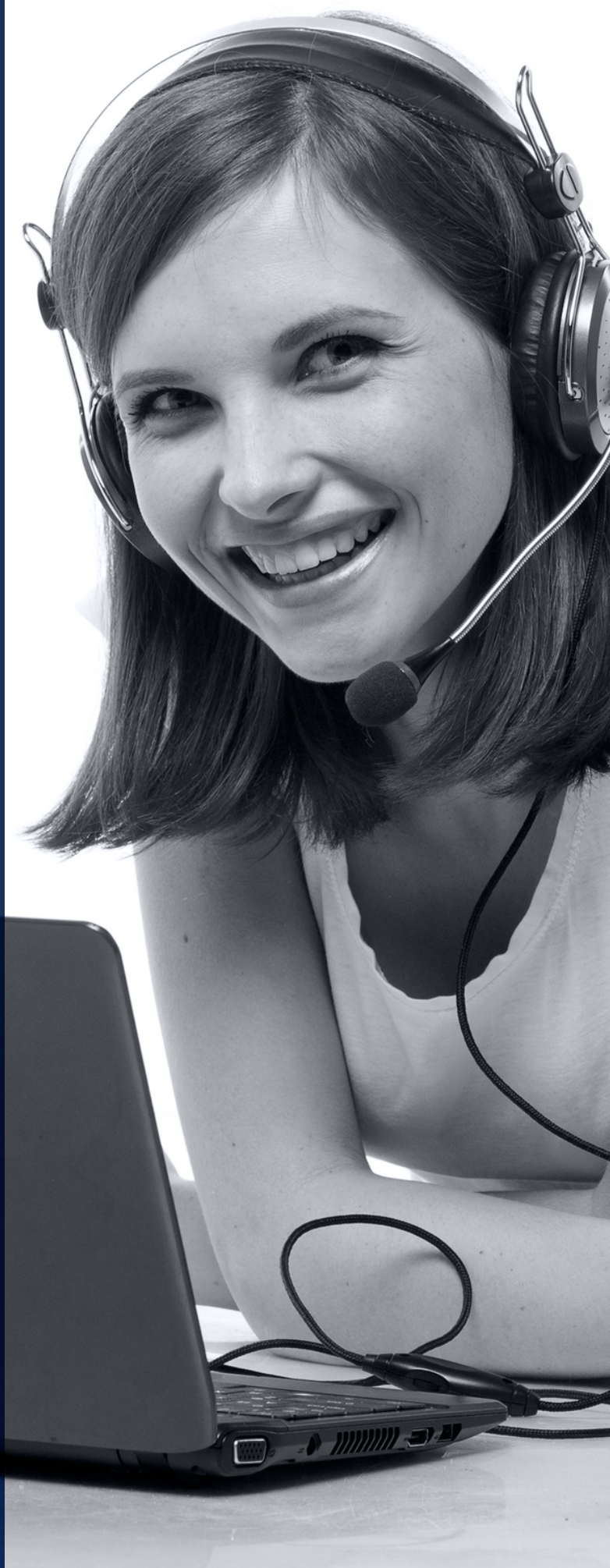
Obit
internet technology

Internet Eigenwijs

Veilig internetten met behoud van van privacy



Onderzoeksrapport 2016

INHOUD

Een eigen(wijs) plan op internet

Is een wereld zonder internet nog voor te stellen? Het antwoord is nee. Het is een nutsvoorziening waar een ieder van afhankelijk is, dat staat als een paal boven water. Kinderen komen op jonge leeftijd in aanraking met internet. Spelletjes op de tablet of telefoon, social media, schoolactiviteiten etc. Kortom, internet is de normaalste zaak van de wereld. Sterker nog: met de opkomst van Internet of Things worden we er nog afhankelijker van. Ondanks dat internet massaal wordt gebruikt, blijkt uit een onderzoek van het Centraal Bureau voor de Statistiek dat de helft van de Nederlandse bevolking zich zorgen maakt om hun veiligheid op het web. Kennis over dit onderwerp ontbreekt vaak in de praktijk. Internetveiligheid staat dan ook op de agenda voor het bedrijfsleven, politie en justitie. In 2017 treedt onder meer het wetsvoorstel gegevensverwerking en meldplicht cybersecurity in werking.

In de zomer van 2016 deed onderzoeksbureau Markteffect in opdracht van BIT onderzoek naar de wijze waarop consumenten internet gebruiken en het bewustzijn van internetveiligheid. Om representativiteit te waarborgen is het onderzoek uitgezet onder 992 Nederlandse consumenten van 18 jaar en ouder met een kantoorbaan.

