

OUCH!

IN DEZE EDITIE...

- **Jezelf Beveiligen**
- **Jouw Computer / Accounts Beveiligen**
- **Voor Ouders**

Veilig Online Gamen

Overzicht

Met online gaming kan je veel plezier beleven, maar dit gaat gepaard met bepaalde risico's. In deze nieuwsbrief hebben we het over hoe je jezelf en jouw familie kan beveiligen tijdens online gaming.

Jezelf Beveiligen

Wat online gaming zo interessant maakt, is dat je kan spelen en communiceren met anderen over de hele wereld.

Vaak ken je de mensen niet met wie je speelt. Terwijl de grote meerderheid van de mensen gewoon plezier willen net zoals jij, zijn er ook met minder goede bedoelingen. Hier zijn enkele dingen die je kan doen om veilig te blijven.

- Wees voorzichtig met elke boodschap die je vraagt om iets te doen, als het klikken van een link of het downloaden van een bestand. Net zoals phishing aanvallen, zullen de slechterikken pogen om jou te overtuigen om dingen te doen die jouw computer zullen infecteren. Indien een boodschap er vreemd, dringend of te mooi om waar te zijn uitziet, wees dan argwanend omdat het over een aanval kan gaan.
- Veel online games hebben hun eigen financiële markten waar je virtuele goederen kunt ruilen of verkopen. Net als in de echte wereld, zijn er oplichters die zullen proberen om jouw geld en goederen te stelen.
- Wees voorzichtig met transacties waarbij echt geld wordt gebruikt om in spel aankopen te doen. Doe deze acties enkel op bekende marktplaatsen met een goede reputatie.
- Beperk de hoeveelheid informatie die je of jouw kinderen online delen. Deel nooit persoonlijke informatie zoals jouw wachtwoord of thuisadres.
- Websites, zoals online banking, maken gebruik van security vragen om jouw identiteit te bevestigen. Aanvallers weten de antwoorden te bemachtigen door vrienden te worden met de slachtoffers in de online games. Herinner dat je geen vragen dient te beantwoorden tijdens het online gamen.

Jouw Computer / Accounts Beveiligen

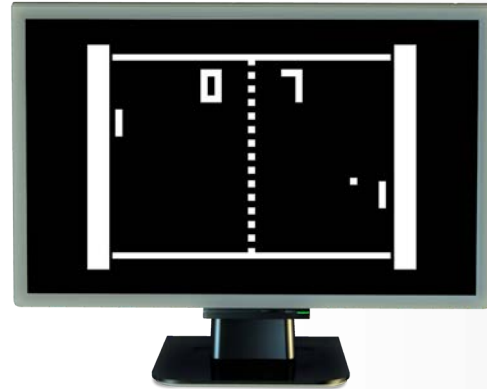
De volgende stap is om de computer te beveiligen. Slechterikken proberen om jouw computer over te nemen of jouw online gaming accounts. Daarom moet je het beveiligen.

Gastredacteur

Jake Williams is de oprichter van Rendition Infosec en is een gecertificeerde SANS-instructeur en auteur van verscheidene SANS-cursussen. Hij is actief op Twitter als [@MalwareJake](https://twitter.com/MalwareJake) en schrijft een blog op malwarejake.blogspot.com.

Veilig Online Gamen

- Gebruik een sterk wachtwoord voor jouw computer en online gaming accounts. Op die manier kunnen aanvallers jouw wachtwoord niet eenvoudigweg raden of overnemen. Indien een game tweestapsverificatie aanbiedt, gebruik het dan. Zorg ervoor bovendien dat je voor iedere account een verschillend wachtwoord neemt. Indien er dan account wordt gelekt, zijn jouw andere accounts nog veilig.
- Beveilig jouw computer door steeds de laatste versie van het besturingssysteem en gaming software te hebben. Net zoals met jouw besturingssysteem en web browsers, heeft oude gaming software bekende zwakheden die aanvallers kunnen exploiteren om zo in jouw computer te hacken. Door jouw computer en game toepassingen te updaten, zal je de meeste van deze zwakheden elimineren.
- Gebruik antivirus, zorg ervoor dat deze up-to-date is en bestanden controleert die worden uitgevoerd.
- Download enkel gaming software van bekende bronnen. Indien je software installeert om een spel te spelen, verzeker je er dan van dat je het downloadt van de leverancier website of van een andere gekende, vertrouwde locatie. Vaak zullen cyberaanvallers een valse of geïnfecteerde versie van een spel maken en deze verdelen vanuit hun eigen server. Indien je deze dan installeert, zullen de slechteriken totale controle hebben over jouw computer.
- Spel add-ons, die vaak ontwikkeld zijn door de community, om meer en nieuwe functies toe te voegen. Aanvallers infecteren soms deze game packs met malware, wat vrij moeilijk te detecteren is door antivirus. Net als wanneer je games downloadt, verzeker je ervan dat de add-ons ook van vertrouwde locaties komen. Indien een add-on vereist dat je jouw antivirus moet uitschakelen, of aanpassingen moet doen aan jouw firewall, gebruik de add-on dan niet.
- Er zijn intussen zwarte markten die cheating activiteiten ondersteunen. Dit is onethisch en veel cheatprogramma's zijn zelf rootkits, de meest gevaarlijke vorm van malware. Installeer of gebruik daarom nooit cheatprogramma's.
- Bezoek de website van de online gaming software die je gebruikt. Veel gaming sites hebben een sectie met advies rond het beveiligen van jezelf en jouw computer, volg deze raad ook op.
- Tenslotte, wees even voorzichtig als je spellen speelt op jouw mobiel toestel. Cyberaanvallers beginnen mobiele toestellen ook te viseren.



De sleutel om veilig te blijven tijdens het online gamen is sterke wachtwoorden te gebruiken, jouw computer te beveiligen en je gezond verstand te gebruiken wanneer je met vreemden praat of wanneer je rare online berichten of verzoeken ontvangt.

Veilig Online Gamen

Voor Ouders

Als je een ouder bent, zorg er dan voor dat jouw kinderen bovenstaande stappen volgen (voor jongere kinderen moet je ze misschien zelf uitvoeren). Communiceer met je kinderen over de risico's. Opleiding en een dialoog met jouw kinderen is een van de meest effectieve stappen die je kan nemen om hen te beschermen. Één van de favoriete trucs is om jouw kinderen te vragen dat ze tonen hoe hun games werken, wandel met hen mee doorheen hun online wereld en vraag hoe een doorsnee spel eruit ziet. Speel even mee met hen. Laat hen ook vertellen over de verschillende mensen die ze online ontmoeten. Online gaming maakt vaak een groot deel uit van jouw kind zijn sociaal leven. Door met hen te praten (en doordat ze met jou praten) kan je problemen ontdekken en hen veel beter beschermen dan eender welke technologie.

Meer Weten?

Ga naar <http://www.securingthehuman.org> 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 Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovaakse. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Passwords:	http://www.securingthehuman.org/ouch/2013#october2013
What is Anti-Virus?:	http://www.securingthehuman.org/ouch/2014#december2014
StaySafe Online:	http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en voor vertalingen.

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



securingthehuman.org/gplus