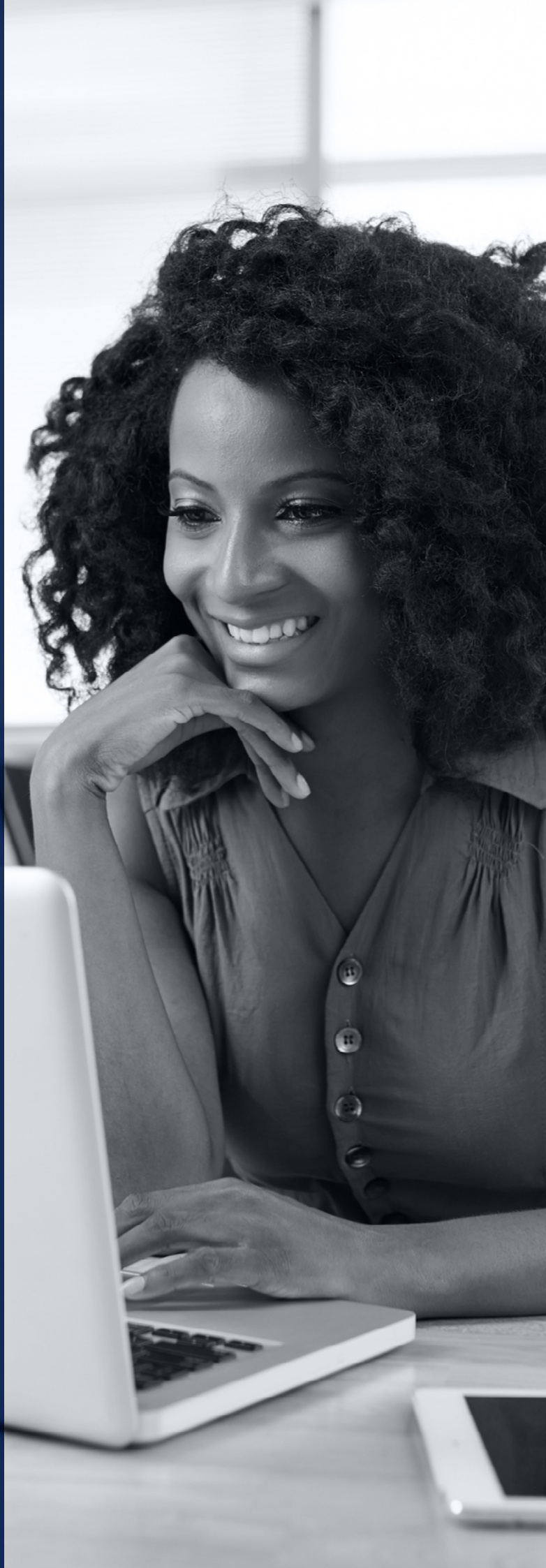
bit
internet technology

Internet Eigenwijs

Veilig internetten met behoud van van privacy



Onderzoeksrapport 2017

INHOUD

(Eigen)wijs de digitale wereld in

We kunnen denk ik rustig stellen dat ieder mens van nature wel een beetje eigenwijs is. Allemaal denken we het weleens beter te weten en trekken we ons eigen plan. Als het echter op het gebruik van internet aankomt, gooien we ons gezond verstand regelmatig overboord. Internet is een essentieel onderdeel van ons leven geworden en dankbaar maken we gebruik van alle mogelijkheden die het ons biedt. We Googlen, Facebooken, bankieren, werken en shoppen wat af online. Fantastisch natuurlijk, maar realiseren we ons ook voldoende wat dit betekent voor onze privacy en veiligheid?

In 2016 is BIT gestart met het onderzoek Internet Eigenwijs. Hierin onderzochten wij hoe werknemers internet gebruiken en hoe het gesteld is met het bewustzijn rondom internetveiligheid. Hieruit bleek dat er op dit gebied nog veel ruimte is voor verbetering. Zorgwekkend, want werknemers lopen hiermee niet alleen persoonlijk risico, maar nemen dit gebrek aan kennis en bewustzijn ook mee naar de werkvloer.

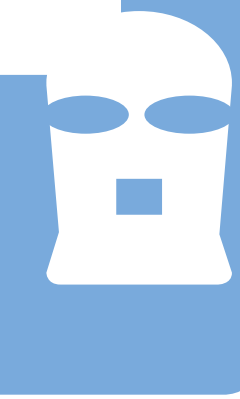
Dit jaar heeft Markteffect in opdracht van BIT opnieuw een groot onderzoek uitgezet onder 1.012 Nederlanders met een kantoorbaan. In dit onderzoek is nog dieper ingegaan op zaken als het omgaan met wachtwoorden, kennis van cybercrime, wet- en regelgeving en Internet of Things (IoT). Nu cybercrime het Nederlandse nieuws bijna dagelijks domineert, is het cruciaal dat kennis en bewustzijn rondom de risico's toeneemt. Dit is een taak voor ons allemaal.

Uit onderzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid is gebleken dat de Nederlandse overheid, bedrijven en haar burgers nog altijd onvoldoende weerbaar zijn tegen digitale aanvallen. De missie die we vanuit BIT hebben, is het bijdragen aan een veilig, vrij en open internet met waarborging van privacy. Daarom besteden wij in dit onderzoeksrapport niet alleen aandacht aan de resultaten van het onderzoek, maar geven wij ook praktische tips en handvatten voor hoe het beter kan. Of moet. Want één ding is zeker, om vrij en open te kunnen internetten met waarborging van privacy, moeten we nu stappen zetten.

Alex Bik *CTO bij BIT*

Cybercrime

Wat weten we eigenlijk?



"Pc's vaker getroffen door ransomware, mobieltjes niet", "Zeker vijftien ziekenhuizen geïnfecteerd met ransomware", "Malvertising geen groot probleem in Nederland, ransomware wel", "TenneT-klanten ontvangen zeer gerichte phishingmails", "Universiteit VS verliest 1,9 miljoen dollar door CEO-fraude", "CIA zette Windows-servers in om malware te verspreiden"... en zo kunnen we nog pagina's lang doorgaan. Cybercrime domineert het nieuws, waardoor security niet langer alleen een gespreksonderwerp op de IT-afdeling is, maar ook bij het koffiezetapparaat of op verjaardagen. Het gaat ons allemaal aan, maar weten we eigenlijk wel waar het over gaat?

Kennis over cybercrime

Om te toetsen wat de gemiddelde Nederlandse werknemer met een kantoorbaan weet over de begrippen die de headlines domineren, hebben we er een aantal voorgelegd. Uit een viertal beschrijvingen, selecteerde 82% van de werknemers de juiste betekenis van phishing, 75% kent de betekenis van malware, 68% weet wat malvertising is en 70% is bekend met ransomware. Opvallend hierbij is dat de percentages structureel hoger liggen bij de groep 55 jaar en ouder en structureel lager bij de groep 18 tot en met 34 jaar. Vooral ransomware is binnen deze laatste doelgroep redelijk onbekend. Slechts 57% selecteerde de juiste betekenis.

Social engineering en CEO-fraude zijn het minst bekend bij de werknemers. 48% selecteerde de juiste betekenis van CEO-fraude en voor social engineering slechts 24%. Wanneer we het over social engineering hebben, is het duidelijk dat de respondenten geen idee hebben. Van de vier antwoordopties scoort iedere optie rond de 25%.