We zien dat mensen nog maar weinig bewust bezig zijn met hun gedrag op internet en het effect daarvan op anderen of op de werkvloer. Het doel van dit rapport is om zowel consumenten als werkgevers te laten inzien wat het belang is van een eigen(wijs) plan op internet. De missie die we vanuit BIT hebben, is het bijdragen aan een veilig, vrij en open internet met waarborging van privacy. Verantwoordelijkheid, beveiliging, virussen en privacy, het komt in dit rapport allemaal aan bod. Zit er verschil in de wijze waarop internet ingezet wordt voor zakelijke of privédoeleinden?

Het onderzoeksrapport dat nu voor u ligt geeft inzicht in internetgebruik en -veiligheid. Na het lezen bent u volledig op de hoogte van het internet bewustzijn in Nederland en weet u wat u te doen staat om veilig, vrij en open te internetten met waarborging van privacy.

JONG VERSUS OUD

ouderen zijn veiliger op internet

Internet is voor jong en oud. Echter zijn er tussen deze twee groepen flinke verschillen als we kijken naar de omgang met internet. Jongeren maken op een werkdag langer gebruik van internet (4 tot 8 uur) dan de ouderen (2 tot 4 uur). Daarnaast zijn jongeren technischer onderlegd, maar lappen de veiligheid aan hun laars.

Downloadgedrag

Films, muziek, afbeeldingen, software of zipbestanden, iedereen heeft hier wel eens iets van gedownload. Zeker met de internetsnelheden van tegenwoordig, kunnen deze downloads snel binnengehaald worden. Echter is dit niet zonder gevaar. Geïnfecteerde bestanden kunnen veel schade aanrichten. Wanneer de bron onbekend is, is de kans groter dat u een besmet bestand downloadt. Opvallend is dan ook dat slechts 28% van de jongeren een download altijd controleert. Ouderen gaan hier verstandiger mee om. Bijna de helft (48%) controleert een download altijd.

Controleert u, voordat u iets downloadt, of dit veilig is?	18 t/m 34 jaar	35 jaar en ouder
✓	28%	48%

Wanneer een download op veiligheid wordt gecontroleerd, dan wordt door beide groepen vooral de virusscanner gebruikt, gevolgd door controle op aanbieder en bestandsnaam.

Methode downloadcontrole	18 t/m 34 jaar	35 jaar en ouder
Virusscanner	65%	76%
Bestandsnaam	54%	33%
Aanbieder	56%	44%

Jongeren openen zonder pardon e-mails (66%) en bestanden (41%) van een onbekende afzender

Onbekende afzender

De onvoorzichtigheid onder jongeren uit zich ook in het openen van e-mail. E-mails (66%) en bestanden (41%) van een onbekende afzender worden in veel gevallen zonder pardon geopend, wanneer zij denken dat er iets in staat waar ze wat aan hebben. Deze goedgelovigheid wordt misbruikt door hackers. Denk aan een e-mail met onderwerp 'Maak kans op €1.000,-'. Iedereen wil wel zo'n bedrag winnen en dus openen we de mail, die maar zo geïnfecteerd kan zijn.

Ik open e-mails van afzenders die mij onbekend zijn	18 t/m 34 jaar	35 jaar en ouder
Ja	10%	5%
Alleen als ik denk dat er iets in staat waar ik wat aan heb	57%	35%
Nee	34%	60%

Ik open bestanden van afzenders die mij onbekend zijn	18 t/m 34 jaar	35 jaar en ouder
Ja	7%	3%
Alleen als ik denk dat er iets in staat waar ik wat aan heb	34%	22%
Nee	58%	75%

Wachtwoorden

Vaak wordt in de media geroepen dat men zorgvuldig dient om te gaan met wachtwoorden. Een wachtwoord biedt net wat meer bescherming tegen inbraak op eigendommen. Daarnaast is het verstandig om geregeld je wachtwoorden te vervangen. Jongeren vervangen hun wachtwoord minder snel en gebruiken één wachtwoord voor meer dan drie logins. Ouderen schrijven hun wachtwoord vaker op papier om deze niet te vergeten.

	18 t/m 34 jaar	35 jaar en ouder
Mijn wachtwoord verander ik regelmatig	42%	61%
Mijn gebruikelijke wachtwoord gebruik ik voor meer dan drie logins	63%	47%
Ik schrijf mijn wachtwoord(en) op om ze niet te vergeten	28%	42%

Opvallend aan de stellingen is dat bijna de helft van de jongeren aangeeft dat zij regelmatig hun wachtwoord veranderen, terwijl de meerderheid aangeeft dit minder dan één keer per jaar te doen (44%). De meerderheid van de ouderen daarentegen verandert het wachtwoord minimaal één keer per kwartaal (34%).

Ondanks dat veel jongeren over het algemeen niet even verstandig omgaan met veiligheid, weten zij zich daarentegen wel goed te beschermen tegen online reclame. Meer dan de helft van de jongeren gebruikt adblockers.

