Word geen slachtoffer of dader van internetcriminaliteit

Informatie voor ouders

De vijf belangrijkste feiten op een rij

Supersnel geld verdienen bestaat niet.
Lijkt iets te mooi om waar te zijn, dan is dat het vaak ook. Zorg dat je kind zich dit realiseert.

Laat je kind NOOIT bankgegevens, identiteitsbewijs, inloggegevens of codes met een ander delen.

Weet dat digitale misdrijven net zo erg en net zo strafbaar zijn als andere misdrijven.

Schaam je niet als je online bent opgelicht.
Het gebeurt heel veel, óók bij volwassenen.

Is je kind een hacktalent? Er zijn volop kansen om hier legaal geld mee te verdienen.

Geldezels

- Mensen die hun rekening uitlenen aan criminelen die daarmee gestolen geld wegsluizen, worden geldezels genoemd. De criminelen benaderen mensen, en dus ook kinderen en jongeren, om hun bankgegevens (betaalpas, pincode, rekeningnummer) te delen. Vaak ontvangen zij hier geld of een product voor.
- Ga in gesprek met je kind over de term *geldezels* en leer je kind om zijn of haar rekening, pinpas of pincode nooit te delen met iemand anders.
- Wie zich bewust of onbewust als geldezel laat gebruiken, kan strafrechtelijk in de problemen komen. Minderjarigen kunnen vier jaar lang een bankblokkade krijgen en volwassenen acht jaar. Dit betekent: geen rekening openen en geen lening of hypotheek afsluiten.
- Criminelen zoeken ook online naar geldezels. Praat hierover met je kind. Ze sturen bijvoorbeeld via Instagram of Snapchat berichtjes als: ‘Wil je snel geld verdienen? Stuur dan een DM.’
- Kijk mee naar de bankzaken van je kind.

- Hoor je van je kind dat iemand om zijn of haar bankgegevens, pinpas of pincode vraagt? Meld het bij de politie. Juist door aangifte te doen, krijgt politie de kans om daders op te sporen. Hoe meer informatie, hoe groter de kans dat daders worden gepakt. Aangifte doen kan ook online.

Identiteitsfraude

- Ga met je kind in gesprek over identiteitsfraude en spreek af dat je kind nooit een foto of kopie van het identiteitsbewijs naar iemand opstuurt. Soms heb je geen andere keuze, bijvoorbeeld omdat een werkgever of verhuurder om een ID vraagt. Scherm dan het Burgerservicenummer (BSN-nummer) af via de kopie ID-app van de Rijksoverheid.

Meld identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude van de Rijksoverheid.

Halt.

- Bespreek met je kind dat hij of zij nooit het identiteitsbewijs, zoals een paspoort of ID-kaart, uitleent. Ook niet aan een broertje, zusje of goede vriend. Met het uitlenen van identiteitsmiddelen riskeer je een strafrechtelijke maatregel zoals een Halt-straf of een boete. Het kan ook leiden tot een bestuurlijke maatregel, zoals opname in het Register Paspoortsignaleringen (RPS). Het gevolg van opname in het RPS is dat de jongere enkele jaren geen nieuw paspoort krijgt. Buiten Europa reizen is dan niet meer mogelijk.

Internetoplichting

- Bespreek met je kind dat als een deal te mooi lijkt om waar te zijn, dat het dat dan ook vaak is.
- Lees altijd recensies van andere kopers over een webshop of aanbieder op Marktplaats. En schrijf zelf een recensie als je bent opgelicht.
- Klik hier voor de website waar je (ver)kopers kunt controleren.
- Via stopheling.nl (of de app stopheling) kun je kijken of een aangeboden product als gestolen bij de politie geregistreerd staat. Voorkom dat je je schuldig maakt aan heling en koop dus niets voor een prijs die te mooi is om waar te zijn zonder goed te controleren of het wel klopt.
- Maak gebruik van de mogelijkheden om veilig te handelen, bijvoorbeeld de veilig oversteken-service en mogelijkheden tot veilig betalen.
- Bel meteen je bank als je denkt dat je bent opgelicht.

