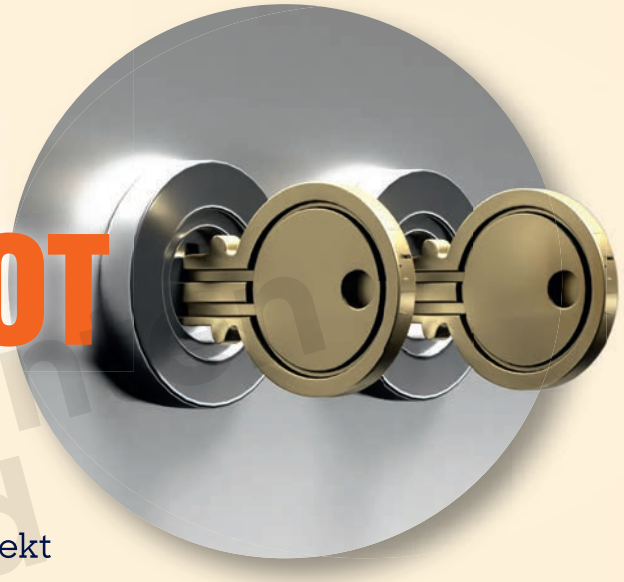
Onderzoek tweefactorauthenticatie

HELFT WEBSITES GEEN DUBBEL SLOT



De helft van de populaire websites beveiligt je account met alleen een wachtwoord: daar ontbreekt tweefactorauthenticatie. Dit maakt je kwetsbaar voor hackers en datalekken.

Al die wachtwoorden onthouden is best vervelend. En sterke wachtwoorden zijn niet eens 100% veilig. Je kunt ze zelf per ongeluk delen, bijvoorbeeld op een nepwebsite. Of ze komen door een hack of datalek in verkeerde handen. Een goede beveiliging tegen hackers die je wachtwoord weten, is het inschakelen van tweefactorauthenticatie (2FA). Lang verhaal kort: bij het inloggen moet je telkens óók een wisselende code invoeren die via een app of ander apparaat binnenkomt. Of je bevestigt je identiteit met een biometrisch kenmerk, zoals een vingerafdruk. Maar om als gebruiker 2FA in te kunnen stellen, moet de website of app de techniek wel aanbieden.

Of dat zo is, onderzochten we bij 109 uiteenlopende sites die populair zijn en/of gevoelige gegevens verwerken. We kozen bewust voor websites en niet voor apps, omdat de site meestal de zwakste schakel is. Aan een app kun je makkelijk een vingerafdrukscan toevoegen – en dat gebeurt gelukkig ook vaak. Via de website heb je dan alsnog toegang tot dezelfde persoonsgegevens. En een hacker pakt altijd de makkelijkste route.

En wat blijkt? Slechts 59 van de 109 websites hebben een 'tweede slot op de deur'. Bij de overige 46% kun je met alleen een (ontfutseld of gelekt) wachtwoord eenvoudig inloggen. Een nuance is wel op zijn plaats: sommige diensten blokkeren inlogpogingen vanaf een vreemde locatie (bijvoorbeeld vanuit Rusland). Maar welke websites dit consequent doen, en hoe precies, is niet eenvoudig goed te peilen. Daarom hebben we dit niet meegenomen in het onderzoek. Vertrouw niet blind op deze beveiligingsmethode.

Big Tech

Bij alle grote techplatforms kun je 2FA instellen. Van Apple, Amazon, Facebook, Google, Microsoft, Samsung tot Twitter. Je beschermt jezelf met 2FA tegen een rampzalige 'accountkaping' na een wachtwoordlek. Bij e-mail en gegevensopslag is 2FA extra belangrijk, omdat het ook de schakel kan zijn naar andere accounts. Bijvoorbeeld via wachtwoordherstel of persoonlijke gegevens in opgeslagen documenten en bijlagen. In het volgende artikel leggen we uit hoe je 2FA instelt bij de genoemde partijen.

Bij alle banken is 2FA al jaren verplicht (denk aan de e-dentifier en de Raboreader). Ook bij de meeste financiële diensten en medische websites in onze steekproef is 2FA mogelijk, of zelfs verplicht. Alleen bij achteraf-betaaldienst Afterpay ontbreekt de optie. Online apotheker dokteronline.com is één van de onderzochte websites die ons heeft beloofd 2FA te gaan invoeren.