Gebruik van adblockers	18 t/m 34 jaar	35 jaar en ouder
✓	51%	39%

BITS

"Jaren geleden hadden we bij BIT een incident met phishing. Een medewerker van BIT had een phishing e-mail ontvangen van PayPal en had bijna op de betreffende link geklikt. Ondanks dat wij bij BIT zeer bekend en alert zijn op dit gebied, overkomt het ons dus ook. Hieruit blijkt maar weer dat de phishing mails met de jaren beter en echter worden."

Larissa Wiedeman *Marketing Coördinator bij BIT*

TIP

Het is handig om voor online accounts, die niet vaak gebruikt worden, moeilijke wachtwoorden in te stellen. Het is niet erg als dit wachtwoord lastig is om te onthouden. Wanneer u op dit account wilt inloggen en u het wachtwoord bent vergeten, is er over het algemeen de mogelijkheid om 'wachtwoord vergeten' aan te klikken. Via een link die u in uw mailbox ontvangt, kunt u dan uw account heractiveren. Op deze manier kan er een nieuw (moeilijk) wachtwoord worden ingesteld en kan er ingelogd worden. Op dit moment kunt u de activiteiten uitvoeren die u van plan was. Vervolgens, bij de keer erop dat u weer wilt inloggen, begint u weer bij het opvragen van uw wachtwoord. Op deze manier maakt u gebruik van meerdere unieke wachtwoorden en zijn u en uw privacy weer een beetje beter beschermd op internet.

laks in veiligheid op de werkvloer

Dat internet onveiligheden met zich meebrengt, is bekend. Interessant is om te kijken hoe we hier thuis en op het werk mee omgaan. Uit het onderzoek blijkt dat men op de werkvloer nogal laks met de veiligheid omgaat en dit afschuift op de IT-afdeling.

Back-up

Iedereen heeft het wel ergens op de planning staan, een back-up van de vakantiefoto's maken. De kans dat deze bestanden verloren gaan, is dan klein. Bijna 60% maakt regelmatig back-ups van bestanden op de privécomputer. Veelal is dit automatisch ingeregeld. Op de werkvloer is de Nederlander echter een stuk lakser. Hier maakt nog maar de helft (29%) back-ups. Maar liefst 48% gaat ervan uit dat de IT-afdeling dit voor hen regelt en kijkt er dan ook niet meer naar om. Op privégebied wordt er dus veel zuiniger omgegaan met de bestanden. Opvallend is dat op zowel privé- als werkgebied rond de 15% helemaal nooit een back-up maakt.

Back-up van het bedrijfsnetwerk wordt in de meeste gevallen goed geregeld door de IT-afdeling. Wat veel werknemers vergeten is dat de lokale schijf van de pc vaak niet automatisch geback-upt wordt. Bij een virus of ander probleem gaan op deze manier vaak nog veel bestanden verloren.

Wanneer maken we een back-up?	Privé	Werk
Regelmatig, ik heb dit automatisch ingeregeld	59%	29%
Wanneer ik denk dat er 'iets mis is' met mijn laptop	17%	4%
Wanneer mijn opslaggeheugen bijna zijn limiet bereikt	9%	4%
Nooit	14%	15%

62%

Ik gebruik privé meer verschillende wachtwoorden dan zakelijk

Tegenwoordig zijn er tal van manieren om een back-up te maken. Maar wat vindt de Nederlander het meest gebruikelijk? De ruime meerderheid (75%) kiest voor het gebruik van een externe harde schijf, gevolgd door een USB-stick (26%) en een abonnement bij een online back-up dienstverlener (11%).

Waarmee maken we back-ups?

Externe harde schijf	75%
CD	6%
Abonnement bij online back-up dienstverlener	11%
USB-stick	26%

Wachtwoorden

Wachtwoorden beschermen de privacy-gevoelige data. Zonder wachtwoord-bescherming bestaat het gevaar dat een vreemde bijvoorbeeld een kopie van uw ID, de privé-administratie of de vakantie-foto's ziet en misbruikt of dat klant-gegevens ongevraagd worden gekopieerd. Slechts 3% heeft de werkcomputer niet voorzien van een wachtwoord.

Ondanks de angst om privébestanden kwijt te raken, geeft 11% aan dat de privé PC niet is beveiligd met een wacht-woord. Personen die hun PC wel beveili-gen, geven aan dat zij privé meer wacht-woorden gebruiken dan zakelijk. Tevens worden er ook verschillende wachtwoor-den gebruikt voor privé- en zakelijk gebruik (88%).

