Politie
Aalst

Online criminaliteit - preventie

In deze folder vind je de meest voorkomende vormen van internetcriminaliteit en geven we je mee wat je kan doen om te voorkomen dat je slachtoffer wordt.

Wat is internetcriminaliteit?

Criminelen maken steeds vaker gebruik van de anonimiteit van het internet en proberen mensen op te lichten via allerlei kanalen.
Internetcriminaliteit is de verzamelnaam voor vormen van criminaliteit waarbij het internet gebruikt wordt.
Oplichters vinden steeds nieuwe invalshoeken om personen in de val te lokken. Meer en meer pikken ze in op onderwerpen in de actualiteit.

Om jezelf te beschermen, kan je steeds de drie T's in je achterhoofd houden:

Te Mooi

De charmes van knappe mannen en vrouwen, de buitenkans van je leven, een uitzonderlijk lage prijs, ...
Als het te mooi lijkt om waar te zijn, dan is het dat meestal ook.

Twijfel

Niemand is vrij van online fraude. Maar je kan wel de alarmsignalen leren kennen. Als je ergens over twijfelt op het internet, doe het dan niet.
Twijfel je er aan of de info die je kreeg klopt? Dan kan je bijvoorbeeld de phishing- of beveiligingstest doen op safeonweb.be. Via de safeonweb-app kan je nagaan welke (nieuwe) bedreigingen er zijn.

Training

Blijf op de hoogte van de meest recente fraudetrucs. Dat kan via de politie of safeonweb.be. Informeer je, neem je tijd en zorg voor de juiste beveiliging.

OPLICHTING VIA INTERNET - PHISHING - SMISHING

Je ontvangt een e-mail of een bericht (sms, Whatsapp of andere chatfunctie) met een link die je naar een valse website stuurt. Daar wordt gevraagd je persoonlijke gegevens in te vullen (pincode, wachtwoord, ...), een app te installeren of je rekening te verifiëren door een kleine betaling te doen. De oplichter ontvangt zo jouw gegevens en kan ze misbruiken.

Wat kan je doen om dit te voorkomen?

> Denk niet te snel "Mij overkomt het niet". Online criminaliteit kan iedereen overkomen. Wat te mooi lijkt om waar te zijn, is dat meestal ook.
> Handel een verkoop nooit af buiten de erkende zoekertjessite. Betaal niet via een pakjes- of transportbedrijf. Vermijd betalingen via geldtransferagentschappen zoals Western Union of Moneygram.
> Stuur nooit identiteitsdocumenten door via mail aan onbekenden. Geef nooit betaalkaartgegevens en/of vertrouwelijke codes door via e-mail of telefoon.
> Meld verdachte e-mails of andere berichten (sms, WhatsApp, ...) via verdacht@safeonweb.be en verwijder ze. Neem in geval van twijfel contact op met de zogenaamde afzender van het bericht.
> Klik nooit zomaar op verdachte links en bijlagen.
> Doe online aankopen enkel via betrouwbare websites. Let op het adres van de websites, het slotje naast de URL 🔒 en http**s**://.

VRIENDSCHAPSFRAUDE

Iemand laat je geloven je vriend/vriendin te zijn, maar is enkel uit op je geld. De oplichter probeert je vertrouwen te winnen en speelt in op emoties. Als de oplichter je vertrouwen gewonnen heeft, vraagt deze (meermaals) om geld over te schrijven.

Wat kan je doen om dit te voorkomen?

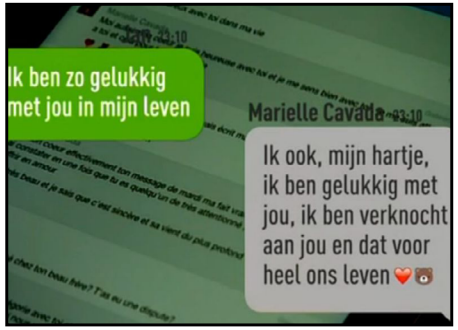
> Leer je iemand online kennen? Wees altijd op je hoede en ga niet blindelings in op de vraag om geld.

HULPVRAAGFRAUDE

Iemand stuurt je een bericht en doet zich voor als een bekende. De oplichter laat je geloven dat die persoon van nummer is veranderd. Met een smoes (verloren gsm, rekening geblokkeerd, ..) vraagt die je om geld over te schrijven.

Wat kan je doen om dit te voorkomen?

> Stel een persoonlijke vraag of bel die persoon op. Zo kan je de identiteit verifiëren.



VISHING

Je wordt gebeld door een persoon van bedrijf X (bank, helpdesk, kantoor, ...) die je vraagt om enkele handelingen uit te voeren of bankkaartgegevens door te geven. Hiermee probeert deze persoon je vertrouwelijke gegevens te verkrijgen of je geld te laten overschrijven.

Wat kan je doen om dit te voorkomen?