- Doe altijd aangifte als je denkt dat je bent opgelicht. Dit verhoogt de pakkans van de dader.
- Aangifte kan op verschillende manieren via internet (politie.nl), telefonisch (0900-8844) of op een politiebureau.

Hulpvraagfraude

- Maak afspraken met je kind over wat hij of zij kan doen als iemand om financiële hulp vraagt.
- Maak nooit alleen op basis van een chat geld over: bel of spreek eerst altijd af met de persoon die om geld vraagt, voordat je geld geeft.
  Niet gebeld = geen geld!
- Maak gebruik van verificatie in twee stappen en deel nooit de code die nodig is om in te loggen.
- Neem bij vermoeden van fraude direct contact op met je bank. Blokkeer het rekeningnummer van de oplichting.
- Doe aangifte bij de politie. Aangifte kan op verschillende manieren via internet (politie.nl), telefonisch (0900-8844) of op een politiebureau.
- Maak een melding bij fraudehelpdesk.nl.

Voorkom phishing

- Phishers gebruiken vaak urgentie of dreigementen om je te verleiden. Bijvoorbeeld: ‘Reageer snel om te voorkomen dat uw account wordt opgeheven.’ Laat je niet onder druk zetten.
- Phishingmail is soms lastig te herkennen. Open in ieder geval nooit bijlagen van onbekende of twijfelachtige afzenders.
- Je kunt bij de Fraude helpdesk een melding doen van phishing. Meld het ook bij jouw bank. Zij kunnen op die manier de andere klanten informeren.
  Hoe je dit doet? Kijk op veiliginternetten.nl.

Halt.

Hacken

- Praat met je kind over de risico's en de gevolgen van hacken. Inbreken in de computer van iemand anders (hacken) of inbreken in een sociale media-account is strafbaar. Er staat maximaal twee jaar gevangenisstraf op, of een boete van € 20.500. Als je gegevens van iemand anders overneemt of verandert dat kan dit nog hoger worden. Je krijgt ook een strafblad en mogelijk geen Verklaring omtrent het Gedrag.
- Als je kind veel snapt van computers en veel talent heeft, dan kan je kind iets positiefs doen met dit hacktalent, Kijk op publicaties.politie.nl/changeyourgame/ en doe challenges, leer wat wel en niet strafbaar is en hoe je eerlijk geld kan verdienen met je talenten.

Bescherm je gegevens

- Maak afspraken met je kind over hoe je gegevens goed kan beschermen. Denk hierbij aan:
  - voor elk account een apart (en lang) wachtwoord gebruiken,
  - een tweestapsverificatie en
  - wachtwoorden nooit met iemand anders delen.
- Als de computer vraagt om je wachtwoord te onthouden doe dit dan niet op een computer die niet van jou is. Iemand kan zo gemakkelijk toegang krijgen tot jouw gegevens. Typ dus elke keer opnieuw je wachtwoord in. Vergeet ook niet je scherm te vergrendelen als je pauzeert en overal uit te loggen voordat je afsluit.
- In treinen, hotels en cafés kun je vaak wifi gebruiken zonder in te loggen. Deze openbare netwerken zijn makkelijker te hacken dan beveiligde netwerken. Een hacker ziet dan alles wat jij op internet doet en intypt (dus ook je bank- en inloggegevens).
- Stel updates van je computer en telefoon niet uit.

Zorgen

Maak je je zorgen over je kind? Je kunt altijd contact opnemen met officiële instanties zoals Meldknop.nl. Deze website geeft je informatie en tips, bijvoorbeeld over wat je kunt doen als je gehackt of opgelicht bent. Maar ze hebben ook informatie als je online lastiggevallen of gepest wordt.
Ook kun je direct contact opnemen met de juiste instanties via chat, mail of telefoon. Meldknop.nl is onderdeel van de Nederlandse politie en is dus een legitieme bron. Ze kunnen je in contact brengen met De Kindertelefoon, de politie en andere officiële websites die je verder kunnen helpen.

Slachtoffer geworden van oplichting?

Praten over oplichting zorg voor opluchting. Praat erover met je kind. Je kunt ook contact opnemen met Slachtofferhulp Nederland via 0900-0101 of via slachtofferhulp.nl

Halt.