Wachtwoorden privé versus werk

Ik heb mijn werkcomputer voorzien van een wachtwoord	97%
Ik gebruik zakelijk meer verschillende wachtwoorden dan privé	33%
Ik gebruik privé meer verschillende wachtwoorden dan zakelijk	62%
Mijn privé- en mijn zakelijke wachtwoord om in te loggen op de computer/laptop komen overeen	12%

Security en cybercrime op de werkvloer

Cybercriminelen worden alsmaar professioneler. Ze hebben steeds meer technische tools, mankracht en financiële middelen tot hun beschikking om een aanval uit te voeren. Uit het onderzoek blijkt dat het zaak is om de werknemers goed op de hoogte te stellen hoe zij met security om moeten gaan. Meer dan de helft (52%) ziet zichzelf namelijk als zwakste schakel binnen de beveiliging van de werkcomputer en bedrijfsgevoelige data. Internet (33%) wordt als tweede zwakke schakel genoemd. De IT-manager is de sterkste schakel in IT-beveiliging op de werkvloer. Bijna alle werknemers (92%) hebben dan ook het volste vertrouwen in de beveiliging die de werkgever heeft geïnstalleerd en gaat ervan uit dat zij zelf vrijwel niets hoeven te doen als het gaat om security op de werkvloer.

Wie of wat is de zwakste schakel binnen beveiliging van de werkcomputer?

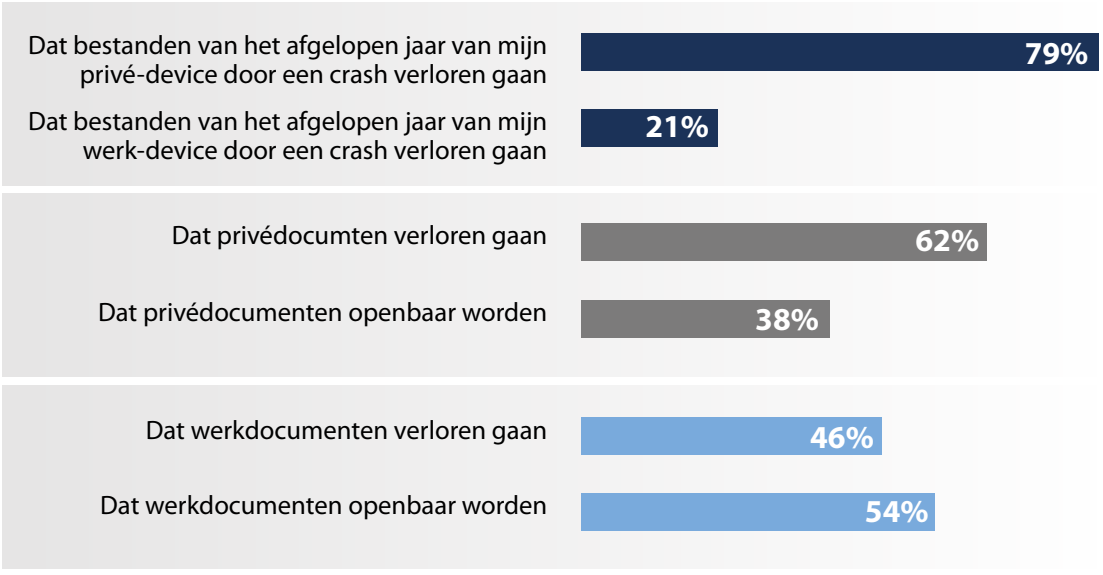
Virusscanner	7%
IT-Manager	2%
IT-afdeling	7%
Ikzelf	52%
Internet	33%

Opvallend! Voor slecht 46% van de werknemers is het een logische stap om de IT-verantwoordelijke te informeren, wanneer zij vermoeden het slachtoffer te zijn geworden van cybercrime. 18% informeert de IT-verantwoordelijke regelmatig, 20% soms en maar liefst 15% doet dit nooit!

Dilemma op Dinsdag

Dilemma op Dinsdag is een simpel concept, maar zet wel de hersenen aan het werk. Een dilemma is een keuze tussen twee zaken die even (on)aantrekkelijk zijn. Dit concept wordt lastiger op het moment dat één van de twee dilemma's gekozen moet worden. Dilemma op Dinsdag is voorgelegd aan de respondenten. Hieronder de resultaten van deze hersenkrakers.

Wat vindt u erger?



BITS

"Op het werk openen werknemers veel gemakkelijker malafide e-mails. Wanneer er twijfel is over de kwaadaardigheid van een mail, dan wordt deze eerder op het werk geopend, dan thuis op het privé-device. Er wordt veelal gedacht: op het werk heeft IT dit wel onder controle, zij regelen het wel."

Wido Potters *Manager Support & Sales bij BIT*

"De laatste maanden horen we van veel bedrijven dat ze te maken hebben met een nieuwe vorm van oplichting: CEO-fraude. De tactieken lijken op phishing, maar de uitvoering is veel geraffineerder. CEO-fraudeurs proberen hun slachtoffers psychologisch te beïnvloeden door echte details in hun verhaal te verwerken. Ze verwijzen bijvoorbeeld naar specifieke karakteristieken van de CEO of noemen namen van collega's. Hierdoor komt de vraag voor een wat ongebruikelijke betaling toch betrouwbaar over. Ik las laatst dat SIDN, specialist op het gebied van .nl-domeinnamen en steunbetuiger voor een beter internet, ook doelwit van CEO-fraude was. De medewerker die de e-mail ontving had twijfels bij de betalingsvraag en vond de e-mail niet overtuigend opgesteld. Deze CEO-fraudeurs hadden zich gelukkig niet goed genoeg voorbereid."