Phishing 82% Identiteitsdiefstal via een e-mail of telefoon waarin wordt gevraagd om actie te ondernemen en daarbij gevoelige informatie wordt buitgemaakt

Malware 75% Software die gebruikt wordt om devices, zoals laptops, telefoons en tablets, te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot bepaalde systemen

Ransomware 70% Dat slachtoffers worden gechanteerd om losgeld te betalen in ruil voor geblokkeerde systemen en/of bestanden

Malvertising 68% Schadelijke software die wordt verspreid via advertenties op websites

CEO-fraude 48% Dat criminelen zich voordoen als een leidinggevende en vanuit deze machtspositie proberen zij werknemers te forceren om buiten de standaardprocedures acties uit te voeren

Social engineering 24% Een hacker die niet het systeem kraakt, maar de mens om de tuin leidt

TIP

Verhoog veiligheid door training medewerkers

Van nature zijn IT-afdelingen geneigd om zaken op te lossen door de inzet van technische maatregelen. Meer monitoring, meer virusscanners en meer firewalls, maar daar ga je het niet mee redden. Om de veiligheid verder te verhogen, is het cruciaal dat medewerkers getraind en opgeleid worden. Bij BIT zijn we er van overtuigd dat bewustwording onder werknemers de veiligheid met nog zeker 25% kan verhogen. Hierbij moet de IT-afdeling zich kwetsbaar opstellen; ja, technische maatregelen zijn noodzakelijk, maar de hulp van medewerkers ook. Informeer de medewerkers over de ontwikkelingen op securitygebied, geef inzicht in de risico's en vraag aandacht voor de maatregelen. Twee keer per jaar kan al afdoende zijn. Denk bijvoorbeeld aan een korte presentatie tijdens de afdelingsoverleggen. Dit helpt de IT-afdeling ook direct een gezicht te geven binnen de organisatie. Eén ding is in ieder geval zeker, een bijdrage aan security begint bij bewustwording en kennis.

Social engineering: de factor mens

Social engineering of social hacking, is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken

Een voorbeeld van hoe dat in de praktijk kan werken, zien we bij het Amerikaanse telecombedrijf AT&T. Een hacker liet het account van de Amerikaanse Justin Williams overzetten op een nieuwe SIM-kaart en telefoon. Hierdoor was de hacker ook gelijk in staat het PayPal-account van Williams over te nemen. Net als DigiD maakt PayPal gebruik van two-factor-authenticatie, waarbij je een sms ontvangt om te checken of de toegang tot het account legitiem is. Hoe het dan toch mis kon gaan? Na een flink aantal weigeringen bij de servicedesk van AT&T ging er uiteindelijk toch één medewerker overstag, zodat de hacker de benodigde veiligheidscode in zijn bezit had.

Op de werkvloer

Waar cybercrime voorheen vooral gezien werd als een IT-onderwerp kan de 'gewone' Nederlandse consument hier zelf ook niet langer omheen. Er veel over horen in het nieuws is één ding, maar voelt de Nederlandse werknemer zich ook aangesproken om zelf kennis te vergaren en actie te ondernemen? Met andere woorden, heeft de Nederlandse werknemer genoeg kennis en handvatten om ervoor te zorgen dat het Nederlandse bedrijfsleven geen onnodige risico's loopt?

68%

van de Nederlandse werknemers is er van overtuigd dat zij nog nooit met cybercrime te maken hebben gehad op de werkvloer

Signalering en actie

Organisaties hoeven zich allang niet meer af te vragen of zij het doelwit zijn van cybercrime. De vraag is niet wanneer het gebeurt (of gebeurd is), maar hoe men ermee omgaat. Van de Nederlandse werknemers is echter maar liefst 68% er van overtuigd dat zij nog nooit te maken gehad hebben met cybercrime op de werkvloer. Slechts 16% zegt hier wel mee te maken gehad te hebben en 16% is hier niet zeker van. Van de werknemers die aangeven weleens slachtoffer geweest te zijn van cybercrime op de werkvloer, geeft 79% aan direct de IT-verantwoordelijke ingeschakeld te hebben en 12% zegt dit niet gedaan te hebben.

Op de vraag wat men zou doen wanneer men slachtoffer is van malware op het werk, antwoordt 77% dat zij dit melden bij de IT-afdeling. 46% meldt dit (ook) bij de leidinggevende, 13% zegt dat hij zelf of de leidinggevende aangifte doet bij de politie, 9% probeert het zelf op te lossen en 5% heeft geen idee wat te doen in zo'n situatie.

Voor ransomware geldt dat 74% dit zou melden bij de IT-afdeling, 54% bij de leidinggevende, 26% zou aangifte doen (of de leidinggevende), 3% denkt dat de leidinggevende direct betaalt en 2% vraagt de leidinggevende te betalen. 5% weet niet wat te doen in zo'n situatie.

Wat doet u als u op uw werk slachtoffer bent van malware?

77%	Ik meld dit bij de IT-afdeling
46%	Ik meld dit bij mijn leidinggevende
13%	Ik of mijn leidinggevende doet aangifte bij de politie
9%	Ik probeer dit zelf op te lossen door de malware te verwijderen
5%	Geen idee wat ik dan doe
1%	Niets

Wat doet u als u op uw werk slachtoffer bent van ransomware?

74%	Ik meld dit bij de IT-afdeling
54%	Ik meld dit bij mijn leidinggevende
26%	Ik of mijn leidinggevende doet aangifte bij de politie
3%	Mijn leidinggevende betaalt dit direct
2%	Ik vraag mijn leidinggevende om het gevraagde bedrag te betalen
5%	Geen idee wat ik dan doe
1%	Niets

Maatregelen op de werkvloer

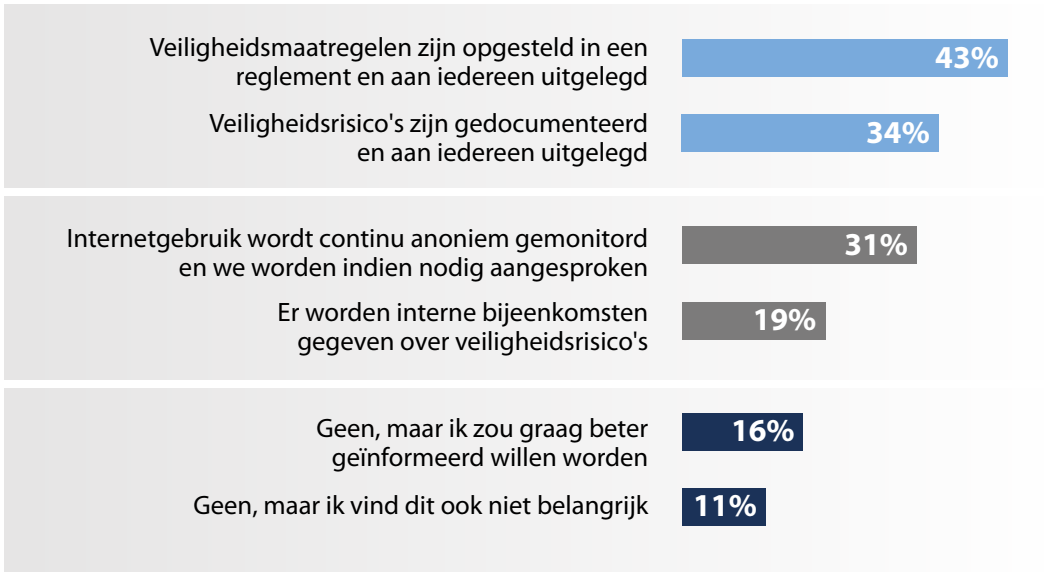
Om de Nederlandse werknemer bewust te maken van de risico's en maatregelen, is het belangrijk dat bedrijven zelf ook actie ondernemen om werknemers te onderwijzen. Daarom hebben wij de respondenten gevraagd welke maatregelen hun werkgever heeft getroffen om hen bewust te maken van cybercrime en de gevaren op internet.

43% van de werknemers zegt dat veiligheidsmaatregelen zijn opgesteld in een reglement en aan iedereen zijn uitgelegd. Volgens 34% zijn veiligheidsrisico's gedocumenteerd en aan iedereen uitgelegd en bij 19% van de bedrijven worden interne bijeenkomsten georganiseerd over veiligheidsrisico's. 31% weet te melden dat internetgebruik continu anoniem wordt gemonitord en dat werknemers worden aangesproken op het moment dat er risicovolle handelingen worden uitgevoerd.

