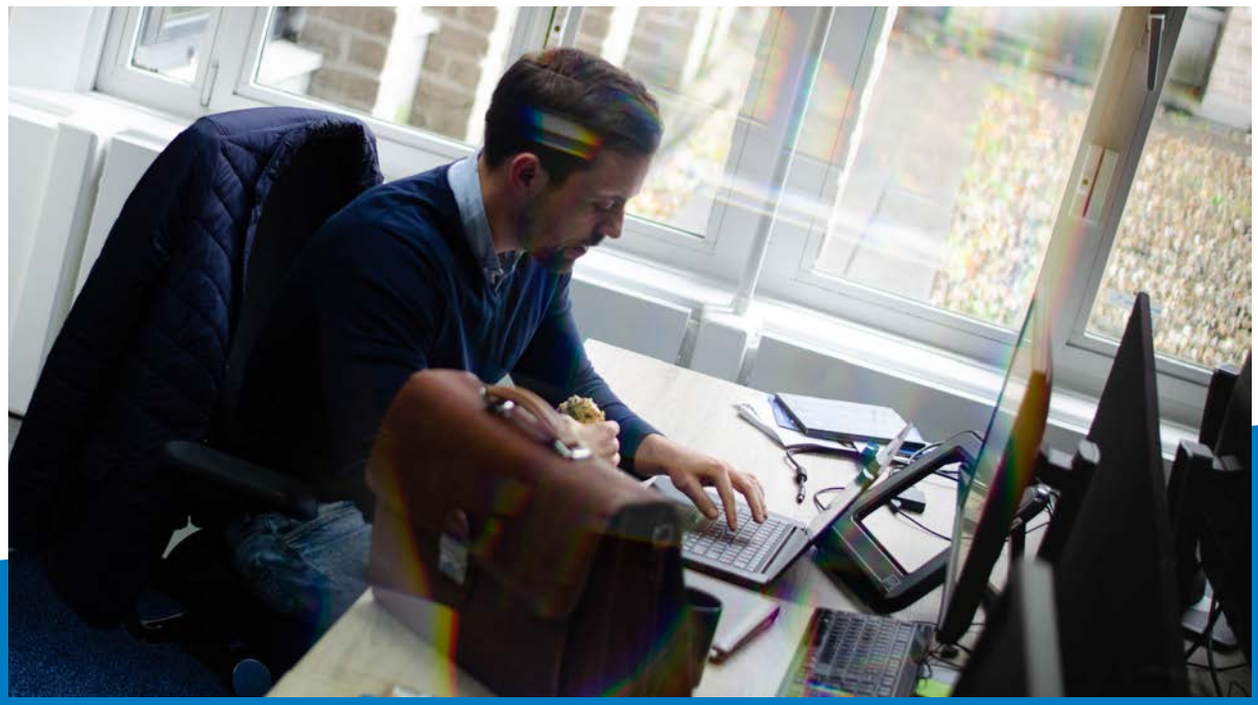
Werken in het openbaar

Flexwerken wordt steeds populairder. Steeds meer medewerkers hebben de mogelijkheid te werken waar en wanneer ze willen: vanuit huis, op kantoor, in de trein of in een openbare ruimte. Maar werken in het openbaar brengt verschillende veiligheidsrisico's met zich mee. Deze bewustwordingsvideo leert je in minder dan 2 minuten hoe je optimaal profiteert van werken in het openbaar zonder daarbij het risico te lopen gevoelige of vertrouwelijke informatie te verliezen.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Waar houd je rekening mee als je in het openbaar werkt?
- Waar moet je op letten als je sociale media gebruikt?





Social engineering

Social engineering is een techniek waarbij iemand vertrouwelijke gegevens probeert te stelen door het 'slachtoffer' te manipuleren. Je werkt met veel informatie die aantrekkelijk is voor anderen. Het is daarom belangrijk dat je de werkwijze van social engineers herkent. Wees bijvoorbeeld altijd voorzichtig als je informatie in het openbaar bespreekt. Als je gevoelige informatie in het openbaar bespreekt, kunnen anderen het horen. Dat kan vervelende gevolgen hebben.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Wat is het doel van social engineers?
- Waar moet je op letten wanneer je een zakelijk gesprek voert in het openbaar?
- Wat moet je doen als een onbekende vraagt om informatie?