Arjen Steinfort Schaap *Accountmanager bij BIT*

TIP

Er worden tegenwoordig meer back-ups gemaakt dan voorheen. Hieruit blijkt dat Nederland bewuster omgaat met verantwoordelijkheid. Toch geven we vanuit BIT nog graag een tip mee om de back-ups te beveiligen. Dit kan gedaan worden door zelf encryptie toe te passen. De back-up wordt op deze manier versleuteld en alleen de personen met deze sleutel kunnen bij de bestanden. Er zijn enkele gratis tools die hiervoor gebruikt kunnen worden.

- **Voor disk en file encryptie: VeraCrypt**
- **Voor archive en file encryptie: 7ZIP**
- **Voor file en e-mail encryptie: GnuPG**

INTERNETVEILIGHEID VERSUS INTERNETGEVAAR

malafide e-mail massaal herkend

In de online wereld bevinden zich vele gevaren als virussen, spyware, malware, scareware, phishing, social engineering, spam en nog veel meer. Nieuws over security is aan de orde van de dag. Hoe gaan consumenten hiermee om?

Virussen

Malware komt in veel gevallen binnen via advertentienetwerken. Zo meldde RTL onlangs dat een advertentienetwerk dat door grote websites als NU.nl, Marktplaats, Kieskeurig en Startpagina wordt gebruikt, probeerde om malware te installeren op de computers van bezoekers. Zonder hier ook maar op te klikken, kan de PC geïnfecteerd worden met alle gevolgen van dien. Uit het onderzoek blijkt dat het vrij lastig is om er zeker van te zijn of de computer is geïnfecteerd door malware of een virus. 12% van de Nederlanders heeft het vermoeden dat ze zijn besmet, maar weten dit niet zeker. Maar liefst 32% geeft aan dat zij het idee hebben dat hun computer nog nooit is geïnfecteerd, maar dat zij hier niet zeker van zijn. Wanneer er een virus is waargenomen, onderneemt 97% direct actie en weet 80% waar zij terecht kunnen in zo'n geval.

Virusvrij internetten: wat heeft Nederland er voor over?

81% van de Nederlanders vertrouwt volledig op de virusscanner. Om een virusscanner zo optimaal mogelijk te laten werken, is het belangrijk om deze tijdig te updaten. 76% doet dit gelijk zodra de update-melding verschijnt. Anderen doen dit 1x per jaar (10%) of maar net wanneer ze er tijd voor hebben (6%).

Bent u al eens gehackt? Bijvoorbeeld door een virusinfectie?

Ja	9%
Ik vermoed van wel, maar dit weet ik niet zeker	12%
Ik denk van niet	32%
Nee	47%

Wanneer update u uw virusscanner voor uw privé-laptop of privé-computer?

Gelijk zodra ik een update-melding krijg	76%
Ongeveer 1 keer per jaar	10%
Wanneer ik er tijd voor heb	6%
Nooit	3%
Wanneer ik een goede aanbieding krijg	2%
Ik heb geen virusscanner	2%

Het is opvallend dat 30% niet bereid is om te betalen voor een virusscanner. Het merendeel van de Nederlanders vindt tot € 50 per jaar een mooi bedrag om hieraan uit te geven (42%).

Bent u bereid te betalen voor een virusscanner en zo ja, hoeveel?

Ja, tot € 50 per jaar	42%
Ja, tot € 75 per jaar	12%
Ja, tot € 100 per jaar	6%
Ja, maar de prijs is niet belangrijk	11%
Nee	30%

Phishing

Phishing e-mails zijn met de jaren alsmaar moeilijker te onderscheiden van de reguliere e-mails. Waar voorheen half Nederlandse en half Engelse zinnen werden verzonden, zijn phishing mails tegenwoordig foutloos geschreven. Dit vraagt om oplettendheid. Meer dan driekwart van Nederland (83%) is ervan overtuigd een malafide e-mail direct te herkennen.

Een e-mail die afkomstig lijkt te zijn van de bank met een betalingsverzoek erin, is een typisch voorbeeld van phishing. De website waar naar gelinkt wordt, wijkt echter iets af van de website van de bank. Hoe handelen Nederlanders in zo'n situatie? 68% weet dat de bank dit soort verzoeken niet deelt per e-mail en verwijdert de mail direct. Een op de tien Nederlanders sluit de website en forward de e-mail naar de bank om te controleren of het bericht klopt. 8% sluit de website, delete de mail en vertrouwt erop dat de virusscanner de computer beschermt. 7% realiseert zich dat ze te maken hebben met phishing en maakt een melding bij zowel de bank als de politie. Een klein deel van de Nederlanders (6%) sluit de website en schenkt hier verder geen aandacht meer aan. En tot slot vult slechts 1% de gevraagde gegevens in.

