Inhoud

1 Waarom op iedere dienst een ander wachtwoord gebruiken?

Wachtwoorden zouden geheim moeten zijn. En de beste manier om een geheim te bewaren is het aan niemand te vertellen. Helaas werken wachtwoorden anders. Iedere keer als je inlogt moet je je wachtwoord aan een dienst doorgeven. Je moet het letterlijk intypen. Zo is je wachtwoord moeilijk geheim te houden, toch? En welk account denk jij dat belangrijker is? Dat van je e-mail of van je bank?

Verkeerde inschatting van het belang van accounts

Elie Bursztein, een onderzoeker van Google, publiceerde[1] welke accounts het beste beschermd moeten worden:

1 E-mail

2 Sociale media

3 Bank en overige accounts

1 Account security – a divided user perception: https://elie.net/blog/security/account-security-a-divided-user-perception/

E-mail staat op de eerste plaats. Via e-mail verstuur je veel persoonlijke informatie. Het belang van een e-mailaccount is de laatste jaren sterk toegenomen, doordat er meer gegevens aan zijn gekoppeld. Denk aan documenten in Google Drive of foto's en documenten bij Apple.

Belangrijker nog: via e-mail kun je bijna al je andere wachtwoorden opnieuw instellen! Als je klikt op **Wachtwoord vergeten** dan krijg je daarvoor vaak een link of code via e-mail.

Sociale media bevatten vaak extra persoonlijke informatie, zoals je geboortedatum, burgerservicenummer, privéberichten en foto's. Ieder stukje extra informatie kan een crimineel gebruiken om zich als jou voor te doen. Soms vergeet je zelfs dat je ergens een account hebt aangemaakt. Helaas gebruiken bedrijven deze relatief eenvoudig te verkrijgen gegevens om bijvoorbeeld tijdens een telefoongesprek te 'bewijzen' dat ze echt met jou te maken hebben. Bedenk maar eens wat de energiemaatschappij, je zorgverlener of je internetprovider ter bevestiging vraagt.

Criminelen kunnen onder jouw account vrienden, familie en collega's overhalen tot het klikken op een link, het overmaken van geld of het afstaan van extra informatie. Ook e-mailberichten aan jou zien er met je naam in de aanhef professioneler uit.

De andere accounts zijn minder belangrijk. Elie Bursztein heeft gevraagd hoe gebruikers daarover denken. De top drie van accounts die het beste beschermd moeten worden is volgens hetzelfde onderzoek:

1 Bank

2 E-mail

3 Sociale media

Dat bankaccounts met stip op nummer één staan is vreemd. Online fraude met je bankaccount kost je maximaal een wettelijk bepaald eigen risico (**en.wikipedia.org/wiki/Bank_fraud**). Dat is veel minder erg dan persoonlijke foto's of teksten die voor altijd op internet vindbaar blijven! Dit is een voorbeeld van het verkeerd inschatten van risico.

Een ander voorbeeld zijn diensten waar je in de loop der tijd meer gebruik van gaat maken, bijvoorbeeld een webwinkel (zoals Amazon of Bol.com). Voor een bestelling geef je al de nodige persoonsgegevens af. Maar op termijn verkoop je misschien zelf (tweedehands) via de etalage van de webwinkel. Wie dan toegang tot je account weet te krijgen, kan het bankrekeningnummer voor de ontvangst van de euro's aanpassen. Of denk aan loyaliteitsprogramma's[2] zoals Air Miles.

Kortom, je schat het belang van accounts verkeerd in én het belang kan geleidelijk aan toenemen. Door voor iedere dienst een ander wachtwoord te gebruiken bescherm je iedere dienst. Als je dat consequent doet hoef je er ook niet meer over na te denken.

Organisaties gaan onzorgvuldig met wachtwoorden om

Bij registreren en inloggen verstuur je je wachtwoord naar een dienst. De communicatie tussen jouw apparaat en de dienst hoort versleuteld te zijn. Helaas is dat nog steeds niet altijd het geval. Als dat niet het geval is, kunnen andere mensen vrij gemakkelijk meelezen. Je herkent een versleutelde verbinding aan het slotje in een

2 Change Your Loyalty Program Passwords Now: https://twocents.lifehacker.com/change-your-loyalty-program-passwords-now-1834748255

webbrowser. Bij een app kun je de verbinding niet zo eenvoudig controleren.

Een dienst hoort vervolgens je wachtwoord zelf niet te bewaren. Criminelen proberen de lijst van alle gebruikers, inclusief persoonsgegevens en wachtwoorden, te kopiëren. Daarnaast is het de bedoeling dat wachtwoorden ook voor medewerkers van de organisatie geheim blijven.

In plaats van je wachtwoord hoort de organisatie een wiskundige verhaspeling van je wachtwoord te bewaren. Verhaspelen is iets anders dan versleutelen. Versleutelen kun je omdraaien – ontsleutelen. Omkeerbaar in wiskunde zijn bijvoorbeeld vermenigvuldigen en delen, optellen en aftrekken of kwadrateren en wortel trekken.

Verhaspelen is onomkeerbaar; het is een zogenoemde *one-way hash*. Een sterk vereenvoudigd voorbeeld van hashen[3] gebruikt een restwaarde. Bijvoorbeeld "de rest bij deling door 5". Als je wachtwoord **6** is, dan is de rest bij deling door 5 de waarde 1. Als je wachtwoord **9** is, dan is de rest bij deling door 5 de waarde 4. De dienst bewaart de waarde 1 of 4 in plaats van het daadwerkelijke wachtwoord. Zelfs als je weet dat de formule "de rest bij deling door 5" is gebruikt, is het onmogelijk om jouw wachtwoord te herleiden.

In dit sterk vereenvoudigde voorbeeld zijn wachtwoorden al snel hetzelfde. De rest bij deling door 5 is bijvoorbeeld 0 bij de wachtwoorden **5**, **10**, **15** enzovoort. In de praktijk zijn veel sterkere hashfuncties in gebruik, met berekeningen die langer duren om criminelen te vertragen.

3 Cryptographic Hash Functions Explained: A Beginner's Guide: https://komodoplatform.com/cryptographic-hash-function/

Helaas is in de praktijk de kans groot dat een dienst je wachtwoord helemaal niet verhaspelt maar gewoon leesbaar (dus zelfs onversleuteld) bewaart. Soms zie je dat zelf doordat je je wachtwoord bij registratie via de e-mail ontvangt. Of een medewerker van de klantenservice leest je wachtwoord van het scherm voor.

In 2019 is onderzoek gedaan door IT-freelancers te vragen de registratie van een sociaal netwerk te verzorgen[4]. Dat zijn de ontwikkelaars die aan de basis van online diensten staan. Veiligheid kreeg pas aandacht als het expliciet onderdeel was van de opdracht. Technisch ging het dan nog vaak mis doordat wachtwoorden eenvoudig te ontsleutelen waren. Soortgelijk onderzoek was al eerder uitgevoerd met IT-studenten. Zelfs bij grote bedrijven ging het regelmatig mis. Google waarschuwde in 2019 dat het wachtwoorden van zakelijke gebruikers onversleuteld[5] bewaarde.

Er zijn daarnaast mensen die moedwillig websites bouwen om wachtwoorden van de klanten van hun klanten te achterhalen en misbruiken[6].

Het vervoersbedrijf Transport for London (TfL) kwam in 2019 in het nieuws – reizigers moesten hun wachtwoord op een formulier invullen[7].

---

4 "If you want, I can store the encrypted password." A Password-Storage Field Study with Freelance Developers: https://net.cs.uni-bonn.de/fileadmin/user_upload/naiakshi/Naiakshina_Password_Study.pdf

5 Notifying administrators about unhashed password storage: https://cloud.google.com/blog/products/g-suite/notifying-administrators-about-unhashed-password-storage

6 Vier jaar voor man die webshops met backdoor ontwikkelde: https://www.security.nl/posting/566472/Vier+jaar+voor+man+die+webshops+met+backdoor+ontwikkelde

7 Yes, TfL asked people to write down their Oyster passwords – but don't worry, they didn't inhale: https://www.theregister.co.uk/2019/08/27/tfl_oyster_cards_plain_text_password_form/

Bij steeds meer diensten kun je ervoor kiezen om na het inloggen met je inlognaam en wachtwoord een code van zo'n zes cijfers te typen. De basis van deze korte cijfercode is een willekeurig getal. Dat willekeurige getal moeten zowel jouw mobiele telefoon als de dienst bewaren. De technische specificaties[8] adviseren het willekeurige getal versleuteld te bewaren, maar de kans is groot dat dat niet gebeurt.

Business Insider beschrijft hoe Facebook-CEO Mark Zuckerberg met het Facebook-wachtwoord van gebruikers heeft ingelogd op hun e-mail: "In other words, Mark appears to have used private login data from TheFacebook[9] to hack into the separate email accounts of some TheFacebook users." In 2019 had Facebook wachtwoorden onversleuteld opgeslagen[10]. Medewerkers van de klantenservice van Bol.com[11] konden vroeger ook gewoon je wachtwoord lezen.

Kortom, je kunt er niet op vertrouwen dat organisaties zorgvuldig met je wachtwoord omgaan. Door voor iedere dienst een ander wachtwoord te gebruiken, beperk je het risico tot die ene dienst.

8 TOTP: Time-Based One-Time Password Algorithm > 5. Security Considerations: https://tools.ietf.org/html/rfc6238#section-5

9 In 2004, Mark Zuckerberg broke into a Facebook user's private email account: https://www.businessinsider.com.au/how-mark-zuckerberg-hacked-into-the-harvard-crimson-2010-3

10 Keeping Passwords Secure: https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/

11 Bol.com medewerker kraakte e-mailaccounts van klanten: https://www.security.nl/posting/10480/Bol_com+medewerker+kraakte+e-mailaccounts+van+klanten

Wachtwoorden worden gestolen en gekraakt

Bijna dagelijks zijn er nieuwsberichten over datalekken (*data breaches*) en hacks. Daarbij is dan vaak de lijst van alle gebruikers, inclusief persoonsgegevens en wachtwoorden, buitgemaakt.

In de afgelopen jaren zijn de gebruikerslijsten van grote organisaties zoals Yahoo, Mariott International, Ebay, Quora, LinkedIn, Dropbox en Adobe op straat komen te liggen. Die inloggegevens proberen criminelen vervolgens op andere plekken uit. Bijvoorbeeld voor het plaatsen van bestellingen bij webwinkels[12]. Dit gebeurt ook in Nederland[13].

Daarnaast gebruiken mensen de inloggegevens om je bang te maken en af te persen. Je krijgt dan bijvoorbeeld een e-mailbericht met de mededeling dat je gehackt bent, dat mensen meekijken op je computer en je in de gaten houden via je webcam. Of je even wilt betalen via bitcoin. In het e-mailbericht staat je wachtwoord als 'bewijs'. Je kunt dergelijke berichten negeren of ze rapporteren bij de fraudehelpdesk[14].

In een nieuwsbericht dat een organisatie zelf over een datalek plaatst staat vaak of de wachtwoorden verhaspeld (gehasht) waren of niet. Verhaspelen van wachtwoorden is onvoldoende. Hackers kunnen aan de hand van woordenboeken, veelgebruikte 'slimme' combinaties die mensen toepassen en eerdere wachtwoorden al snel de meeste wachtwoorden achterhalen.

12 The Market for Stolen Account Credentials: https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/

13 Van Zalando tot Bol.com: duizenden gehackte webshopaccounts doorverkocht: https://www.rtlnieuws.nl/tech/artikel/4298786/duizenden-gehackte-webshopaccounts-doorverkocht-op-het-internet

14 Fraudehelpdesk – Ik heb een valse e-mail ontvangen: https://www.fraudehelpdesk.nl/fraude/ik-heb-een-valse-e-mail-ontvangen/

Er zijn zelfs woordenboeken aangelegd om gehashte wachtwoorden te achterhalen. Organisaties die zorgvuldig met je wachtwoord omgaan voegen voor het hashen per gebruiker extra tekens als twist ('zout' of *salt*) toe aan de berekening. Je leest in dat geval over "gesalte gehashte wachtwoorden". Salt vertraagt alleen het kraken van alle wachtwoorden. Als hackers geïnteresseerd zijn in specifieke accounts dan nemen ze het salt gewoon mee in het kraakproces voor specifieke accounts waar zij interesse in hebben.

Voor ontwikkelaars belangrijk om te weten: het leesbaar bewaren van wachtwoorden is strafbaar volgens artikel 32 GDPR. Hoe moet het dan wel? *Salted Password Hashing – Doing it Right*[15]. Het hashen van alleen het wachtwoord van de gebruiker is onvoldoende. Je moet er per gebruiker (en bij het wijzigen van het wachtwoord) willekeurige tekens (*salt*) aan toevoegen. Salt mag je onversleuteld bewaren. Daarnaast is de aanbeveling los van het gehashte wachtwoord en salt een extra reeks van willekeurige tekens versleuteld te bewaren, bijvoorbeeld in een configuratiebestand (*pepper*).

Kortom, al gaat een organisatie zorgvuldig met je wachtwoord om, het kan op straat komen te liggen. Door voor iedere dienst een ander wachtwoord te gebruiken beperk je het risico tot die ene dienst.

15 Salted Password Hashing – Doing it Right: https://crackstation.net/hashing-security.htm

Wachtwoorden delen

In theorie houd je een wachtwoord altijd voor jezelf. Maar soms heb je een generiek account waar een collega ook bij moet kunnen. Of een huisgenoot, denk bijvoorbeeld aan Netflix.

Door voor iedere dienst een ander wachtwoord te gebruiken geef je je collega of huisgenoot eenvoudig gericht toegang tot één account.