Daarnaast geeft 27% aan dat er geen maatregelen getroffen zijn. 16% hiervan zou graag beter geïnformeerd willen worden, maar aan de andere kant vindt maar liefst 11% veiligheidsmaatregelen helemaal niet belangrijk.

Maar liefst 27% geeft aan dat er geen maatregelen getroffen zijn, dus er valt voor de Nederlandse werkgevers zeker nog winst te behalen als het gaat om security en bewustzijn onder haar werknemers.

Welke maatregelen heeft uw werkgever getroffen om u bewust te maken van cybercrime/gevaren op het internet?



Downloaden

Aan de respondenten is gevraagd of zij op het werk een bestand controleren voordat deze gedownload wordt van een website. 68% geeft aan dit te doen. 64% vertrouwt hiervoor vooral op de virusscanner, 43% doet dit op basis van de bestandsnaam, 49% controleert de aanbieder en 52% geeft aan dat de werkgever toegang tot bepaalde websites beperkt en gaat er dus vanuit dat de download veilig is.

De werknemers die een download niet controleren, doen dit met name niet omdat zij volledig vertrouwen op de maatregelen die de IT-afdeling heeft genomen (56%), omdat zij vertrouwen op de antivirussoftware (34%) en omdat ze er vanuit gaan dat IT mogelijke problemen meteen ziet en op kan lossen (26%). De IT-afdeling en technologie spelen dus een belangrijke rol wanneer het gaat om cybercrime op de werkvloer, ook in de perceptie van werknemers.

E-mail

Veel securityproblemen ontstaan doordat men in e-mails klikt op schadelijke linkjes of doordat men schadelijke bestanden opent. 14% van de werknemers klikt op de werkvloer weleens op linkjes in e-mails van onbekende afzenders; 5% geeft zelfs aan dit alleen maar op het werk te doen. Maar liefst 22% geeft aan dat hierdoor de werkcomputer of -laptop weleens geïnfecteerd is met een virus. 12% heeft geen idee of dit gevolgen gehad heeft, privé of op het werk.

Daarnaast geeft 11% aan op de werkvloer weleens bestanden te openen uit mails van onbekende afzenders. 26% heeft hierdoor te maken gekregen met een virus en 15% weet niet of het gevolgen heeft gehad, privé of op het werk. Meer bewustwording over de gevaren hiervan zou dus zeker geen kwaad kunnen.

28%

van de werknemers geeft aan dat het wachtwoord van hun werkcomputer bekend is bij minimaal één ander persoon in de privé-omgeving

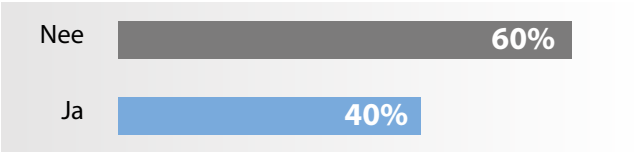
Wachtwoorden

De meeste werkcomputers en -laptops zijn beveiligd met een wachtwoord. In de praktijk is het echter de vraag hoe efficiënt deze beveiliging is. 28% van de werknemers geeft namelijk aan dat het wachtwoord van deze computer bekend is bij minimaal één ander persoon in de privé-omgeving. 8% geeft zelfs aan dat dit bekend is bij twee of meer mensen. Met deze inloggegevens hebben deze derden in 40% van de gevallen ook toegang tot bedrijfssystemen en -informatie.

Hoeveel mensen in de privé-omgeving kennen de inloggegevens van de werklaptop/-computer of weten waar ze dit kunnen achterhalen?

Alleen ik	72%
Nog 1 iemand	20%
Nog 2-3 mensen	6%
4 of meer mensen	2%

Hebben deze personen toegang tot bedrijfssystemen en -informatie?



Mobiele telefoon

Tot slot hebben we ook gevraagd naar de veiligheidsmaatregelen die de werkgever heeft getroffen voor het gebruik van de mobiele telefoon. 22% geeft aan dat er een virusscanner geïnstalleerd is, 19% zegt wel e-mail van werk te kunnen lezen, maar geen toegang te hebben tot bedrijfssystemen en -informatie, 12% zegt dat de beheerder bepaalde apps heeft geblokkeerd, in 11% van de gevallen kan de beheerder de telefoon op afstand managen en 9% geeft aan dat de beheerder het zelf installeren van apps volledig heeft geblokkeerd. 38% heeft geen mobiele werktelefoon en 15% heeft geen idee of er maatregelen getroffen zijn.

Dilemma: wat vindt u erger?

75%
Mijn externe harde schijf wordt gestolen met al mijn privé-foto's, bestanden en documenten

25%
Mijn werkcomputer wordt gestolen met bedrijfsgevoelige informatie

TIP

Maak medewerkers medeverantwoordelijk

Weinig interne bijeenkomsten, lang niet iedereen meldt problemen bij de leidinggevende of IT-afdeling en een grote groep medewerkers die beter geïnformeerd wil worden. Werk aan de winkel dus. Het klinkt behoorlijk schools, maar maak werknemers medeverantwoordelijk voor security door hen te belonen voor goed gedrag. Een USB-stick op de parkeerplaats gevonden, een vreemde e-mail binnengekregen of rare telefoontjes? Meld het bij de leidinggevende of de IT-afdeling en word verrast met een taart voor de hele afdeling. Zo neem je mogelijke drempels weg en groeit het bewustzijn.

Zorg voor gastaccounts op laptops

Bedrijfslaptops die mee naar huis gaan en vervolgens ook door familieleden en vrienden gebruikt worden; het gebeurt aan de lopende band, maar de risico's zijn enorm. Wanneer het geen probleem is dat medewerkers hun laptop mee naar huis nemen, zorg dan in ieder geval dat er gastaccounts geïnstalleerd zijn voor derden.

Securityrisico's vs slim online

Zoals in het voorwoord al besproken, mogen we met zijn allen weleens wat eigenwijzer worden als het gaat om internetgebruik. Daarvoor is het belangrijk om je bewust te zijn van de online risico's. Om inzage te krijgen in de kennis van de Nederlandse werknemer en de risico's die zij al dan niet bewust lopen en nemen, heeft BIT een aantal onderwerpen onder de loep genomen, namelijk; downloaden, e-mail en phishing en wachtwoorden. Wat gaat er goed en waar zijn er nog stappen te maken?

Downloaden

We hebben al vastgesteld dat 68% van de Nederlandse werknemers op het werk een bestand controleert voordat zij deze van een website downloaden. Thuis is dit percentage ruim hoger, namelijk 79%. Hier heeft men geen IT-afdeling waar op teruggevallen kan worden, waardoor men wellicht iets voorzichtiger is. De mensen die de download niet controleren, doen dit niet omdat zij vertrouwen op antivirussoftware (52%), de reputatie van een website (32%) of op de persoon die hem of haar naar de website heeft verwezen (16%). 8% geeft aan niet te verwachten dat je hierdoor slachtoffer van cybercrime wordt.

Om thuis een download te controleren, gebruikt 79% de virusscanner, controleert 51% de aanbieder en 45% controleert de bestandsnaam. Met name jongeren lijken hierbij ook te vertrouwen op hun eigen kennis: 59% van de respondenten tussen de 18 tot en met 34 jaar controleert de bestandsnaam en 61% controleert de aanbieder. Of het inderdaad terecht is dat jongeren meer op hun eigen kennis vertrouwen, blijkt onder andere uit de volgende resultaten.

E-mail & phishing

Om verstandig om te kunnen gaan met internet is het belangrijk dat risico's worden uitgelegd en herkend. De Nederlandse werknemer geeft zelf aan dat het op dit gebied nog aan de nodige kennis ontbreekt. 63% zegt overtuigd te zijn een malafide e-mail te herkennen. Slechts 10% is hier heel erg van overtuigd, waarbij we zien dat dit percentage voor de jongeren hoger ligt, namelijk 17%.