Ik vul de gevraagde gegevens in, websites veranderen immers regelmatig	1%
Ik sluit de website en schenk hier verder geen aandacht aan	6%
Ik sluit de website, delete de e-mail en vertrouw erop dat mijn virusscanner het eventuele virus, dat door het klikken op de link naar mijn computer is verzonden, verwijdert	8%
Ik sluit de website en forward de e-mail naar mijn bank om te controleren of het bericht klopt	10%
Ik realiseer mij dat ik mogelijk op een vervuilde link heb geklikt en mogelijk slachtoffer ben geworden van phishing. Ik meld dit direct bij mijn bank en doe aangifte bij de politie	8%
Ik weet dat mijn bank dit soort verzoeken niet deelt per e-mail. Ik verwijder de mail direct	68%

Wat vindt u het meest waarschijnlijk?

42% Een inbreker dringt mijn huis binnen
58% Een cybercrimineel weet mijn bankgegevens te achterhalen

80% Mijn gestolen portemonnee wordt netjes teruggebracht
20% Mijn kwaadwillig verwijderde bestanden worden netjes teruggezet

66% Mijn telefoonnummer wordt achterhaald
34% Mijn inloggegevens worden achterhaald

33% Bij de aankoop van een nieuwe laptop, tablet of smartphone is de beveiliging ook gelijk geregeld
68% Bij de aankoop van een nieuwe laptop, tablet of smartphone is de beveiliging nog niet geregeld

83%
Ik ben overtuigd dat ik een malafide e-mail direct herken

BITs

Het is opvallend dat maar liefst 83% van de Nederlanders overtuigd is direct een malafide e-mail te herkennen. Recentelijk is uit onderzoek gebleken dat 70% van de Nederlanders al eens slachtoffer is geweest van phishing mailings, 33% van social engineering en 40% van malware. Hieruit kunnen we concluderen dat Nederlanders de overtuigingskrachten van malafide e-mails onderschatten.

Respondenten hebben ook een verkeerde inschatting als het gaat om het terugzetten van kwaadwillig verwijderde bestanden. 80% gaat ervan uit dat dit niet waarschijnlijk is. Bij ransomware worden bestanden versleuteld. Tegen betaling worden de bestanden ontsleuteld. Opvallend hieraan is het verdienmodel, betaling leidt eigenlijk bijna altijd tot ontsleuteling. De criminelen zouden hun 'goede naam' op het spel zetten als bekend wordt dat zij na betaling de bestanden toch niet ontsleutelen. Overigens mag het duidelijk zijn dat wij bij BIT niet pleiten voor betaling.

Een ander aandachtspunt is de beveiliging op nieuwe devices. Bij de aankoop van een nieuwe laptop, tablet of smartphone gaat een groot deel van de Nederlanders ervan uit dat de beveiliging dan al is geregeld. Voor een nieuwe laptop gaat dit nog gedeeltelijk op. Bij de aankoop hiervan is er in de meeste gevallen wel een virusscanner geïnstalleerd, maar deze is vaak maar één maand geldig (proefabonnement). Daarna is het de bedoeling dat deze virusscanner wordt verlengd met een betaald abonnement.

Voor tablets en smartphones geldt dat er helemaal geen beveiliging zit op een operating system, zoals Android. Nieuwe releases van Android worden over het algemeen niet ondersteund op oudere hardware. Overigens laat Google de verantwoordelijkheid om oudere toestellen te upgraden met de nieuwste versie van het OS bij de softwarefabrikanten, zoals Samsung, HTC, LG, etc. Telefoons en tablets kunnen over het algemeen na één à twee jaar niet meer geüpdatet worden met de nieuwste versie. Technisch gezien zou dit wel mogelijk zijn, maar vanuit commercieel oogpunt is dit niet aantrekkelijk. Suppliers willen dat consumenten overstappen op een nieuwe telefoon, met de nieuwste software. Wanneer software niet langer ondersteund wordt, is dit een obstakel voor de veiligheid en dus een probleem.

"In Nederland kunnen we op het gebied van internetsecurity spreken van schijnveiligheid. Tijdens de aanschaf van een nieuwe laptop, tablet of telefoon wordt er door 32% gedacht dat de beveiliging dan al wel is geregeld. Daarnaast is meer dan een kwart van de Nederlanders niet bereid om te betalen voor een virusscanner."