Toegangscontrole

Deze video laat zien waarom toegangscontrole belangrijk is bij het beveiligen van informatie. Het gebruik van een toegangspas versterkt de beveiliging van een gebouw, omdat alleen mensen met een pas directe toegang hebben. Het maakt ook inzichtelijk wie er in het gebouw zijn. Bij calamiteiten is dat belangrijke informatie. Meld verlies van je pas daarom meteen bij de verantwoordelijke persoon of afdeling.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Wat moet je doen met je toegangspas?
- Hoe ga je om met bezoekers?

Social media & werken in de cloud

Social media stelt je in staat om een groot publiek te bereiken, maar het is ook een bron voor identiteitsdiefstal. Clouddiensten zijn zeer toegankelijk, maar bij sommige clouddiensten heeft de dienstverlener dezelfde toegangsrechten tot jouw informatie als jij zelf. Om te voorkomen dat dit vervelende gevolgen heeft voor jou en je organisatie, leer je in deze bewustwordingsvideo over de risico's van het gebruik van social media en de cloud.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Welke soort informatie kan je veilig delen via social media en welke niet?
- Wat zijn de risico's van het delen van informatie via een clouddienst?
- Hoe kan je de incidenten voorkomen?

Informatieclassificatie

Het werken met informatie is een belangrijk onderdeel van een organisatie. Door informatie op de juiste manier te classificeren, geef je aan welk beschermingsniveau nodig is. Iedereen weet dan welke niveaus van vertrouwelijkheid, integriteit en beschikbaarheid ze moeten toepassen als ze met de informatie werken. Het doel hiervan is dat informatie niet kwijt raakt of in verkeerde handen komt. Deze bewustwordingsvideo licht toe waarom het belangrijk is om elk stukje informatie correct te classificeren.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Waarom is het belangrijk om informatie op de juiste wijze te classificeren?
- Wat zijn de meest voorkomende classificatiesoorten?
- Welke gevaren heeft het verliezen van informatie van een bepaald soort classificatie?
- Wat moet je doen als mensen om informatie vragen?

Malware

Malware staat voor 'malicious software', of kwaadaardige software. Het is een verzamelnaam voor verschillende soorten schadelijke software. Malware kan tot veel schade in je organisatie leiden. Deze bewustwordingsvideo leert je aan welke signalen je malware herkent en wat je moet doen als je denkt last te hebben van malware.

Na de bewustwordingsvideo (2-3 min) kun je de volgende vragen beantwoorden:

- Wat is malware?
- Wat doet malware?
- Wat zijn de signalen van malware?

Baseline tests

Nulmeting Informatiebeveiliging

De baseline test laat zien wat het huidige kennisniveau binnen de organisatie is. Het is geen toets. De resultaten maken duidelijk welke onderwerpen meer aandacht vragen. Zo stemmen we de trainingen en informatie af op de behoefte die er is.

De baseline test behandelt de volgende onderwerpen:

- Algemene Verordening Gegevensbescherming (AVG)
- Cyber security
- Fysieke beveiliging
- Malware
- Phishing
- Risicomanagement

Meer weten? Voor meer informatie over onze producten, prijzen en werkwijze, bezoek:

https://www.infosequre.com/nl

Referenties

De e-learningprogramma's van Infosequre hebben zich in de praktijk bewezen in honderden multinationals, middelgrote bedrijven, overheidsorganisaties en instellingen over de hele wereld. Deze organisaties werken een stuk veiliger sinds hun medewerkers met onze programma's weten hoe ze cybergevaren buiten de deur houden.

- Antoni van Leeuwenhoekziekenhuis
- Bank of Cyprus
- Bertelsmann
- Boskalis
- Gemeente Maastricht
- Philips

Benieuwd hoe Infosequre jouw medewerkers op scherp zet?

Voor al je vragen over onze e-learningprogramma's: neem gerust contact met ons op. Desgewenst geven we je graag een demonstratie. Wij staan voor je klaar!

Neem contact met ons op:
https://www.infosequre.com/nl/contact

infosequre

Olympia 2L, 1213 NT Hilversum, Nederland
Telefoon: +31 (0)85 30 397 10
www.infosequre.com