Voorkom dat je slachtoffer of dader wordt van internetcriminaliteit!

Denk na over welke informatie je over jezelf deelt en welke foto`s en video`s je plaatst

Je adres of telefoonnummer gaan alleen echte vrienden iets aan. Bij de privacy-instellingen van je social media accounts kun je aangeven wie op je social-account kan kijken. Denk goed na wat je online plaatst, informatie kan jaren later weer opduiken en voor problemen zorgen. Let ook op met het doorsturen van foto`s en video`s. Het doorsturen van naaktfoto`s en video`s is strafbaar.

Houd je wachtwoord geheim

Bedenk een wachtwoord dat niet makkelijk te raden is en houd het geheim. Gebruik hoofdletters, kleine letters, cijfers en leestekens door elkaar. Met een tweestapsvertifcatie kun je het beste je account beveiligen. Gebruik voor ieder account een ander wachtwoord. Als je overal hetzelfde wachtwoord gebruikt, ben je een gemakkelijke prooi voor internetcriminelen.

Pas op met je online-aankopen

Niet alles wat op internet staat is betrouwbaar. Betrouwbare webwinkels maken gebruik van veilige online betaalmethoden zoals ideal. Via www.stopheling.nl kun je kijken of het 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 checken of het wel klopt.

Houd je bankrekening, pinpas en pincode privé!

Als iemand vraagt of je snel geld wil verdienen? Ga er niet op in en geef nooit je bankrekeningnummer of bankpas aan vreemden. Ben je benaderd voor het uitlenen van je pas of pincode? Meld dit dan bij de politie. Zo help je de politie criminele netwerken op te rollen. Melden kan op drie manieren:

- Bel de politie op 0900-8844 of bij spoed 112.
- Anoniem: bel 0800-7000 of meldmisdaadanoniem.nl.
- Meld het bij je bank.

Pas op voor phishing! Klik niet zomaar op een link

Een e-mail, whatss-app/SMS of betaalverzoek met een foute link erin is een veelgebruikte manier om je gegevens te achterhalen of je over te halen om geld om te maken. Dit heet phising. **Je moet altijd eerst checken, dan klikken.**

- Check de URL van een link door er met je muis te gaan staan (niet klikken). Kijk goed of er vreemde dingen in de URL staan.
- Check het e-mailadres van de afzender.
- Krijg je onverwacht een betaalverzoek van een bekende of een bedrijf? Bel op en vraag of het klopt.

Vertrouw je iets niet? Of er is online iets vervelends gebeurd?

Vertel het dan aan je ouders of ga naar meldknop.nl voor advies.

www.halt.nl