Om dit te toetsen, hebben wij in het onderzoek een aantal links, e-mailadressen en bestandsnamen voorgelegd met de vraag welke van deze mogelijk vals zijn. Overall zien we dat jongeren hier gemiddeld inderdaad hoger scoren dan de werknemer vanaf 35 jaar. Jongeren herkennen een mogelijk valse link of vals adres beter. Tegelijkertijd zien we ook dat de correcte links en adressen veel aangemerkt worden als vals. Dit laat zien hoe moeilijk het is om malafide e-mails te herkennen zonder richtlijnen.

Welke van onderstaande linkjes is waarschijnlijk vals en dus niet van ING?

		>35 jaar	jongeren
login.ing.nl	correcte link	40%	34%
login-ing.nl	mogelijk vals	59%	59%
ing.nl/nieuwsbrief2016	correcte link	14%	10%
ing.nl.nieuwsbrief2016.nl	mogelijk vals	60%	73%
Ik heb geen idee		17%	10%

Welk van onderstaande e-mailadressen is waarschijnlijk vals en dus niet van ING?

		>35 jaar	jongeren
nieuwsbrief@mail.ing.nl	correct adres	32%	35%
nieuwsbrief@mail-ing.nl	mogelijk vals	58%	62%
klantenservice@mail.ing.nl	correct adres	30%	34%
klantenservice@mail-ing.nl	mogelijk vals	58%	63%
Ik heb geen idee		27%	18%

Welk type bestand brengt mogelijk schade aan uw computer toe?

De Nederlandse werknemers is ook gevraagd welk type bestand mogelijk schade zou kunnen toebrengen aan een computer. Feitelijk kan ieder bestand schade toebrengen aan een computer, maar dat dit niet bekend is bij de respondenten, blijkt uit de resultaten in de tabel hiernaast.

.doc	17%
.exe	45%
.lnk	33%
.jar	38%
.jpg	13%
.js	35%
.pdf	14%
.psg	28%
.scr	34%
.wsf	32%
.zip	35%
Ik heb geen idee	32%

Nederlandse werknemers geven tenslotte aan niet echt betrokken te zijn bij de signaleringsfunctie van nep e-mails. 40% geeft aan weleens contact opgenomen te hebben met een bedrijf, omdat uit naam van dat bedrijf een nep e-mail verstuurd was. 40% heeft geen contact opgenomen (of dit niet gesignaleerd) en 20% zegt dergelijke mails wel gesignaleerd te hebben, maar geen contact te hebben opgenomen.

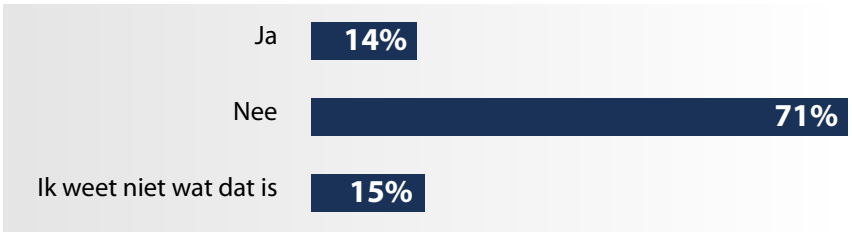
9%
van de Nederlanders verandert zijn wachtwoord van de privécomputer nooit

Wachtwoorden

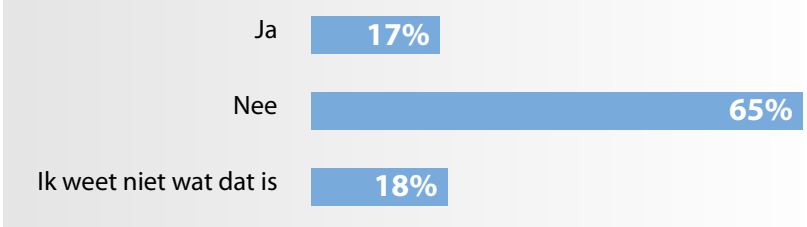
In het vorige hoofdstuk heeft u al kunnen lezen dat inloggegevens van werkcomputers gedeeld worden met derden, maar hoe zit het met de privécomputer of -laptop? 45% geeft aan dat buiten hemzelf nog anderen de inloggegevens kennen of weten waar ze deze kunnen achterhalen.

Wachtwoorden worden niet vaak veranderd: 9% verandert deze nooit, 21% minder dan 1 keer per jaar, 19% doet dit 1 keer per jaar en 50% 1 keer per kwartaal. Er worden nog weinig tools ingezet om wachtwoorden te genereren of op te slaan. Slechts 14% gebruikt een passwordgenerator en 15% weet niet wat het is. Het gebruik onder jongeren lig iets hoger, namelijk op 21%. Voor de passwordmanager geldt dat 17% deze gebruikt en 18% weet niet wat het is. 25% van de jongeren gebruikt wel een passwordmanager.

Gebruikt u een passwordgenerator?



Gebruikt u een passwordmanager?



Daarnaast hebben we de Nederlandse werknemers ook een aantal stellingen voorgelegd met betrekking tot het gebruik van wachtwoorden. Opvallend is dat maar liefst 38% aangeeft wachtwoorden op te schrijven om ze niet te vergeten en 18% e-mailt wachtwoorden naar zichzelf met hetzelfde doel.

Daarnaast gebruikt slechts 42% voor ieder account een uniek wachtwoord; 46% maakt variaties op één wachtwoord voor alle online accounts. 53% gebruikt zijn of haar gebruikelijke wachtwoord voor meer dan drie logins, voor jongeren is dit zelfs 64%.

Mijn privécomputer is voorzien van een wachtwoord	82%
Mijn werkcomputer is voorzien van een wachtwoord	92%
Mijn wachtwoord verander ik regelmatig	64%
Mijn wachtwoord bevat meerdere leestekens	79%
Mijn gebruikelijke wachtwoord gebruik ik voor meer dan drie logins	53%
Ik schrijf wachtwoorden op om ze niet te vergeten	38%
Ik gebruik privé meer verschillende wachtwoorden dan zakelijk	58%
Ik maak variaties op 1 wachtwoord voor alle online accounts	46%
Ik gebruik voor ieder account een uniek wachtwoord	42%
Mijn privé en zakelijke wachtwoord om in te loggen op de computer/laptop komen overeen	14%
Ik e-mail inloggegevens naar mezelf om ze niet te vergeten en makkelijk op te zoeken	18%

TIP

Blijf up-to-date

Alle type bestanden kunnen een veiligheidsrisico opleveren. Een groot deel van de mogelijke problemen wordt opgelost door de antivirussoftware, maar daarnaast is het cruciaal dat software continu up-to-date gehouden wordt. Een pdf is één van de veiligste bestanden, maar op het moment dat Adobe niet is bijgewerkt, ontstaan ook hier securityrisico's.

Daarnaast kunnen IT-afdelingen er voor kiezen om bepaalde extensies te blokkeren of bijvoorbeeld macro's uit te schakelen. Dit zijn slimme maatregelen, maar het is hierbij wel belangrijk dat IT-afdelingen de werknemers informeren over de alternatieven. Zo voorkom je dat mensen om de maatregelen heen werken.

Gebruik een passwordmanager en -generator

We kunnen het niet vaak genoeg zeggen: maak gebruik van passwordmanagers en -generators. Unieke wachtwoorden zijn begrijpelijkerwijs niet allemaal te onthouden, zeker niet op het moment dat er allerlei voorwaarden aan verbonden zijn. Als u de veiligheid op de werkvloer verder wilt verhogen, is het verstandig om medewerkers proactief te informeren en adviseren over de beschikbare tools.
Voorbeelden hiervan zijn:

- **1Password**
- **KeePass**
- **PWGen**

Een wachtwoordbeleid binnen organisaties moet werkbaar zijn om te voorkomen dat mensen er omheen gaan werken. Op het moment dat u van werknemers vraagt de wachtwoorden elke maand te veranderen, 25 karakters te gebruiken en uniek te blijven, dan is de kans groot dat er overal post-its geplakt gaan worden. Als maatregelen werkbaar blijven, is de kans dat mensen bedrijfswachtwoorden bijvoorbeeld ook buiten de bedrijfsserver gebruiken kleiner.

Check of uw e-mailadres is gelekt

Bijna dagelijks worden er datalekken bekend waarbij er logingegevens gestolen zijn. Een website waarop u kunt nagaan of uw e-mailadres voorkomt op een gelekte lijst, is https://haveibeenpwned.com. Interessant om zelf eens te checken en te communiceren naar collega's. Komt uw e-mailadres op een lijst voor? Dan raden wij aan uw wachtwoord te veranderen op iedere plek waar u dit e-mailadres gebruikt om in te loggen.

Internet of Things... of risks?

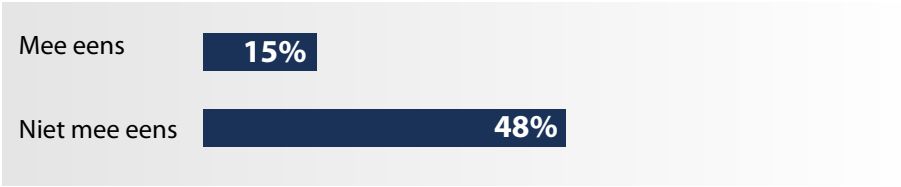
Internet of Things; in een razend tempo verbinden we onszelf en de apparatuur die we gebruiken steeds vaker met het internet. Van energiemeters, tot fitbits, telefoons en televisies, alles raakt verweven met het wereldwijde web. Behalve dat dit veel zaken makkelijker maakt, denk bijvoorbeeld aan de meterstand die je niet meer zelf door hoeft te geven, brengt het ook de nodige risico's met zich mee op het gebied van privacy en security. Hoe staat de Nederlandse werknemer hierin?

Op de vraag hoeveel apparaten men in huis heeft die verbonden zijn met het internet, antwoordt de grootste groep twee tot vijf (59%). 15% geeft aan dat dit er zes tot tien zijn, 13% zegt dat dit er slechts één is en 8% geen. Vervolgens is de vraag of zij zich verdiept hebben in de veiligheidsrisico's van het aansluiten van apparaten op het internet.

29% geeft aan zich hierin verdiept te hebben en daadwerkelijk zelf of met behulp van een externe partij maatregelen te hebben getroffen. 28% heeft zich wel verdiept, maar geen maatregelen getroffen. Daarnaast gaat 20% er vanuit dat de fabrikant dit al goed geregeld heeft, wist 12% niet dat er überhaupt risico's aan verbonden zijn en gelooft 11% niet dat zij risico lopen.

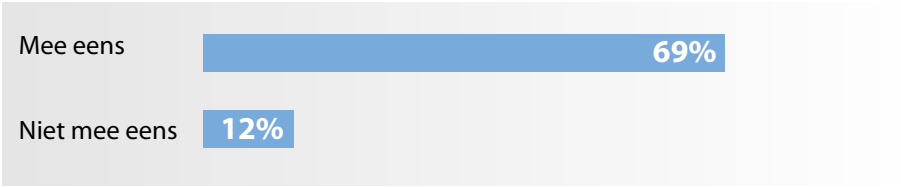
Ondanks dat er niet veel actie ondernomen wordt, lijken de meesten zich wel bewust te zijn van enig risico. Dat blijkt wanneer we naar de resultaten van de volgende stellingen kijken:

Apparaten die aangesloten zijn op het internet zijn bij de aankoop al goed beveiligd



Ik ben mij ervan bewust dat apparaten die verbonden zijn met het internet gehackt kunnen worden

Ik update alle apparaten die op het internet zijn aangesloten regelmatig



TIP

Zorg voor een veilig IoT-beleid

71% van de medewerkers geeft aan dat zij geen extra veiligheidsmaatregelen genomen hebben rondom hun IoT-devices. In de praktijk zien we op de werkvloer hetzelfde gebeuren. Er worden steeds meer apparaten aan het netwerk gekoppeld zonder dat hierbij bewust nagedacht wordt over de securityrisico's. Slecht beveiligde IoT-devices leveren drie problemen op:

1

U schaadt mogelijk anderen op internet. Het is niet ongebruikelijk dat slecht beveiligde IoT-devices worden ingezet voor grote DDoS-aanvallen. Op het moment dat een hacker toegang verschaft tot bijvoorbeeld een beveiligingscamera die is aangesloten op het internet, dan kan deze gebruikt worden in een netwerk van verschillende devices om een grootschalige aanval uit te voeren.

Ook voor IoT-devices geldt dat het belangrijk is dat updates altijd worden uitgevoerd en sterke wachtwoorden gebruikt worden.

2

Op het moment dat uw apparaat betrokken is bij zaken die niet horen, loopt u het risico hier juridisch of bijvoorbeeld door de provider op aangesproken te worden. Zodra het IP-adres bekend is, loopt u een serieus risico op vergelding, zonder dat u waarschijnlijk heeft doorgehad dat uw apparaat voor problemen heeft gezorgd.

3

Slecht beveiligde IoT-devices zijn mogelijk een springplank naar de rest van uw netwerk. Het is een plek voor een hacker om binnen te komen en van daaruit verder het netwerk te betreden.

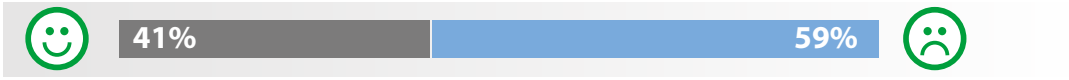
Privacy bewaren vs opgeven

Internetveiligheid draait niet alleen om ransomware-aanvallen en phishingmails, maar zeker ook om privacy. Er komt steeds meer wet- en regelgeving rondom privacy, waarbij bedrijven gedwongen worden op een verantwoorde manier om te gaan met persoonlijke informatie. Krantenkoppen over persoonlijke informatie die op straat is komen te liggen, lijken al bijna niemand meer te verbazen, maar zijn daarom niet minder zorgwekkend. Naast de wet- en regelgeving voor bedrijven is het belangrijk dat wij onszelf ook afvragen wat we doen om onze privacy te waarborgen. Hoe gaat de Nederlandse werknemer om met het delen van privacygevoelige informatie? En wat weten zij over en vinden zij van huidige wet- en regelgeving die onze privacy aangaat?

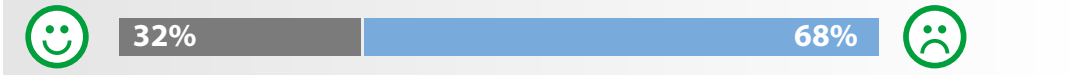
Online privacy – wat doen we zelf?

Aan de Nederlandse werknemer hebben wij gevraagd of men weet wat te doen om zijn of haar privacy goed te beschermen op het internet. Maar liefst 59 procent zegt dit niet te weten, 41% wel. Op de vraag of zij weten wat er gebeurt met informatie die zij online achterlaten, zegt 32% dat zij dit weten en 68% heeft geen idee. Tenslotte hebben we gevraagd of zij weten waar een beveiligde website aan te herkennen is; 59% weet dit en 41% niet. Op basis van deze resultaten kan geconcludeerd worden dat privacy niet top of mind is wanneer men gebruikmaakt van internet.

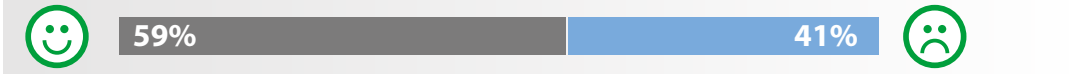
Ik weet precies welke acties ik moet ondernemen om mijn privacy goed te beschermen op het internet



Ik weet wat er met de informatie gebeurt die ik online achterlaat



Ik weet waar ik een beveiligde website aan kan herkennen



6%
van de Nederlanders doet niets om de online privacy te beschermen

Dat blijkt ook wanneer we vragen welke privacygevoelige informatie je weleens online achterlaat. We zien hier hoge percentages als het bijvoorbeeld gaat over naam- en voornaam (beide 75%), postcode en woonplaats (63% en 64%), maar lagere percentages bij bankrekeningnummers (20%), paspoortnummer (7%) en creditcardgegevens (12%). 13% geeft zelfs aan nooit online privacygevoelige informatie achter te laten.

De resultaten van deze vraag kunnen tweeledig zijn. Aan de ene kant is het waarschijnlijk dat men voorzichtiger is met bankrekeningnummers, paspoortnummers en creditcardgegevens, maar gezien het hoge aantal online boekingen voor bijvoorbeeld hotels en vluchten zou je ook kunnen verwachten dat deze percentages hoger zijn.

De vraag is dus hoe bewust men zich is van alle informatie die online gedeeld wordt.

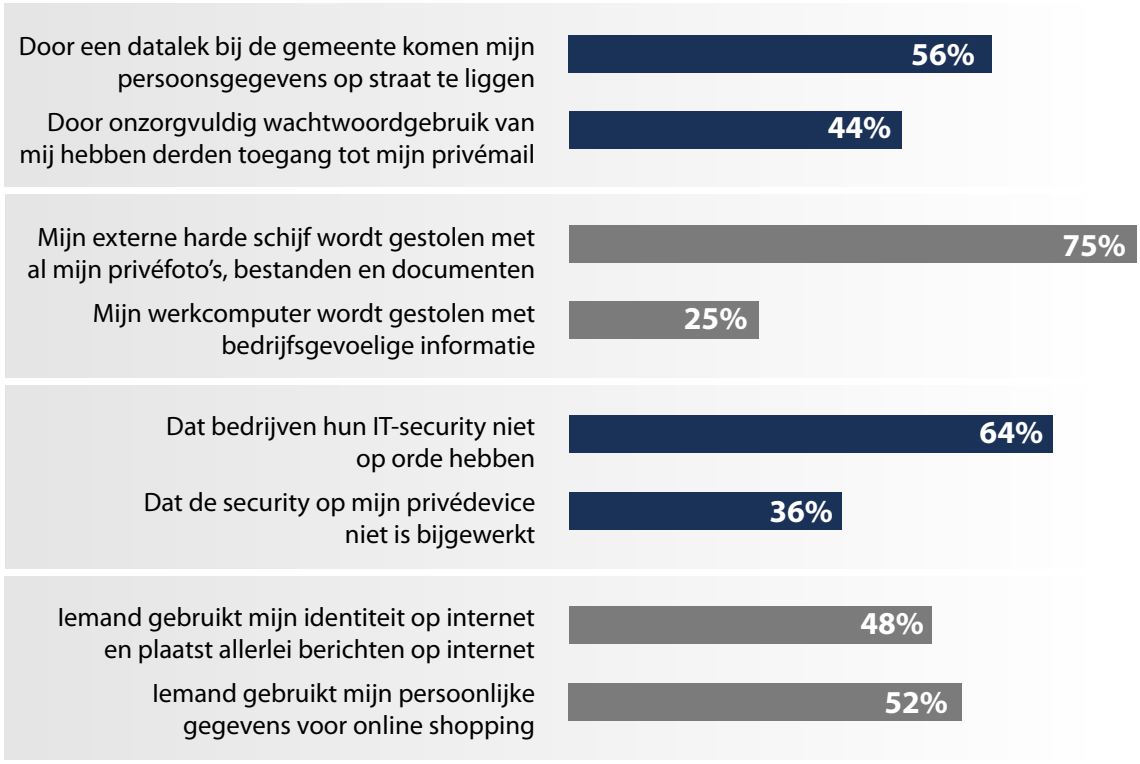
Op de vraag hoe de respondenten hun online privacy beschermen, antwoordt 64% door sterke wachtwoorden en 53% door verschillende wachtwoorden. Een interessant contrast met de resultaten eerder in dit rapport, waaruit blijkt dat men nog weinig gebruikmaakt van unieke wachtwoorden en bijvoorbeeld passwordgenerators. 51% zegt de online privacy te beschermen door systemen regelmatig te updaten, 50% door beveiligde internetverbindingen te gebruiken. Slechts 33% geeft aan bewust geen gegevens achter te laten, we vertrouwen dus vooral op techniek. 6% doet niets om de online privacy te beschermen.

Hoe beschermt u uw online privacy?

Privacydilemma's

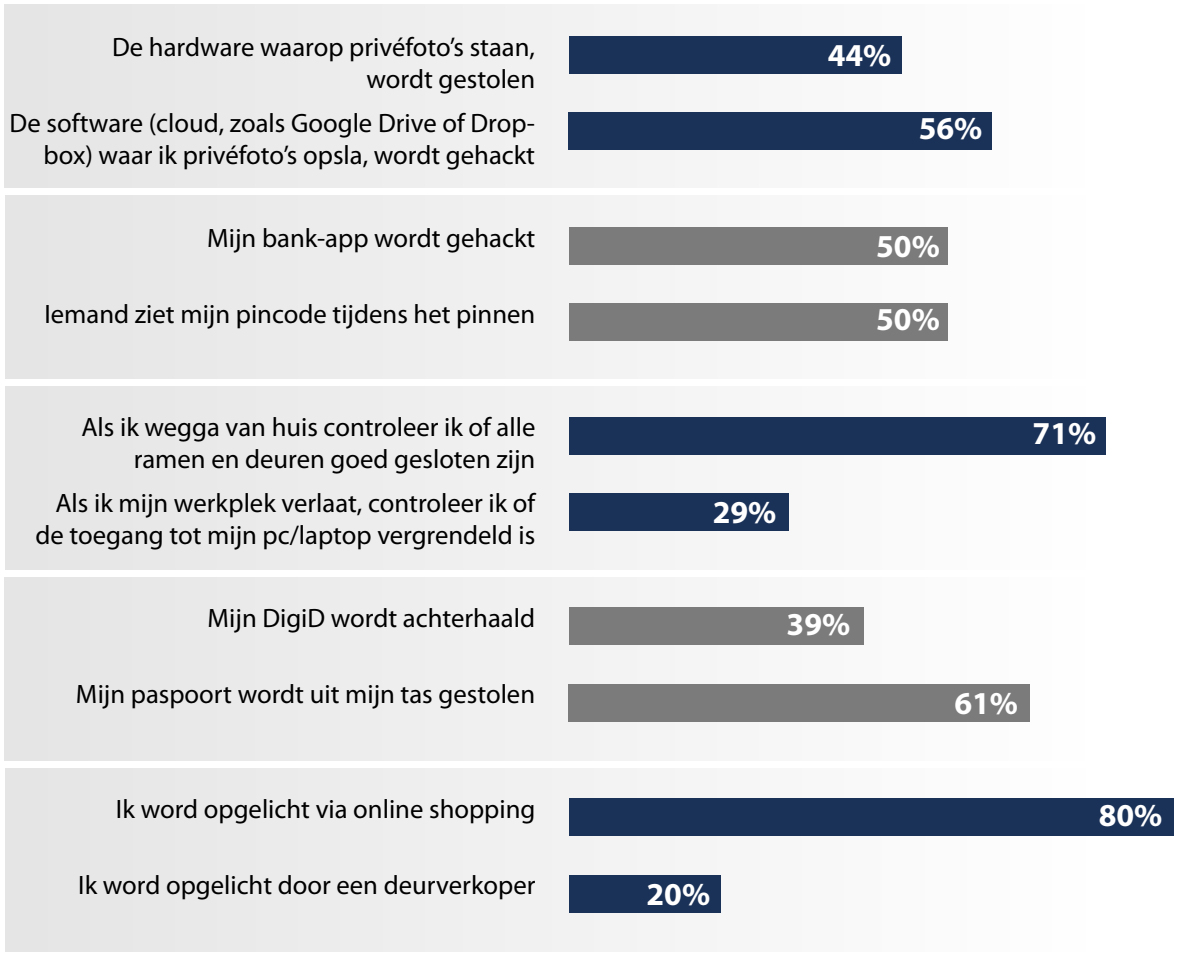
Om een beeld te krijgen van hoe de Nederlandse werknemer zich voelt bij een aantal privacy-issues, hebben wij hen een aantal dilemma's voorgelegd. Wat zou u kiezen?

