

OUCH!

IN DEZE EDITIE...

- Overzicht
- De basis
- Kinderen op bezoek

De cyber generatiekloof beveiligen

Overzicht

De meesten van ons voelen zich vertrouwd met technologie, ook om dit op een veilige manier te gebruiken. Maar iedereen heeft familieleden die niet zo vertrouwd zijn met technologie, zeker als ze niet zijn opgegroeid met computers of het Internet. Hier zijn enkele stappen die je kan nemen om deze generatiekloof te beveiligen. Bijkomend zijn er stappen die je kan nemen om jouw kinderen thuis te beveiligen, maar dezelfde maatregelen kunnen worden genomen wanneer jouw kind familieleden bezoekt. Hierdoor gaan we ook verder in op hoe je kan helpen om een veiligere online omgeving te maken, wanneer jouw kinderen familieleden bezoekt.

Gastredacteur

Brian Honan (Twitter [@brianhonan](https://twitter.com/brianhonan)) is een onafhankelijke security consultant in Dublin, Ierland. Hij is de stichter en verantwoordelijke van het eerste CERT van Ierland, een speciale adviseur voor Europol's Cybercrime Centre (EC3) en doceert informatiebeveiliging aan het University College in Dublin. Hij heeft verschillende boeken geschreven en schrijft voor verscheidene industrie instanties.

De basis

Slechts enkele basisstappen helpen je al een eind op weg om iemands digitale leven te beveiligen. Dit zijn dezelfde stappen die we ieder familielid aanraden. Als je familielid deze stappen niet begrijpt, loop er dan samen door of voorzie ze zelf.

- **Social Engineering:** leg het begrip social engineering uit op een eenvoudige manier die iedereen kan begrijpen. Oplichterij en oplichters bestaan al duizenden jaren, deze praktijken zijn niet nieuw. Het enige verschil is dat slechteriken nu dezelfde tactieken toepassen op het Internet. Geef daarom voorbeelden van de meest voorkomende vormen van oplichting, zoals de gebruikelijke phishing e-mails of de beruchte Microsoft tech support telefoontjes. Leg ook uit aan jouw familieleden waarom ze nooit hun wachtwoord moeten delen of toegang vanop afstand moeten verlenen voor hun computer. Ten slotte, geef aan dat wanneer zich ongemakkelijk voelen of vragen hebben bij een e-mail of telefoongesprek, dat ze jou eerst kunnen bellen alvorens de informatie vrij te geven.
- **Wi-Fi thuisnetwerk:** Neem de tijd om te kijken of het Wi-Fi netwerk bij hun thuis is beveiligd. Zorg er minstens voor dat het standaard admin wachtwoord is gewijzigd en dat er een sterk wachtwoord wordt gebruikt voor het Wi-Fi thuisnetwerk en dat het netwerk de meest recente vorm van beveiliging gebruikt.
- **Patching:** Systemen volledig up-to-date houden is een van de belangrijkste stappen die je kan nemen om iedere

De cyber generatiekloof beveiligen

technologie te beveiligen. Zorg ervoor dat alle thuishoestellen (inclusief mobiele toestellen) en toepassingen volledig zijn gepatcht. De simpelste manier om dit te bereiken is door automatische updates in te schakelen waar mogelijk.

- **Antivirus:** Mensen vergissen zich wel eens, soms klikken en installeren we dingen die we niet hadden moeten doen. Hoewel antivirus niet alle malware kan vermijden, helpt het in het detecteren en stoppen van veelvoorkomende aanvallen. Zorg ervoor dat computers thuis een antivirus hebben en dat deze actief is.
- **Wachtwoorden:** sterke wachtwoorden zijn belangrijk om toestellen en online accounts te beschermen. Begeleid uw familieleden in het creëren van sterke wachtwoorden. Wachtzinnen zijn hier het makkelijkst om te gebruiken en onthouden. Een ander idee is om een wachtwoord manager te installeren en leer ze dit dan te gebruiken. Als dat niet lukt, leer hen dan om wachtwoorden op te schrijven en ze op een veilige plek te bewaren waar zij enkel in kunnen. Voor belangrijke online accounts kan je ook twee-staps-verificatie instellen.
- **Back-ups:** Wanneer al de rest niet werkt, bieden back-ups de redding. Zorg ervoor dat familieleden een eenvoudige en betrouwbare file back-up oplossing hebben.



Oudere generaties kunnen hulp nodig hebben om hun technologie te beveiligen en bij het creëren van een veilige omgeving voor jongere kinderen die met bezoek zijn.

Je kan maandelijks of ieder kwartaal controles doen om ervoor te zorgen dat alle maatregelen nog actief zijn. Overweeg in het slechtste geval om software dat beheer vanop afstand mogelijk maakt te installeren op het toestel, maar zorg ervoor dat het is beveiligd met encryptie en een sterk, uniek wachtwoord.

Kinderen op bezoek

Vaak wanneer kinderen op bezoek zijn bij een familielid, zoals de grootouders, gelden de regels van thuis niet meer. Dit kunnen ook regels zijn die jouw kinderen online helpen te beschermen. Hier zijn enkele stappen die je kan nemen om kinderen te beschermen:

- **Regels:** zorg ervoor dat wanneer je regels of verwachtingen hebt over de veiligheid van jouw kind dat jouw familieleden op de hoogte zijn. Bijvoorbeeld, zijn er regels over hoe lang de kinderen online mogen gamen of

De cyber generatiekloof beveiligen

wanneer ze precies toegang hebben tot hun mobiele toestellen? Geloof ons, probeer niet om de regels uit te leggen aan de grootouders of andere familieleden. In de plaats daarvan maak een regels overzicht en deel dit met familieleden die het kind vaak bezoekt.

- **Controle:** indien jouw kinderen de technologie beter begrijpen dan de oppas, zullen ze er mogelijk misbruik van maken. Bijvoorbeeld, kinderen kunnen vragen achter beheerdersrechten op de computer van de grootouders om dan te doen wat ze willen. Zoals het installeren van een spel dat ze van jou niet mogen spelen. Zorg ervoor dat familieleden begrijpen dat ze kinderen geen extra toegangen mogen geven dan datgene wat ze reeds hebben.

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 Slovakije. 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
Securing Your Home Network:	http://www.securingthehuman.org/ouch/2014#january2014
Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Anti-Virus:	http://www.securingthehuman.org/ouch/2014#december2014
Protecting Your Kids Online:	http://www.securingthehuman.org/ouch/2013#april2013
Tech Phone Support Scams:	http://www.onguardonline.gov/articles/0346-tech-support-scams
Creating a Cyber Secure Home Poster:	http://www.securingthehuman.org/resources/posters

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](https://www.securingthehuman.org/gplus)