# 2-4-2024 echt niet vandaag!

Digitale criminaliteit kent vele vormen en helaas vele slachtoffers. Dagelijks weten gewiekste criminelen veel geld buit te maken door bedrijven op te lichten of door burgers te misleiden of bedrijven op te lichten. Dat moet stoppen! Door op één dag de handen ineen te slaan, hopen heel veel organisaties in Gelderland en Overijssel slachtoffers te voorkomen en bewustwording te vergroten.

## Echt niet vandaag!

*Echt niet vandaag* is een campagne tegen digitale criminaliteit. Politie, Centrum voor Digitalisering en Veiligheid (CVD), Platform Veilig Ondernemen (PVO) en Veiligheidsnetwerk Oost-Nederland willen op 2-4-2024 één dag samen bewustwording creëren en slachtoffers weerbaar maken! Deze dag vinden er tientallen acties plaats in Gelderland én Overijssel. Denk aan agenten die voorlichting geven, bibliotheken die extra digitale hulp aan bieden en ICT-bedrijven die extra aandacht vragen voor beveiliging van bedrijfsgegevens.

## Nodig

De cijfers liegen er niet om. Dagelijks zijn er slachtoffers, zowel bij bedrijven als onder burgers.

* Dagelijks tientallen slachtoffers in Gelderland en Overijssel. In Oost-Nederland melden zich dagelijks gemiddeld 23 slachtoffers bij de politie. (bron: politie)
* Jaarlijks miljoenen slachtoffers in Nederland. Landelijk waren er in 2022 2,2 miljoen Nederlanders

slachtoffer van digitale criminaliteit. Dat zijn gemiddeld 6.000 slachtoffers per dag! (bron:CBS)

* Miljoenen euro’s winst voor criminelen
* Bedrijven worden in 95% van de gevallen slachtoffer van digitale criminaliteit door menselijke fouten.

Bij digitale criminaliteit speelt schaamte een grote rol. ‘Hoe kon ik zo stom zijn’, is een veel gehoorde uitspraak. Maar ook bedrijven schamen zich en zijn bang voor reputatieschade na een ransomeware-aanval, zij betalen liever het geëiste losgeld in plaats van het doen van aangifte.

* Slechts 2 op de 10 slachtoffers doet melding en aangifte van digitale criminaliteit (bron: CBS)
* Slechts 1% van de bedrijven doet aangifte. (bron: CBS)
* 37% van de mensen heeft na een online oplichting minder vertrouwen in mensen. (bron: CBS)
* Eén derde voelt zich zelfs minder veilig. (bron: CBS)

## 2-4-2024

Eén dag samen aandacht vragen voor de problematiek! Met de campagne *Echt niet vandaag*, willen de deelnemende organisaties samen optrekken en op veel verschillende manieren aandacht vragen. Maar met één dag alleen red je het niet. De hoop is dat iedereen ook na 2 april vol blijft inzetten op preventie en hulp. Naast de deelnemende organisaties kan iedereen zich aansluiten bij de beweging. Op echtnietvandaag.nl kunnen acties, groot en klein, aangemeld worden. Halverwege maart is op de site zichtbaar welke acties er in de provincies opgestart worden.

## Fenomenen

Digitale criminaliteit kent verschillende vormen. De lijst aan fenomenen wordt alsmaar langer.

Burgers worden vooral slachtoffer van:

* [Bankhelpdeskfraude](#_Bankhelpdeskfraude)
* [Sextortion](#_Sextortion)
* [Vriend-in-Noodfraude](#_Vriend-in-noodfraude)
* [Boilerroomfraude](#_Boilerroomfraude)
* [Phishing](#_Phishing)

Bedrijven zijn vooral slachtoffer van:

* [Phishing](#_Phishing)
* [Ransomeware](#_Ransomeware)
* [Datalek](#_Datalek)

In het kort de fenomenen en tips om te voorkomen dat je slachtoffer wordt.

## Bankhelpdeskfraude

Bij bankhelpdeskfraude doet een oplichter zich voor als bankmedewerker. In veel gevallen wordt gezegd dat het geld op een betaalrekening gevaar loopt en snel veiliggesteld moet worden. Dat kan door de pinpas mee te geven aan een bankmedewerker. Om vertrouwen te wekken, wordt vaak een code door gegeven die alleen bekend is bij de bankmedewerker die langskomt. Alles bij elkaar klopt er niets van! Door druk te zetten en vertrouwen te wekken, weten oplichters gemakkelijk veel slachtoffers te maken. Trap er niet in! Een bank vraagt niet geld over te maken op een andere rekening en ook het bankpasje wordt thuis nooit opgehaald.

## Sextortion

Een sexy foto sturen is spannend en natuurlijk niet strafbaar. Als de foto in verkeerde handen komt, kan er wel misbruik van worden gemaakt. Als er gedreigd wordt beelden online te zetten als er niet meer materiaal gestuurd wordt of geld, spreken we van sextortion. Dit kun je doen om dat te voorkomen:

* Laat je niet verleiden foto’s van jezelf te sturen naar mensen die je niet echt goed kent
* Wil je toch een foto sturen, zorg dan dat je er niet herkenbaar op staat.

Toch slachtoffer? Dit zijn wat tips:

* Ga niet in op chantage geld of meer beelden te delen. Dit is geen garantie dat de chantage stopt! Vaak is het het begin van meer dreiging.
* Neem contact op met de politie, misschien spannend, maar we kunnen je wel helpen! Vind de chantage nu plaats, bel dan direct 112. Agenten komen dan direct bij je langs om je te helpen.
* Zorg voor een goede beveiliging van je accounts
* Praat erover met iemand die je vertrouwt

## Vriend-in-noodfraude

‘Hoi pap, …’ Bij vriend-in-nood fraude neemt een ‘bekende’ contact op met het slachtoffer. Met een smoes over de telefoon die niet meer werkt, gevolgd door een verzoek om snel geld over te maken, worden veel slachtoffers gemaakt. Vaak is die bekende een familielid of een vriend van het slachtoffer. In werkelijkheid is het een crimineel die zich voordoet als familielid/ vriend.

Het slachtoffer wordt direct gevraagd om één of meerdere rekeningen te betalen omdat de bekende snel hulp nodig heeft en zelf niet in staat is om te betalen, bijvoorbeeld omdat degene zelf even niet bij de bankrekening kan. Het advies: neem contact op met het familielid/de bekende om te checken of het verhaal klopt. Toch opgelicht? Bel direct de politie.

## Boilerroomfraude

Criminelen benaderen mensen om een klein bedrag te investeren waar een hoge rente op zit. Hun geld kan snel nog meer waard worden door te investeren in (crypto)valuta. Om vertrouwen te winnen hoeven slachtoffers in het begin maar een klein bedrag in te leggen. Op een persoonlijke website zijn al snel de winsten te zien. Eenmaal gevangen in het web van de crimineel wordt er om meer geld gevraagd. Als de winsten maar blijven stijgen en het slachtoffer het geld wil laten uitbetalen blijkt alles gebakken lucht te zijn. Het geld is weg en met de crimineel is geen contact meer te krijgen. Slachtoffers van boilerroomfraude zijn vaak tonnen kwijt!

## Phishing

Het vissen naar gegevens wordt phishing genoemd. Een link in een e-mail, sms, of via bijvoorbeeld WhatsApp komt uit bij een inlogwebsite van bijvoorbeeld een bank of een andere inlogpagina. Na het invoeren van wat inloggegevens blijkt de site niet te werken. Je bent slachtoffer geworden van phishing. Dit komt zowel bij burgers als bedrijven voor. De inlogwebsite van de link waar je op hebt geklikt, is een perfect nagebouwde website die niet van een bank of andere instantie te onderscheiden is. In feite is het een nagebouwde website gemaakt door iemand met als doel om achter inloggegevens te komen en deze uiteindelijk te misbruiken. Het kan zijn dat er daadwerkelijk al geld van de rekening is afgeschreven. Het kan ook zo zijn dat dit nog niet is gebeurd, maar de inloggegevens wel bekend zijn bij de andere partij.

## Ransomeware

Bij ransomeware kunnen cybercriminelen op verschillende manieren toegang krijgen tot bestanden van bedrijven. Dat kan door een ‘foute’ link of via een bijlage in een mail. Eenmaal binnen kunnen de criminelen gegevens ‘gijzelen’. Om weer toegang te krijgen tot de gegevens of de systemen wordt geld geëist. Vaak in de vorm van bitcoins. Wist je dat één op de vijf bedrijven in Nederland naar eigen zeggen niet goed beveiligd is? Dat kan *echt niet*!

## Datalek

Als criminelen door een ‘lek’ in het systeem van een bedrijf beschikking krijgt over heel veel data, noemen we dat een datalek. Met name persoonsgegevens van klanten zijn een goudmijn voor cybercriminelen. Met die data kunnen criminelen heel gericht zoeken naar potentiële slachtoffers. Bij bankhelpdeskfraude zijn vooral ouderen het slachtoffer. Lijsten met persoonsgegevens waarop geboortedata staan, zijn gemakkelijk te filteren in een doelgroep geboren tussen 1945-1955. Op die manier kan een crimineel heel gericht toeslaan en gemakkelijk vele slachtoffers maken.

De omvang van online criminaliteit is gigantisch en groeit met de dag! Sluit aan bij 2-4-2024 en kom in actie! Alle acties zijn welkom. Kijk jij die dag naar je eigen online veiligheid of sta met je collega’s stil hoe ieders online veiligheid is. Of ga de boer op om mensen bewust te maken van de online gevaren.

## Meer weten

*Echt niet vandaag* is een initiatief van Politie Oost-Nederland, Centrum voor Digitalisering en Veiligheid (CVD), Platform Veilig Ondernemen (PVO) en Veiligheidsnetwerk Oost-Nederland. Meer informatie over de campagne en de verschillende acties is te vinden op [*echtnietvandaag.nl*](https://www.echtnietvandaag.nl/).