> Wantrouw telefoons van bedrijven die vertrouwelijke informatie of pincodes opvragen.
> Deel geen identiteits- en/of bankgegevens met onbekenden. Banken vragen namelijk nooit vertrouwelijke informatie of pincodes via e-mail/telefoon/sms.

HACKING ACCOUNT

Jouw account wordt gehackt waardoor er, zonder dat je het weet, berichten worden verstuurd naar je contactpersonen. Er kunnen ook berichten of foto's in jouw naam geplaatst worden.

Wat kan je doen om dit te voorkomen?

> Gebruik een sterk wachtwoord. Maak gebruik van een wachtwoordmanager en tweestapsverificatie.
> Gebruik voor elk account een ander wachtwoord en verander ze regelmatig.
> Deel je wachtwoorden nooit met iemand anders.
> Klik nooit zomaar op verdachte links en bijlagen.

VALS PROFIEL

Er wordt een vals profiel gemaakt met jouw identiteitsgegevens en/of persoonlijke afbeelding.

Wat kan je doen om dit te voorkomen?

> Gebruik een sterk wachtwoord. Hoe je een veilig wachtwoord kiest, kan je terugvinden op http://www.veilig-wachtwoord.be/nl.
> Verspreid geen persoonlijke gegevens via internet. Deel een wachtwoord nooit met derden. Geef geen identiteitsdocumenten aan derden.
> Let op met het verspreiden van persoonlijke gegevens via sociale media.

CYBERSTALKING & CYBERPESTEN

Je wordt herhaaldelijk via elektronische weg (sociale media, sms, e-mail, ...) bedreigd, vernederd of lastiggevallen.

Wat kan je doen om dit te voorkomen?

> Let op met het delen van persoonlijke gegevens met onbekenden. Scherm je account zo goed mogelijk af.
> Blijf steeds beleefd in je communicatie. Wees voorzichtig met het gebruik van webcams of video.
> Negeer vriendschapsverzoeken van onbekenden.

SEXTORTION & SEXTORTIONSCAM

Je wordt overtuigd om intieme beelden van jezelf door te sturen en daarna afgeperst voor geld of bitcoins om verspreiding te voorkomen.
Je ontvangt een bericht waarin oplichters beweren intieme beelden van jou te bezitten en geld of bitcoins vragen om ze niet te verspreiden.

Wat kan je doen om dit te voorkomen?

> Negeer vriendschapsverzoeken van onbekenden.
> Deel geen seksueel getinte foto's of video's van jezelf met onbekenden.
> Ga niet in op berichten waarin je wordt afgeperst (hacking/intieme beelden) en meldt ze bij de beheerder van het online platform.
> Scherm je webcam af.

RANSOMWARE

Je computer, mobiele apparaat of bestanden worden vergrendeld en er wordt losgeld gevraagd om ze terug te ontgrendelen.

Wat kan je doen om dit te voorkomen?

> Update regelmatig je software.
> Installeer antivirus- en firewallsoftware.
> Maak regelmatig een back-up van je bestanden.
> Meld verdachte e-mails of berichten van onbekende afzenders via verdacht@safeonweb.be en verwijder ze.

Je bent toch slachtoffer geworden... Wat nu?

Maak steeds melding of doe aangifte

Valse of verdachte personen/organisaties kan je melden via **https://meldpunt.belgie.be**. Kies het thema dat van toepassing is en doorloop de verschillende stappen om de melding te maken.

Stuur verdachte mails of screenshots van verdachte berichten naar **verdacht@safeonweb.be**. Het Centrum voor Cybersecurity België (CCB) onderzoekt en blokkeert frauduleuze links.

Konden de oplichters je bankgegevens bemachtigen? Blokkeer dan onmiddellijk je betaalkaarten via **Cardstop** (078/170 170). Neem ook **contact** op **met je bank**. Cardstop blokkeert namelijk niet de toegang tot je bankapp. Als er al transacties gebeurd zijn, kan je bank ze misschien nog onderscheppen.

Is er effectief geld verdwenen en heb je dus financieel nadeel? **Neem** dan zo snel mogelijk **contact op** met de politie via het nummer **053/73 27 27**.

Werd je account **gehackt**? **Licht je vrienden in** dat ze mogelijks verdachte berichten kunnen ontvangen en daar niet op mogen ingaan. Vraag aan zoveel mogelijk vrienden om het profiel te **rapporteren**. Voor Facebook kan je gebruik maken van de link https://facebook.com/hacked.

Politie Aalst

Wil je meer informatie? Surf naar onze website voor nuttige links en tips om online criminaliteit te voorkomen.

Heb je vragen rond internetcriminaliteit? Neem dan contact op met onze dienst Preventie via PZ.Aalst.Preventie@police.belgium.eu.

Beekveldstraat 29
9300 Aalst

053 73 27 27
PZ.Aalst@police.belgium.eu

www.politieaalst.be
/PolitieAalst

Child Focus 116000

Stad Aalst