Ook bij telecombedrijven is 2FA instellen een goede zet. Logt een crimineel in op iemand anders' account, dan kan hij bijvoorbeeld een nieuw abonnement met een smartphone bestellen of een nieuwe simkaart aanvragen. Als de fraudeur eenmaal een simkaart van een ander in handen heeft, kan hij alle controle-smsjes onderscheppen, zoals die van DigiD en WhatsApp. De grote telecomproviders bieden 2FA aan om zulke 'simswapping' en ander onheil te stoppen. Maar bij de kleinere providers als Budget thuis, Caiway/Delta en simpel.nl ontbreekt 2FA. De meeste hebben wel plannen 2FA volgend jaar in te invoeren, melden ze desgevraagd.

Providermail blijft riskant

Een goede beveiliging van je mailomgeving is van groot belang. Criminelen hebben anders toegang tot een zee aan privéinformatie, en kunnen via de 'herstel via mail'-optie je andere accounts overnemen. Toch heeft geen enkele internetprovider 2FA op zijn mailomgeving. Veel abonnees met mailadressen als jjansen@kpnmail.nl of ppietersen@ziggo.nl lezen hun mail in een e-mailprogramma als Windows Mail, en niet in de browser.

En 2FA in combinatie met een mailprogramma is technisch erg complex. Heb je een providermailadres, dan is het vanuit veiligheidsoogpunt beter om over te stappen op een nieuw e-mailadres bij een onafhankelijke maildienst als Gmail, Outlook.com of Protonmail. Die mailomgevingen zijn wél met 2FA te beveiligen.

Intieme producten

De meeste onderzochte grote webwinkels bieden geen 2FA ter bescherming tegen bestelfraude (pakket op ander adres laten bezorgen) en privacyinbreuken. Dat geldt ook voor de webwinkels die vaak intieme of medische producten leveren. Denk aan christineleduc.nl, easytoys.nl en de bekende online drogisterijen. Bestelgegevens over intieme producten en aandoeningen zijn in juridische zin bijzondere persoonsgegevens. Die verdienen volgens de wet extra bescherming. Webwinkelreus bol.com belooft al enkele jaren dat het 2FA zal introduceren. Medio 2023 komt het er dan echt van, zegt de woordvoerder.

Op marktplaats.nl kun je je gebruikersaccount gelukkig extra beschermen met een sms-controlecode bij inlogpogingen vanaf een andere dan je gebruikelijke computer. Dat is zeker aan te raden. Je voorkomt zo dat criminelen (die je wachtwoord weten of raden) uit jouw naam mensen gaan oplichten. Bij nieuwe accounts is deze sms-controle verplicht.

Verzekeraars beheren gevoelige gegevens. Veel bieden op hun sites 2FA of ze beloven er snel mee te komen. ASR en FBTO hebben nog geen 2FA. FTBO meldt dat bij het declareren van zorgkosten wel alsnog via DigiD moet worden ingelogd. ‘Naar onze mening zorgen we hiermee voor een optimale combinatie tussen gebruiksgemak en veiligheid’, aldus een woordvoerder. Daarmee suggereert FBTO dat 2FA de boel onnodig ingewikkeld zou maken. Dat hoeft niet het geval te zijn als het goed wordt uitgelegd.

Om het eigen energiegebruik te volgen, loggen veel klanten regelmatig in bij hun energieleverancier. Het risico van een gelekt wachtwoord is hier niet enorm, maar een kwaadwillende kan wel volgen wan-

2FA op websites	Biedt tweefactor-authenticatie aan	Planning invoering 2FA
Banken		
abnamro.nl	✓	
asnbank.nl	✓	
bunq.nl	✓	
ing.nl	✓	
knab.nl	✓	
rabobank.nl	✓	
regiobank.nl	✓	
sns.nl	✓	
triodos.nl	✓	
Telecomproviders (account)		
budgetthuis.nl	×	medio 2023
caiway.nl	×	2023
delta.nl	×	2023
freedominternet.nl	×	-
hollandsnieuwe.nl	×	begin 2023
kpn.nl	✓	
simpel.nl	×	-
solcon.net	✓	
t-mobile.nl	✓	
tele2.nl	✓	
vodafone.nl	✓	
ziggo.nl	✓	
E-maildiensten providers		
Caiway mail	×	-
Freedom Internet Webmail (via Imap)	×	-
KPN mail	×	-
Online.nl mail	×	-
Solcon Mail	×	-
T-mobile Thuis webmail	×	-
ZeelandNet mail	×	-
Ziggo Mail	×	-
Webmaildiensten		
gmail.com	✓	
mail.yahoo.com	✓	
outlook.com	✓	
protonmail.com	✓	
Big Tech		
amazon.nl	✓	
apple.com	✓	
facebook.com	✓	
google.nl	✓	
microsoft.com	✓	
samsung.com	✓	
twitter.com	✓	
Webwinkels		
albertheijn.nl	✓	
aliexpress.com	×	-
amazon.nl	✓	
bijenkorf.nl	×	-
bol.com	×	medio 2023
coolblue.nl	×	-
hm.com	×	-
mediamarkt.nl	×	-
wehkamp.nl	×	-
zalando.nl	×	-
Handelsplaatsen		
marktplaats.nl	✓	
Dure producten		
breitling.com	×	-
porsche.com	×	-
Gezondheid & intiem		
christineleduc.nl	×	-
easytoys.nl	×	-
etos.nl	×	-

