OUCH! | June 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Achtergrond
- De risico's
- Kinderen opvoeden

Kinderen cyberveiligheid bijleren

Achtergrond

Kinderen kunnen vandaag op heel wat verschillende manieren online gaan om met andere te communiceren. Nieuwe sociale media rijzen op als paddenstoelen en er zijn steeds meer en meer apps of games die een online verbinding vereisen. Bovendien maken veel scholen nu gebruik van diensten als Google Drive en verwachten dat het huiswerk online wordt ingediend. De kinderen groeien letterlijk op een "verbonden" manier op. Dit heeft verscheidene voordelen maar gaat ook gepaard met risico's. In deze nieuwsbrief, hebben we het over drie risicogebieden voor kinderen en vertellen we wat je kan doen zodat ze veilig blijven.

Gastredacteur

Bob Rubis is een Security Data wetenschapper bij Verizon, auteur van het 2015 Data Breach Investigations Report en vader van vier geweldige kinderen. Bob heeft effectieve security awareness programma's opgezet en beheerd bij verschillende Fortune 100 ondernemingen. Je kan Bob op Twitter volgen via **@hrbrmstr**.

De risico's

1. **Gedrag**: Wanneer kinderen in online of virtuele werelden dingen doen, kunnen ze zich anders gedragen dan in de echte wereld. Het gebrek van fysieke aanwezigheid creëert een gevoel van anonimiteit vooral voor kinderen. Vaak zullen ze in de verleiding komen om andere kinderen te kwetsen door te cyberpesten of door griefing. Bovendien kunnen jouw kinderen het slachtoffer worden van anderen die hen willen kwetsen of gemeen zijn.

2. **Contact**: Kinderen zijn nu bijna continu in verbinding met anderen via sms, online communities of door te spelen in virtuele werelden. Het gebrek aan fysieke aanwezigheid zorgt ervoor dat ze vergeten dat het individu aan de andere kant mogelijk iemand anders is. Roofdieren zijn actief in deze digitale wereld en zullen iedere tactiek gebruiken om relaties op te bouwen met potentiële slachtoffers, door zich voor te doen als kinderen.

3. **Inhoud**: er zijn veel mogelijkheden om video, geluid, foto's en tekstboodschappen online te plaatsen. Kinderen hebben de neiging om overvloedig te posten of veel informatie te delen over zichzelf en andere familieleden, zonder te beseffen wat de gevolgen kunnen zijn. Kinderen beseffen mogelijk niet wat de gevaren zijn van identiteitsdiefstal of

Kinderen cyberveiligheid bijleren

malware infecties wanneer anderen achter informatie vissen of vragen om iets te doen als het klikken op links. Ten slotte, leven we in een tijdperk waarbij we zaken die we online posten of delen met anderen niet ongedaan kunnen maken. Kinderen denken dat Facebook, Instagram, Snapchat en andere posts een tijdelijk karakter hebben, maar ze kunnen terugkeren op een later tijdstip om henzelf of andere familieleden te beschamen.

Het belangrijkste om je kinderen online te beschermen is door ze de gevaren te leren die ze kunnen tegenkomen en door ervoor te zorgen dat ze met jouw erover praten.

Kinderen opleiden

Het belangrijkste wat je kan doen om je kinderen te beschermen is door met ze te praten. Weet wat je kinderen online uitvoeren, leer hen over de risico's en wat ze kunnen doen om zichzelf te beschermen.

1. **Veiligheid thuis**: Thuis is de plek waar veilig online gedrag start. Hoe jonger je begint met hen te praten en zij met jou, des te beter. Houd regelmatig gesprekken over online veiligheid en ga zelfs zover dat je voorbeelden toont van hoe het fout kan lopen. Als je niet weet wat je kinderen doen, vraag het dan gewoon. Speel even de onwetende ouder en vraag hen of ze de laatste technologieën willen tonen en hoe je deze gebruikt. Kinderen vinden het idee om leraar te zijn fijn en zullen dit met plezier doen. Bijvoorbeeld als ze actief zijn op Instagram, vraag dan hoe Instagram werkt en laat ze een account voor jou opzetten en zorg dan dat je ze volgen. Hierdoor zal je niet enkel jouw kinderen volgen, maar maak je het ook makkelijker voor hen om met jou te praten. Bovendien, zorg ervoor – in de mate van het mogelijke – dat alle online activiteiten in gemeenschappelijke ruimtes van het huis plaatsvinden en beperk de tijd dat ze dit mogen gebruiken. Door computers te plaatsen in een gemeenschappelijke ruimte, zullen kinderen zich minder waarschijnlijk met gevaarlijke zaken bezighouden. Overweeg een centrale oplaadplaats voor mobiele toestellen, dit is de plaats waar mobiele toestellen zijn wanneer de kinderen 's nachts gaan slapen.

2. **Veiligheid bij anderen**: Wanneer kinderen weg zijn van thuis, lopen ze meer risico. Zorg ervoor dat ze begrijpen dat de cyber etiquette overal van toepassing is en communiceer jouw regels aan diegenen waaraan je hun zorg toevertrouwt. Indien ze mobiele toestellen hebben, bekijk dan de gebruikspatronen (tijd en datagebruik) om te zien of ze mogelijk misbruik maken van de situatie buitenshuis. Je kan niet alles verhinderen, maar jouw raad zal hen doen nadenken wanneer ze met hun mobiele toestellen dreigen af te dwalen.

3. **Veiligheid, een zaak van iedereen**: je bent niet alleen in deze cyberwacht en je dient andere ouders, familieleden, leerkrachten en vrienden te motiveren om mee een oogje in het zeil houden voor mogelijk schadelijk gedrag. Probeer

Kinderen cyberveiligheid bijleren

ervoor te zorgen dat ze mee zijn met de kinderen en moedig hen aan om een positieve opvoeding te gebruiken wanneer kinderen gevaarlijke zaken doen.

Ten slotte wanneer kinderen fouten maken, behandel het dan als een leerervaring in plaats van ze meteen te berispen en te straffen. Leg hen iedere keer het 'waarom' uit en herinner hen er aan dat je ze wil beschermen tegen de gevaren die ze momenteel nog niet zien. Laat ze weten dat ze naar jou kunnen komen als ze ongewone zaken ervaren tijdens online activiteiten. Laat hen misschien zelfs een screenshot nemen om aan jou te tonen. Zorg ervoor dat ze zich op hun gemak voelen als ze jou aanspreken wanneer ze beseffen dat ze iets ongehoord hebben gedaan. Een open en actieve communicatie is de beste manier om kinderen online te beschermen in de hedendaagse digitale wereld.

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)

Child focus Clicksafe:	http://www.childfocus.be/nl/preventie/clicksafe-veilig-internetten
Tips tegen online pesten:	http://www.kennisnet.nl/kids/watnou/mediawijsheid/tips-tegen-online-pesten/
Kinderen online:	https://veiliginternetten.nl/themes/kinderen-online/
Cyber Smart:	http://www.cybersmart.gov.au/Parents.aspx
Stay Safe Online:	https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens
Online opvoedhulp:	http://www.online-opvoedhulp.nl/blog/kinderen-media/60/grooming-cyberlokken-hoe-zorg-je-als-ouder-ervoor-dat-jouw-kind-het-niet-overkomt.html

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