Politie
Aalst

Online criminaliteit - slachtoffer

Je bent slachtoffer van internetcriminelen. Wat nu gedaan?
In deze folder vind je de meest voorkomende vormen van internetcriminaliteit en wat je kan doen als jou dat overkomen is.

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.

In deze folder vind je een aantal van de meest voorkomende vormen van online criminaliteit. De folder geeft je ook een paar tips die je kan volgen als je slachtoffer werd.

Je bent slachtoffer... Wat kan je doen?

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.

OPLICHTING VIA INTERNET - PHISHING - SMISHING

Je ontvangt een e-mail of een bericht (sms, WhatsApp of een 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?

> Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
> Bel onmiddellijk Cardstop: 078/170 170.
> Werd je opgelicht via een zoekertjessite? Contacteer dan de helpdesk.
> Maak melding op: https://meldpunt.belgie.be of stuur door naar verdacht@safeonweb.be.
> Dien eventueel klacht in. Verzamel hiervoor zoveel mogelijk bewijs.


ING

Veiligheidsupdate Home Banking / ING
Brussel - 30-08-2012

Sinds woensdag 29 augustus 2012 werken wij met een nieuw beveiligingssysteem. Dit nieuwe systeem
misbruik kan worden gemaakt van uw rekening door bijvoorbeeld kwaadwillende software of een virus da
heeft geïnstalleerd.

Om ervoor te zorgen dat ook uw rekening wordt beveiligd door ons nieuw systeem, verzoeken wij u hierc
hyperlink te volgen om vervolgens uw gegevens te verifiëren. Zodra u dit heeft gedaan, zal uw rekening
nieuwe beveiligingssoftware.

Klik hier om uw gegevens te verifiëren


U ontvangt een terugbetaling van €89,74. Bevestig uw bankrekening om de terugbetaling te ontvangen: https://fiinancies-belgium.net/be/ontvangen/terugbetaling

7 nov. 14:50

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?

> Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
> Bel onmiddellijk Cardstop: 078/170 170.
> Maak melding op: https://meldpunt.belgie.be of stuur door naar verdacht@safeonweb.be.
> Dien eventueel klacht in. Verzamel hiervoor zoveel mogelijk bewijs.

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?

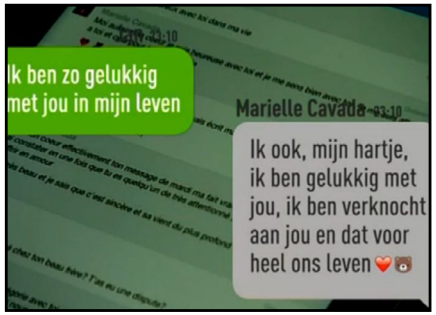
> Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
> Bel onmiddellijk Cardstop: 078/170 170.
> Maak melding op: https://meldpunt.belgie.be of stuur door naar verdacht@safeonweb.be.
> Dien eventueel klacht in. Verzamel hiervoor zoveel mogelijk bewijs.

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?

> Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
> Bel onmiddellijk Cardstop: 078/170 170.
> Probeer een terugbetaling te bekomen bij je bank.
> Maak melding op: https://meldpunt.belgie.be of stuur door naar verdacht@safeonweb.be.
> Dien eventueel klacht in. Verzamel hiervoor zoveel mogelijk bewijs.



ONLINE SHOPPING FRAUDE

Via een (valse) webshop of advertentie kom je in contact met een oplichter die iets verkoopt aan een (abnormaal) lage prijs. Zodra de betaling in orde is, hoor je niets meer van de verkoper.

Wat kan je doen?

> Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
> Bel onmiddellijk Cardstop: 078/170 170.
> Maak melding op: https://meldpunt.belgie.be of stuur door naar verdacht@safeonweb.be.
> Rapporteer de fraude bij de (vervalste) website.

HACKING ACCOUNT

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

Wat kan je doen?

> Verander onmiddellijk je wachtwoord als je nog toegang hebt tot je account.
> Contacteer de helpdesk van de website zelf indien je geen toegang meer hebt.
> Laat je contactpersonen weten dat jij deze berichten niet hebt gestuurd.
> Koppel je computer of apparaat los van het internet.
> Laat zoveel mogelijk vrienden het account rapporteren.

NEEM CONTACT OP

Ben je slachtoffer van online criminelen?

Neem dan zo snel mogelijk contact op met de politie via het nummer 053/73 27 27.

VALS PROFIEL

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

Wat kan je doen?

> Contacteer de beheerder van de website en rapporteer het misbruik.
> Bewaar zoveel mogelijk bewijs.
> Licht vrienden in dat ze mogelijks verdachte berichten kunnen ontvangen en daar niet op mogen ingaan.

CYBERSTALKING & CYBERPESTEN

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

Wat kan je doen?

> Bewaar zoveel mogelijk bewijsmateriaal (schermafdrukken, accountnaam, e-mailberichte, mailheaders, ...).
> Maak melding bij de beheerder van de website.
> Leg klacht neer bij de politie.

SEXTORTION & SEXTORTIONSCAM

Je werd overtuigd om intieme beelden van jezelf door te sturen en wordt nu 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?

> Ga niet in op de vraag om te betalen.
> Antwoord niet op het bericht.
> Bewaar zoveel mogelijk bewijsmateriaal (berichten, schermafdrukken, ...).
> Markeer het bericht als spam of ongewenst.
> Blokkeer de afzender.

RANSOMWARE

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

Wat kan je doen?

> Koppel je computer of apparaat los van het internet.
> Koppel alle andere toestellen los (USB, externe harde schijf, ...).
> Bewaar zoveel mogelijk bewijsmateriaal (berichten, schermafdrukken, ...).
> Ga niet in op de vraag om te betalen.
> Zoek gratis decryptiesleutels op https://www.nomoreransom.org of laat je toestel opnieuw installeren.

Tips om je in de toekomst te beschermen

Om jezelf te beschermen in de toekomst, hou je best de 3 T's in je achterhoofd: Te mooi, Twijfel en Training. Meer info hierover vind je in de brochure Online criminaliteit - preventie.

> Klik niet zomaar op een link die je ontvangt via e-mail, sms of sociale media. Probeer na te gaan of je de afzender kent.

> Banken of overheidsbedrijven vragen nooit vertrouwelijke gegevens online of via de telefoon. Bij twijfel neem je best zelf contact op met de organisatie van wie het bericht zogezegd afkomstig is.

> Doe alleen online betalingen via beveiligde websites (zoek het hangsloticoon 🔒 en 'https' in de URL-balk) en via een beveiligde internetverbinding. Wees voorzichtig met welke gegevens je ingeeft op een openbaar netwerk.

> Twijfel je aan een bericht of aan degene die je opbelt? Neem contact op met de persoon/het bedrijf van wie het bericht afkomstig zou zijn.

> Wees voorzichtig met de persoonlijke info of foto's die je deelt via sociale media. Deze gegevens liggen voor oplichters voor het grijpen en kunnen hen helpen om jou in de val te lokken.

> Maak voor al je accounts gebruik van tweestapsverificatie.

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