OUCH! | April 2017

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wachtzinnen**
- **Wachtzinnen veilig gebruiken**
- **Referenties**

Wachtzinnen

Achtergrond

Iedere dag gebruiken we wachtwoorden om zaken te doen als het raadplegen van jouw e-mail, online bankieren of online te winkelen via de smartphone. Wachtwoorden zijn echter de zwakste schakel, wanneer iemand jouw wachtwoord kent of raadt, hebben ze ook toegang tot jouw accounts. Hierdoor kunnen ze ook geld overmaken, jouw e-mails lezen of jouw identiteit stelen. Net daarom dien je jouw wachtwoorden zeer goed te beschermen. De veelvoud aan wachtwoorden, maakt het moeilijk om ze allemaal te onthouden en vaak maak je fouten als je ze wil gebruiken. In deze nieuwsbrief leer hoe je met een wachtzin werkt, dit is een wachtwoord dat makkelijker is om te onthouden en in te voeren.

Gast redacteur

My-Nogc Nguyen (uitgesproken als Me-Nop Wynn) is een gecertifieerde SANS-instructeur, die de CEO en Principal Consultant is voor Secured IT Solutions. Ze heeft meer dan 14 jaar ervaring en expertise in het ontwikkelen, verbeteren en beheren van cyber security programma's in verschillende sectoren en industrieën. Twitter: **@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Wachtzinnen

Cyber criminelen hebben geavanceerde en effectieve technieken ontwikkelt om wachtwoorden te brute forcen. Dit is het automatisch gaan raden van wachtwoorden. Slechteriken kunnen hierdoor wachtwoorden, die eenvoudig of zwak zijn, makkelijk raden. Door een sterk wachtwoord te kiezen, ben je beter beveiligd. Eerst werd er geadviseerd om complexe wachtwoorden te kiezen, maar het bleek dat deze wachtwoorden moeilijk zijn om te onthouden en in te geven. Wachtzinnen zijn een beter en simpelere keuze. Het is gebaseerd op een reeks van willekeurige woorden of een zin. Hoe meer tekens de wachtzin heeft, hoe veiliger het is. Het voordeel is dat je ze makkelijker kan onthouden en invoeren. Tevens zijn ze moeilijker te hacken door cybercriminelen. Hieronder vind je twee verschillende voorbeelden:

Duurzaam-Simpel-Gevangenis
Tijd voor koffie om 13:23

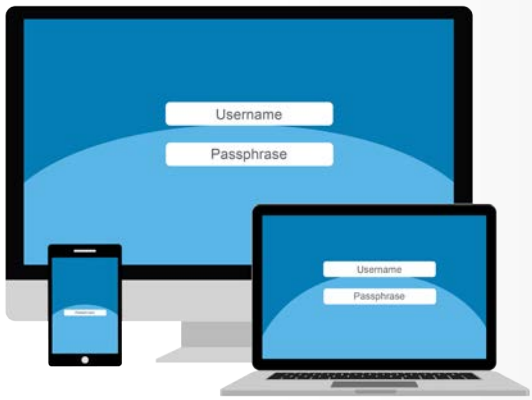
De reden waarom deze wachtzinnen zo veilig zijn, is niet enkel omwille van hun lengte. Het is omdat ze hoofdletters en symbolen bevatten (zoals spaties en leestekens). Tegelijkertijd kan je deze wachtzinnen makkelijk onthouden en invoeren. Je kan de wachtzin nog veiliger maken door de letters te vervangen met cijfers en symbolen. Bijvoorbeeld door de letter "a" te vervangen met het "@" symbool of een "o" met een nul. Indien de website of programma slechts een beperkt

Wachtzinnen

aantal tekens toelaat in het wachtwoord, gebruik dan het maximum toegelaten aantal tekens.

Wachtzinnen veilig gebruiken

Je moet ook opletten hoe je jouw wachtzinnen gebruikt. Als de slechteriken ook de wachtzin kunnen stelen of kopiëren, biedt het weinig toegevoegde waarde.



Wachtzinnen zijn een simpelere manier om sterke wachtwoorden te maken en onthouden.

1. Gebruik een andere wachtzin voor iedere account of toestel dat je hebt. Gebruik nooit dezelfde wachtzin voor jouw werk- of bankaccount die je voor een persoonlijke account gebruikt, zoals Facebook, YouTube of Twitter. Op die manier zorg je ervoor dat wanneer één van jouw accounts wordt gehackt, de rest veilig blijft. Heb je veel wachtzinnen en kan je deze moeilijk onthouden, gebruik dan een password manager. Dit programma kan al jouw wachtzinnen voor je opslaan. Op die manier moet je enkel de wachtzinnen onthouden van jouw computer, toestel en de password manager.
2. Geef geen informatie over de manier waarop je wachtzinnen kiest aan andere personen, zoals jouw collega's of leidinggevende. Besef dat een wachtzin zoals een geheim is, van zodra iemand het weet, is het niet langer veilig. Deel je een wachtzin per ongeluk met iemand of denk je dat het bekend is geraakt of gestolen, verander het dan meteen. De enige uitzondering is wanneer je in een noodsituatie zit (niet gerelateerd met jouw werk), bewaar ze op een veilige locatie en geef de locatie door aan een familielid dat je vertrouwt. Op deze manier zullen jouw geliefden toegang hebben tot jouw accounts als er iets met je gebeurt en hulp nodig hebt.
3. Gebruik geen publieke computers, zoals deze in hotels of andere publieke plaatsen, om in te loggen op jouw account. Iedereen kan deze computers gebruiken en kunnen mogelijk besmet zijn waardoor ze al jouw toetsaanslagen op het keyboard registreren. Gebruik enkel jouw accounts op vertrouwde computers en mobiele toestellen.
4. Wees voorzichtig met websites die verwachten dat je persoonlijke vragen invult. Deze vragen worden gebruikt wanneer je een wachtzin bent vergeten en deze opnieuw wil instellen. Het probleem met persoonlijke vragen is dat je de antwoorden vaak op het Internet kan vinden, wellicht op jouw Facebook pagina. Zorg ervoor dat je persoonlijke vragen antwoordt met informatie die niet publiek beschikbaar is of verzin antwoorden op deze vragen. Heb je moeite om de antwoorden op deze vragen te onthouden? Kies dan een filmpersonage en baseer jouw antwoorden op dit personage. Een andere optie is om een password manager te gebruiken, hier kan je vaak ook extra informatie in bewaren.
5. Bij veel online accounts kan je tegenwoordig inloggen met twee-factor authenticatie, ook wel twee-staps verificatie

Wachtzinnen

genoemd. Naast jouw wachtzin heb je nog iets extra nodig om in te loggen, zoals een code die naar jouw smartphone wordt verstuurd. Deze optie is veel veiliger dan alleen de wachtzin. Schakel het altijd in waar mogelijk en maak gebruik van deze veiligere methode.

6. Mobiele toestellen zijn vaak beveiligd met een PIN-code. Onthoud dat een PIN-code een wachtwoord is. Hoe langer jouw PIN-code, hoe veiliger. Bij veel mobiele toestellen is het mogelijk om jouw PIN-code te veranderen naar een wachtzin of een biometrisch wachtwoord zoals jouw vingerafdruk.
7. Indien je een account niet meer gebruikt, zorg ervoor dat je deze dan afsluit, verwijdert of uitschakelt.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Two Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Lock Down Your Login:	https://lockdownyourlogin.com
SANS SEC301 - Five day course on cyber security basics:	https://sans.org/sec301

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Vertaald door: Sven Jacobs, Tom Palmaers