Wido Potters *Manager Support & Sales bij BIT*

"Opvallend is het percentage consumenten dat aangeeft dat zij een kwaadaardige e-mail direct herkennen. Uit contact met onze klanten blijkt regelmatig dat er op een malafide e-mail wordt geklikt, met alle gevolgen van dien. Onlangs heeft een klant van ons op de link in een phishing mail geklikt. Hierdoor werden de bestanden versleuteld op zowel het eigen werkstation als op de fileserver. De sleutel is de enige manier om de bestanden te ontsleutelen. Via No More Ransom, een initiatief van onder andere Europol en de Nederlandse politie, kan de sleutel gevonden worden. Werkt dit niet? Dan is de enige oplossing om een back-up terug te zetten. Dit betekent echter wel dat het een en ander aan data verloren gaat tussen het moment van de laatste back-up en de aanval, wat tijd en geld kost. Dit gebeurde maar liefst zeven keer bij onze klant. Hieruit blijkt dat phishing e-mails vaak nauwelijks zijn te onderscheiden van echte e-mails."

Kristian de Bruijn *Security Officer bij BIT*

TIP

Virussen die in e-mails worden meegestuurd, kunnen over het algemeen goed worden afgevangen door de virusscanner. Malware die binnenkomt via geïnfecteerde advertentienetwerken hebben daarentegen een veel grotere impact. Als een systeem succesvol is geïnfecteerd, kan de aanvaller besluiten om bijvoorbeeld ransomware op de computer te installeren. Of het apparaat wordt toegevoegd aan een zogeheten botnetwerk, waarmee DDoS-aanvallen op websites worden uitgevoerd. Deze vorm van malware verspreiden wordt ook wel 'malvertising' genoemd en vormt een steeds groter risico.

De tip om u te beschermen tegen malvertising is om een adblocker te installeren. Er zijn vele verschillende adblockers beschikbaar. Eén van onze favorieten is uBlock origin, een gratis en open source browser extensie voor Chrome, Firefox en Opera.

Het installeren van een adblocker gaat ten koste van het verdienmodel van veel websites die gratis content aanbieden. Met een tracking blocker worden nog wel de (meeste) advertenties getoond, maar wordt de privacy beschermd door het blokkeren van systemen die uw gangen over het internet volgen. Een goed voorbeeld hiervan is Privacy Badger. Deze gratis en open source browser extensie blokkeert spying advertenties en onzichtbare trackers.

PRIVACY WAARBORGEN VERSUS OPENBARE DATA

kennis privacybescherming ontbreekt

Privacy is een groot goed. Het is voor consumenten en bedrijven een nachtmerrie als data op straat komt te liggen. Maar is het bekend hoe privacy beschermd moet worden met alle data die openbaar wordt gemaakt?

Informatie uitwisselen

Informatie met elkaar uitwisselen gebeurt 24/7 via allerlei verschillende kanalen. Bedrijfsdata wordt vooral gedeeld via de e-mailvoorziening van de werkgever (84%), e-maildiensten als Gmail (13%) en online messenger-services als WhatsApp (13%).

Delen van privacy-gevoelige data

Via allerlei wegen wordt er geprobeerd om persoonlijke informatie te achterhalen, vooral via de telefoon, websites en e-mailings. Dit wordt ook wel social engineering genoemd. Bij deze techniek proberen hackers om vertrouwelijke of zelfs geheime informatie te verkrijgen, wat leidt tot cybercriminaliteit.

Let op! Hoe meer privacygevoelige informatie u deelt via internet, des te moeilijker u phishing mails kunt onderscheiden van echte mails.

Hoe wisselt u bedrijfsdata uit met collega's en/of externen?

Via de e-mailvoorziening die mijn werkgever biedt	84%
Via e-maildiensten als Gmail	13%
WhatsApp of andere online messenger-services	13%
Via de post	11%
Via Dropbox	10%
Via Google Drive	8%

Maar gaat Nederland op deze verzoeken in? Of wordt dit afgeslagen? En hoe zit het als men een prijs kan winnen, worden er dan meer privacygegevens achter gelaten?

Het is goed om te zien dat, zowel via de telefoon als via de e-mail, maar 3% bereid is om privacygevoelige data te delen. Wanneer er een prijs te winnen valt, wordt de privacy op het spel gezet. Dit is het moment dat een kwart van de Nederlanders in staat is om privacygevoelige informatie achter te laten op een onbekende website. Gelukkig is 15% net wat verstandiger en onderzoekt de website eerst.

42%

Ik weet niet precies hoe ik mijn privacy moet beschermen op internet

Welke informatie zijn we bereid om achter te laten voor een prijs of korting? Uit het onderzoek blijkt dat we het geen probleem vinden om vrijwel alle mogelijke persoonlijke informatie achter te laten, zoals NAW-gegevens. Behalve ons bankrekeningnummer (2%), die geven we niet zomaar af.