neer je op vakantie bent, omdat dan je energiegebruik (bijna) nul is. Alleen Budgetenergie en NLE (van hetzelfde moederbedrijf) zeggen medio 2023 2FA te willen invoeren en Vattenfall heeft het al. Tot slot de Consumentenbond zelf. Onze eigen site heeft nog geen 2FA, maar die komt er wel, als optie. Onze sitebeheerder meldt dat het de bedoeling is om de extra beveiliging de komende maanden te introduceren.

Conclusie

Zeker gezien het aantal datalekken van de laatste jaren is het een goede zaak als de toegang tot online omgevingen met persoonlijke gegevens kan worden beschermd met een extra slot. Tweefactorauthenticatie bestaat al langere tijd. Dat anno 2022 slechts de helft van de belangrijkste bedrijven extra beveiliging aanbiedt, valt ons tegen. ■

Overheid verplicht 2FA

Bij belastingdienst.nl en toeslagen.nl log je al jaren in met je persoonlijke DigiD-account. Bij het inloggen kon je al enige tijd 2FA aanzetten voor meer veiligheid. Dat kan in de vorm van een controlecode in de DigiD-app of een code in een sms'je. Een telefoon is dus beslist nodig voor 2FA. Sinds 1 oktober is 2FA verplicht bij inloggen op belastingdienst.nl en vanaf 1 januari 2023 ook op toeslagen.nl. De nieuwe eis is best wel een stap, omdat niet iedereen een eigen mobiele telefoon heeft. Digid.nl meldt echter dat de consument ook een vaste telefoonlijn kan opgeven. Dan krijgt die de codes voorgelezen.

2FA op websites (vervolg)	Biedt tweefactor-authenticatie aan	Planning invoering 2FA
kruidvat.nl	×	-
pabo.nl	×	-
trekpleister.nl	×	-
vegro.nl	×	-
Financiele diensten		
afterpay.nl	×	-
bitonic.nl	✓	
bitvavo.com	✓	
coinbase.com	✓	
degiro.nl	✓	
klarna.com	✓	
litebit.eu	✓	
paypal.com	✓	
peaks.com	✓	
Medische diensten		
amc.nl	✓	
antoniusziekenhuis.nl	✓	
dokteronline.com	×	begin 2023
efarma.nl	✓	
erasmusmc.nl	✓	
infomedics.nl	✓	
isala.nl	✓	
mst.nl	✓	
radboudumc.nl	✓	
rijnstate.nl	✓	
umcg.nl	✓	
umcutrecht.nl	✓	
zgt.nl	✓	
Overheid		
belastingdienst.nl	✓	
mijnoverheid.nl	✓	
toeslagen.nl	✓	
Verzekeraars		
aegon.nl	✓	
asr.nl	×	-
cz.nl	✓	
dela.nl	✓	
fbto.nl	×	-
nn.nl	✓	
ohra.nl	×	medio 2023
onvz.nl	✓	
zorgenzekerheid.nl	✓	
Vakbonden		
cnv.nl	×	-
fnv.nl	×	-
Energieproviders		
budgetenergie.nl	×	medio 2023
deltaenergie.nl	×	-
eneco.nl	×	-
energiedirect.nl	×	-
engie.nl	×	-
essent.nl	×	-
greenchoice.nl	×	-
innovaenergie.nl	×	-
nle.nl	×	medio 2023
oxxio.nl	×	-
unitedconsumers.com	×	-
vandebron.nl	×	-
vattenfall.nl	✓	

Over dit onderzoek: we zochten een goed vindbare optie (of plicht) om 2FA in te stellen bij de gebruikersaccounts van 109 populaire online diensten die populair zijn en/of gevoelige gegevens verwerken. De checkten alleen websites, geen apps, omdat websites vaak de zwakste accountbeveiliging hebben. Een streepje bij 'Planning invoering 2FA' betekent: geen reactie of geen plannen.

Consumenten bond

Digitaal bijblijven?

In de Digitaalgids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding