Ransomware

Je computer, mobiele apparaten of digitale bestanden zijn vergrendeld en er wordt losgeld gevraagd om deze terug te krijgen.

Wat te doen?

- Verbreek de verbinding met het internet (wifi of internetkabel).
- Koppel onmiddellijk alle andere toestellen los, zoals een externe harde schijf of een USB-stick.
- Als je toestel helemaal geblokkeerd is en er wordt losgeld gevraagd, zoek dan op www.nomoreransom.org of de sleutel voor deze ransomware beschikbaar is.
- Laat je toestel helemaal opnieuw installeren en gebruik achteraf een back-up of reservekopie om je gegevens terug te zetten.
- Betaal niet: je hebt geen enkele garantie dat je effectief op een veilige manier je gegevens terugkrijgt.

Hoe voorkomen?

- Gebruik anti-ransomwaresoftware.
- Doe regelmatig updates.
- Scan je computer regelmatig met een anti-virussoftware.
- Leer valse berichten (phishing) herkennen.

Hulpvraagfraude en vriendschapsfraude

Iemand die je kent of iemand die je hebt leren kennen op het internet vraagt geld.

Wat te doen?

- Contacteer het familielid of kennis via een ander kanaal om te horen of de hulpvraag van hem of haar komt.
- Maak geen geld over aan mensen die je online hebt leren kennen of familieleden die 'plots' een ander rekeningnummer hebben.
- Verbreek elk contact met de fraudeur.

Hoe voorkomen?

- Negeer vriendschapsverzoeken van onbekenden.
- Deel geen seksueel getinte foto's of video's.

Phishing

Phishing is online oplichting door valse e-mails, websites of berichten. Cybercriminelen proberen misbruik te maken van je vertrouwen. Ze proberen in te spelen op emoties zoals verlangen en angst.

Wat te doen?

- Als je een wachtwoord hebt doorgegeven dat je ook op andere plaatsen gebruikt, verander het dan onmiddellijk.
- Als je op een link heb geklikt die opent in een website waar je bankgegevens moet indienen, controleer dan eerst of dit de echte website van je bank is. Bij de minste twijfel voer je geen betaling in.
- Als je iets hebt gedownload, verwijder het dan en voer een anti-virusscan uit.

Hoe voorkomen?

- Leer verdachte berichten herkennen.
- Denk twee keer na voor je klikt
- Download enkel applicaties uit een officiële app store

Account hack

Een account hack gebeurt wanneer een hacker toegang heeft tot de logingegevens van een online account. De hacker kan in jouw naam berichten posten of je contacten contacteren.

Wat te doen?

- Heb je nog toegang? Verander je wachtwoord (ook in andere accounts waar je dat wachtwoord gebruikt) en verwittig je contacten.
- Heb je geen toegang meer? Gebruik de herstelopties om opnieuw toegang te krijgen en verander daarna al je wachtwoorden.

Hoe voorkomen?

- Activeer tweestapsverificatie.
- Gebruik voor elk account een ander (sterk) wachtwoord en bewaar het in een wachtwoordkluis.
- Deel je wachtwoorden nooit met anderen.

Tech Scam

Je wordt opgebeld via de vaste lijn door iemand die zich voordoet als medewerker van een ICT bedrijf (Microsoft, Apple, je ICT dienst). De oplichter zegt dat er een veiligheidsprobleem is met je computer en stelt voor om te helpen.

Hoe voorkomen?

- Wantrouw altijd telefoonoproepen van bedrijven die vragen om een acties uit te voeren op je computer.
- Laat je computer nooit overnemen door iemand die je niet kent.
- Voer geen betalingen uit terwijl een onbekende de computer heeft overgenomen.

CEO-fraude

CEO-fraude is een vorm van oplichting waarbij cybercriminelen een onderneming contacteren met de vraag een betaling uit te voeren. De cybercriminelen nemen de identiteit aan van de CEO, CFO of een vertrouwde persoon en vragen een medewerker van de financiële dienst of boekhouding om een dringende betaling uit te voeren.

Hoe voorkomen?

- Medewerkers goed informeren en waarschuwen voor deze manier van handelen.
- De boekhoudkundige dienst hanteert duidelijke procedures en afspraken voor betalingen.

Sextortion scam

Je krijgt een e-mail waarin afpersers bluffen dat ze je computer hebben gehackt en intieme beelden van je hebben gemaakt. De afpersers dreigen ermee om de beelden te verspreiden op het internet tenzij je een bedrag betaalt.

Wat te doen?

- Ga niet in op de vraag om een som geld te betalen.
- Verwijder het bericht.
- Markeer het bericht als spam of ongewenst.
- Blokkeer de afzender.

Wie contacteren na een cyberaanval of online oplichting?

Politie

Als je geld kwijt bent of afgeperst wordt, raden wij aan om een aangifte te doen bij de politie. Een aangifte doe je bij de lokale politie van je woonplaats.

Het is belangrijk om zoveel mogelijk informatie mee te nemen naar het politiekantoor. Hieronder vind je een lijst van informatie die je vooraf kan verzamelen:

- Is er geld van je rekening verdwenen? Neem de bankafschriften mee.
- Heb je contact gehad met iemand op sociale media ? Neem een schermafdruk mee van het profiel van de verdachte en enkele schermafdrukken van gesprekken die gevoerd zijn.
- Heb je een valse website geopend die bv. lijkt op die van je bank of een andere instelling? Maak een schermafdruk en neem deze mee voor je aangifte.
- Ben je opgelicht via een online verkoopsite? Neem een schermafdruk mee van het zoekertje of de aanbieding waarop je gereageerd hebt, en een schermafdruk van het profiel van de oplichter.
- Heb je een e-mail ontvangen van de oplichter? Bewaar het bericht en druk het af.

Je bank en Cardstop

Contacteer je bank en Cardstop op 078 170 170 als je bankgegevens hebt doorgeven, er geld van je bankrekening verdwijnt of als je geld hebt overgemaakt aan een oplichter.

Op die manier kunnen eventuele frauduleuze transacties geblokkeerd worden.
Wil je fraude melden, dan kan je bij je bank terecht op een speciaal nummer:
https://beschermjezelfonline.be/bank-contacteren-voor-hulp

Safeonweb

Heb je een verdachte e-mail of een verdacht bericht ontvangen?

Stuur het door naar verdacht@safeonweb.be en verwijder het daarna. Je krijgt geen persoonlijk antwoord. De links in het bericht worden geblokkeerd waardoor minder oplettende internetgebruikers geen slachtoffer kunnen worden. Als je een verdacht bericht op het werk ontvangt, moet je de procedures die daar gelden voor phishing opvolgen, bv. doorsturen naar de ICT-dienst.

Meldpunt

Ben je slachtoffer van misleiding, bedrog, fraude, oplichting?

Doe dan een melding via https://meldpunt.belgie.be van de FOD Economie. Je krijgt steeds een advies op het einde van je melding. De bevoegde diensten analyseren de melding en stellen mogelijk een onderzoek in.

Centrum voor Cybersecurity België

Als je organisatie geconfronteerd wordt met een cyberaanval of het slachtoffer is van een ransomware en dit wil melden of in alle vertrouwen advies wil vragen, kan dit bij CERT.be, het Federale Cyber Emergency Respons Team van het CCB via https://www.cert.be

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Cyberaanvallen en online oplichting

Wat is het, wat moet je doen en hoe voorkomen?

Safeonweb.be