Privacybescherming in eigen handen

Privacybescherming ligt in onze eigen handen. Echter weet maar liefst 42% van de Nederlanders niet precies welke acties zij moeten ondernemen om hun privacy goed te beschermen op internet. Iets dat nog vaak fout gaat is het discreet omgaan met online inloggegevens.

Maar liefst 40% geeft aan dat de logingegevens naast zichzelf bij nog één ander persoon bekend zijn. Ook zijn er Nederlanders die hun logingegevens delen met zelfs twee of drie personen (10%). Daarnaast blijkt uit het onderzoek dat 47% 2 t/m 5 wachtwoorden online gebruikt en 34% rond de 6 à 20 wachtwoorden heeft. Tevens worden wachtwoorden over het algemeen minder dan 1x per jaar veranderd (35%) of 1x per jaar (24%).

Welke privacygevoelige informatie bent u bereid te verstrekken om kans te maken op een prijs of om een korting te krijgen?

E-mailadres	56%
Voornaam	47%
Achternaam	39%
Woonplaats	38%
Postcode	29%
Straat	22%
Telefoonnummer	18%
Bankrekeningnummer	2%

Hoeveel verschillende wachtwoorden heeft u die u online gebruikt?

1	4%
2 t/m 5	47%
6 t/m 20	34%
Eén voor iedere dienst	15%

Hoeveel mensen kennen uw inloggegevens van uw privé-laptop/computer ofweten waar ze dit kunnen achterhalen?

Niemand, alleen ik	50%
Naast mijzelf nog 1 iemand	40%
Naast mijzelf nog 2-3 mensen	10%

Hoe vaak verandert u uw wachtwoord?

Nooit	10%
Minder dan 1x per jaar	35%
1x per jaar	24%
1x per kwartaal	31%

Nederlandse wachtwoordweetjes

Opvallend is dat bijna de helft van de Nederlanders (45%) het hinderlijk vindt dat aanbieders van e-maildienstverleningen kunnen meelezen, maar dat ze niet afstappen van deze gratis dienstverleningen. Gratis e-mail providers hebben toegang tot de inbox van hun klanten en scannen deze op inhoud. Hierdoor worden bijvoorbeeld ook gepersonaliseerde advertenties in uw e-mailomgeving getoond.

BITS

Het valt op dat mensen gemakkelijk hun gegevens achterlaten. Dit brengt twee risico's met zich mee. Allereerst kunnen hackers direct met de gegevens aan de slag. Indirect kunnen gegevens in slechte handen komen, omdat u via een bonafide website, als Albert Heijn, gegevens heeft achter gelaten. Deze data wordt massaal opgeslagen voor marketingdoeleinden, maar kan op straat komen te liggen door een datalek.

Sinds 1 januari 2016 is de Meldplicht Datalekken van kracht. Na tien maanden zijn er al 3.400 meldingen binnengekomen bij de Autoriteit Persoonsgegevens. Hieruit blijkt dat ook bij bonafide ondernemingen regelmatig lekken voorkomen. Het is dus belangrijk om af te wegen hoeveel gegevens u met dergelijke ondernemingen wilt delen. Vanaf 2018 zal de Meldplicht Datalekken overgaan in een nieuwe Europese wet: de Algemene Verordening Gegevensbescherming (AVG).

Een paar jaar geleden heeft er bijvoorbeeld een grote hack plaatsgevonden, waarbij in eerste instantie werd gedacht aan een lek bij KPN, zo meldt de NOS. Later bleek dat de gelekte klantgegevens niet van KPN maar van Baby-Dump afkomstig waren. De verwarring ontstond doordat er een lijst met KPN e-mailadressen was vrijgekomen. Echter bleek dat de hashes, een digitale vingerafdruk die een tekstreeks of bestand identificeert via een reeks karakters, van wachtwoorden gelijk waren tussen KPN en Baby-Dump. Dit bewijst maar weer dat het niet verstandig is om wachtwoorden voor meerdere accounts te gebruiken.

TIP

Om de privacy beter te beschermen, zijn er een aantal zaken noodzakelijk:

- Hergebruik wachtwoorden nooit, maar creëer unieke wachtwoorden voor ieder account. Dit kan met password generators, die online gratis te vinden zijn.

- Het is begrijpelijk dat al deze wachtwoorden niet te onthouden zijn. Gelukkig zijn daar speciale tools voor. Deze password managers onthouden alle wachtwoorden.

- Gebruik daar waar mogelijk two factor authenticatie, zodat u naast een wachtwoord ook een steeds wisselende code op moet geven. Voorbeelden hiervan zijn de DigiD met SMS code en de Google Authenticator.

- Bij accounts die niet vaak gebruikt worden, daarbij kunt u de wachtwoorden bij gebruik opvragen en opnieuw instellen.

- Pas encryptie toe op back-ups. Wanneer u dan bijvoorbeeld uw USB-stick verliest, dan kan niemand bij uw persoonlijke bestanden en gegevens.

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