Wat vindt u erger?



Hier zien we duidelijke verschillen tussen de leeftijdsgroepen. Van de werknemers van 55 jaar en ouder vindt 64% het erger als iemand de persoonlijke gegevens voor online shopping gebruikt, voor de groep 18 tot en met 34 jaar is dit 45%; zij vinden het dus erger als er namens hen online berichten geplaatst worden.

Wat vindt u het meest waarschijnlijk?



80%
"Ik word opgelicht via online shopping"

20%
"Ik word opgelicht door een deurverkoper"

Over het algemeen ontstaat hier het beeld dat mensen het erger, en soms ook waarschijnlijker, vinden als de schuld buiten hen zelf ligt. Daarnaast maken we ondanks de digitale wereld waarin we leven, nog vrij traditionele keuzes.

We vertrouwen eerder de deurverkoper, of we denken die sneller te kunnen doorgronden, checken wel deuren en ramen, maar niet de toegang tot onze pc's en laptops, en denken eerder dat er iets uit onze tas gestolen wordt dan dat onze DigiD wordt achterhaald.

Wet- en regelgeving en privacy

Er gebeurt veel in Nederland, Europa en de rest van de wereld wanneer we het hebben over wet- en regelgeving met het oog op onze veiligheid en privacy. Wat weten de Nederlandse werknemers hier vanaf en wat vinden zij hiervan?

De respondenten kregen vijf (mogelijke) wetten of wetsvoorstellen voorgelegd en hen is gevraagd of deze waar zijn of verzonnen. Wat denkt u?

1 De officier van justitie kan in iedereen zijn of haar mail kijken als hij/zij dat nodig vindt.

2 Internetbrowsers moeten consumenten vragen of er tijdelijke bestandjes mogen worden geplaatst die het surfgedrag van internetgebruikers volgen en persoonsgerichte advertenties mogelijk maken.

3 Het opslaan van alle locatie- en telecomdata van iedereen mag.

4 De politie heeft de bevoegdheid om computers te hacken.

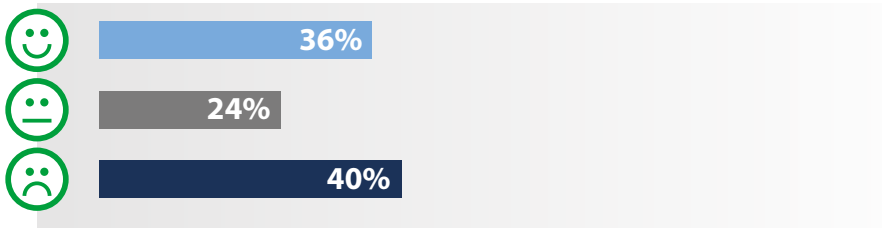
5 De Nederlandse inlichtingen- en veiligheidsdiensten hebben de bevoegdheid om al het internetverkeer (mobiel en vast) van alle inwoners in een willekeurige Nederlandse stad af te tappen en in te zien.

Alleen nummer 3 is niet waar (57% had dit goed), de rest is allemaal waar. De meerderheid van de respondenten dacht dat 2 (81%) en 5 (59%) waar waren, van nummer 1 dacht 57% ten onrechte dat het niet waar was.

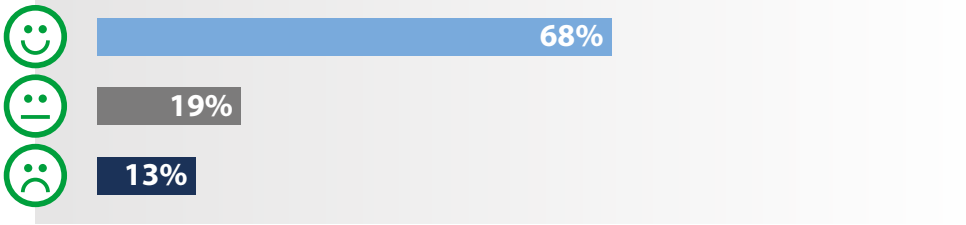
Voor nummer 4 was het fifty-fifty. Behalve voor nummer 2 zien we geen grote meerderheid die het juiste antwoord geeft. Men lijkt dus niet algemeen bekend te zijn met deze wetten of wetsvoorstellen.

Vervolgens hebben we ook gevraagd in hoeverre men het eens zou zijn met deze wetten. Hieruit blijkt dat de Nederlandse werknemer hier redelijk over verdeeld is en bovendien ook vaak kiest voor de middenweg 'neutraal'.

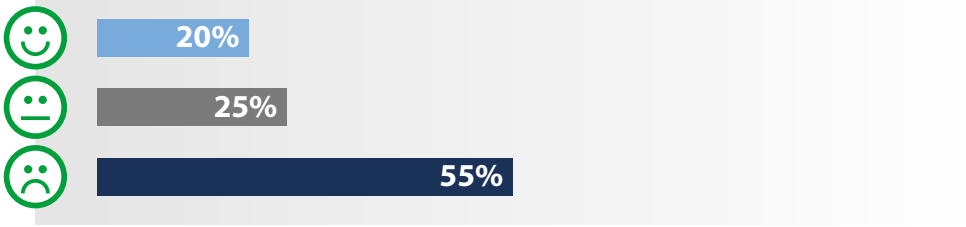
De officier van justitie kan in iedereen zijn of haar mail kijken als hij/zij dat nodig vindt.



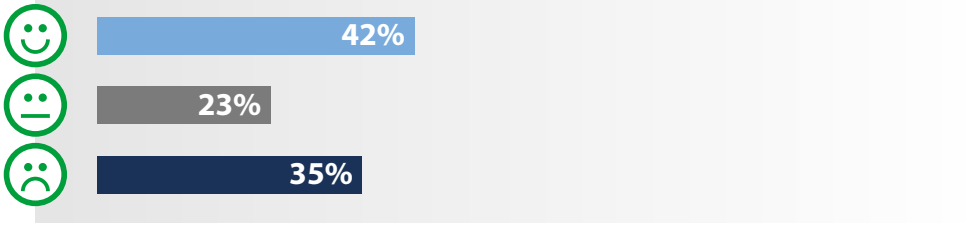
Internetbrowsers moeten consumenten vragen of er tijdelijke bestandjes mogen worden geplaatst die het surfgedrag van internetgebruikers volgen en persoonsgerichte advertenties mogelijk maken.



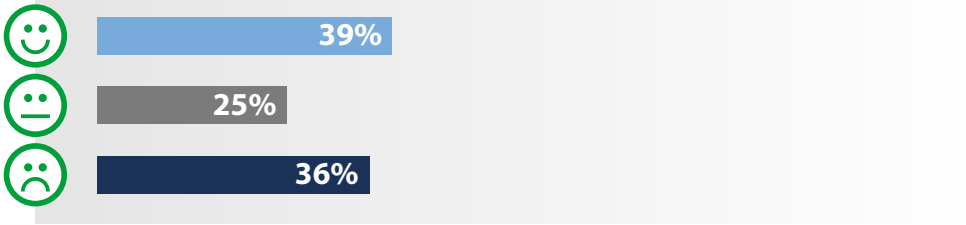
Het opslaan van alle locatie- en telecomdata van iedereen mag.



De politie heeft de bevoegdheid om computers te hacken.



De Nederlandse inlichtingen- en veiligheidsdiensten hebben de bevoegdheid om al het internetverkeer (mobiel en vast) van alle inwoners in een willekeurige Nederlandse stad af te tappen en in te zien.



TIP

Minder informatie verzamelen is ook minder beschermen

Privacy by design: als u minder informatie verzamelt, heeft u ook minder te beschermen. Veel organisaties vragen al dan niet bewust om meer klantgegevens dan nodig is voor de dienstverlening. Veel van deze 'informatievragers' zijn verborgen, denk bijvoorbeeld aan trackingsoftware die uw website-ontwikkelaar mogelijk implementeert. U bent zich hier misschien niet altijd bewust van, maar u verzamelt zo wel gegevens van bezoekers; vaak ook zonder bedrijfseconomische redenen. Zorg dat u in kaart krijgt welke informatie uw bedrijf verzamelt en bekijk kritisch of dit nodig is.

Schijnveiligheid vs veilig online - Digitale dilemma's

Anno 2017 kunnen we bijna geen nieuws meer tot ons nemen zonder dat we iets meekrijgen over cyberaanvallen, datalekken en andere security-issues. Security is niet langer meer een onderwerp waar alleen IT'ers zich mee bezig dienen te houden, het gaat ons allemaal aan.

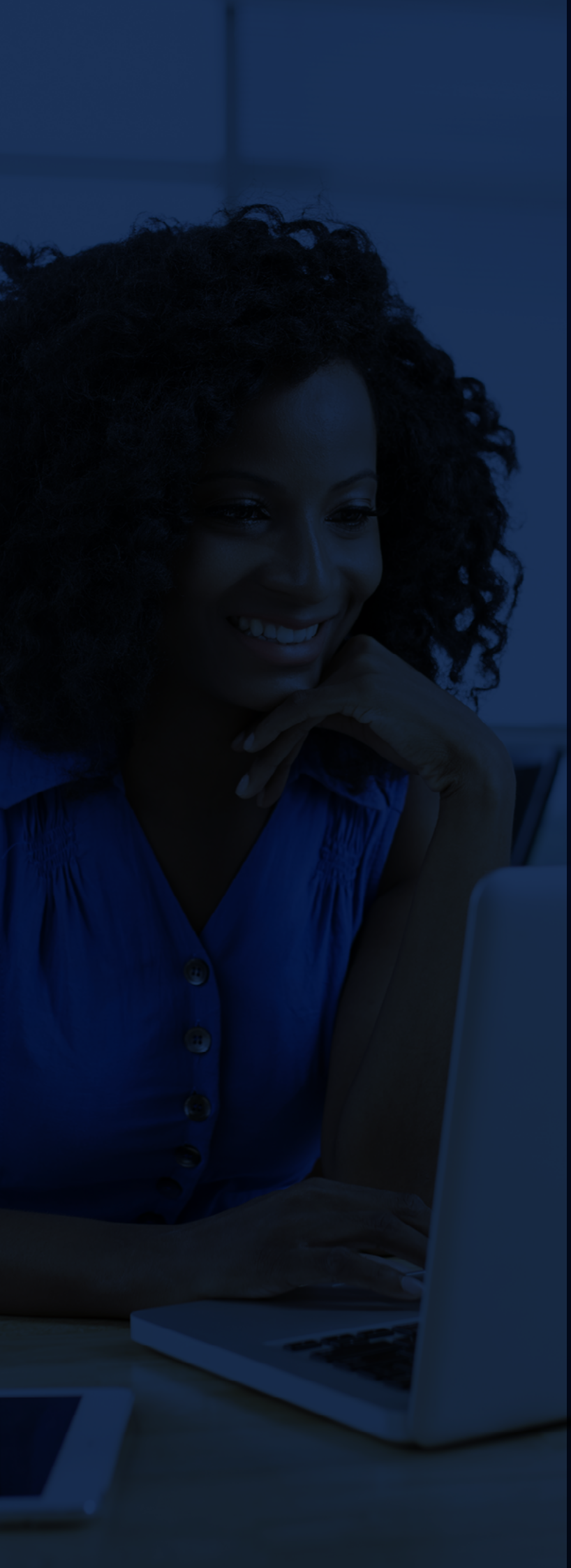
Uit onderzoek van PwC blijkt dat veel Nederlandse bedrijven en organisaties vanaf volgend jaar het risico lopen op hoge boetes, omdat ze nog niet klaar zijn voor een nieuwe Europese privacywet (GDPR). Van de 350 bedrijven blijkt ruim de helft nog niet serieus begonnen te zijn met de voorbereidingen, terwijl de Meldplicht Datalekken al meer dan een jaar van kracht is. De wet betekent goed nieuws voor burgers en veel werk voor bedrijven, maar daarnaast hebben we als individuen ook de verantwoordelijkheid om ons goed te informeren en waar mogelijk maatregelen te nemen.

Uit ons onderzoek blijkt dat de Nederlandse werknemer veel vertrouwen legt in antivirussoftware, wachtwoorden en de IT-afdeling. Tegelijkertijd zijn zij echter niet goed geïnformeerd over de risico's, klikken er velen op mogelijk valse links, kunnen derden bij bedrijfsinformatie en hebben zij eigenlijk geen idee hoe zij hun online privacy het beste kunnen beschermen. We willen alles snel kunnen doen, op ieder moment van de dag en wellicht dat oog voor security en privacy er daardoor weleens bij inschiet. Begrijpelijk, maar iedereen bevindt zich daardoor wel in een situatie van schijnveiligheid. Denk bijvoorbeeld aan het hergebruiken van wachtwoorden of het maken van variaties op dat ene wachtwoord. Op het moment dat uw e-mail wordt gehackt, is het voor cybercriminelen geen grote stap meer om ook toegang te krijgen tot andere online accounts. Het e-mailadres hebben ze al en ook de toegang daartoe.

Het enige dat nu nog hoeft te gebeuren is op andere sites aangeven dat u zogenaamd uw wachtwoord bent vergeten en de toegang tot een volgend account is ook geregeld. Voor u er erg in heeft, beschikt een cybercrimineel over een compleet profiel van u.

Als consument hebben we de taak om ons te laten informeren, maar ook om bewust om te gaan met ons internetgebruik. Laten we niet onnodig teveel gegevens achter? Veranderen we ons wachtwoord wel vaak genoeg? En is ieder wachtwoord uniek? Dit kost soms wat meer tijd dan u wellicht zou willen, maar het zorgt er wel voor dat een situatie van schijnveiligheid verandert in daadwerkelijk veilig gebruik van internet.

Werkgevers en IT-verantwoordelijken spelen hierbij ook een belangrijke rol. Stel securitypolicies op, train medewerkers en zorg dat werknemers begrijpen waarom maatregelen nodig zijn. In de praktijk wordt er nog teveel vanuit gegaan dat de medewerker het zelf allemaal wel weet, maar dit is vaak helemaal niet het geval. Het afdwingen van bepaalde securitypolicies, bijvoorbeeld een wachtwoordbeleid, roept in eerste instantie wellicht wat weerstand op. Uiteindelijk gaat het echter niet alleen om die hoge (mogelijk desastreuze) boete die u riskeert, maar om de veiligheid en privacy van uw werknemers, klanten en andere relaties. De sleutels van de archiefkast legt u toch ook niet onder de mat bij de voordeur?



bit
internet technology

BIT beheert een drietal datacenters in Ede en is gespecialiseerd in colocatie, internetverbindingen, managed hosting en outsourcing voor zakelijke gebruikers van het internet.
BIT levert aan kwaliteitsbewuste organisaties de ruggengraat voor hun IT- en internet-infrastructuur. Betrouwbaarheid is het uitgangspunt van de dienst-verlening, zodat klanten zich zorgeloos met hun kernactiviteiten bezig kunnen houden.

BIT onderscheidt zich door een hoog kennisniveau, jarenlange ervaring en een pragmatische aanpak.
BIT is ISO 27001 en NEN 7510 gecertificeerd.

Contact opnemen met BIT mag altijd:
Galileïlaan 19, 6716 BP Ede
T +31 (0)318 648 688
E info@bit.nl **I** https://www.bit.nl