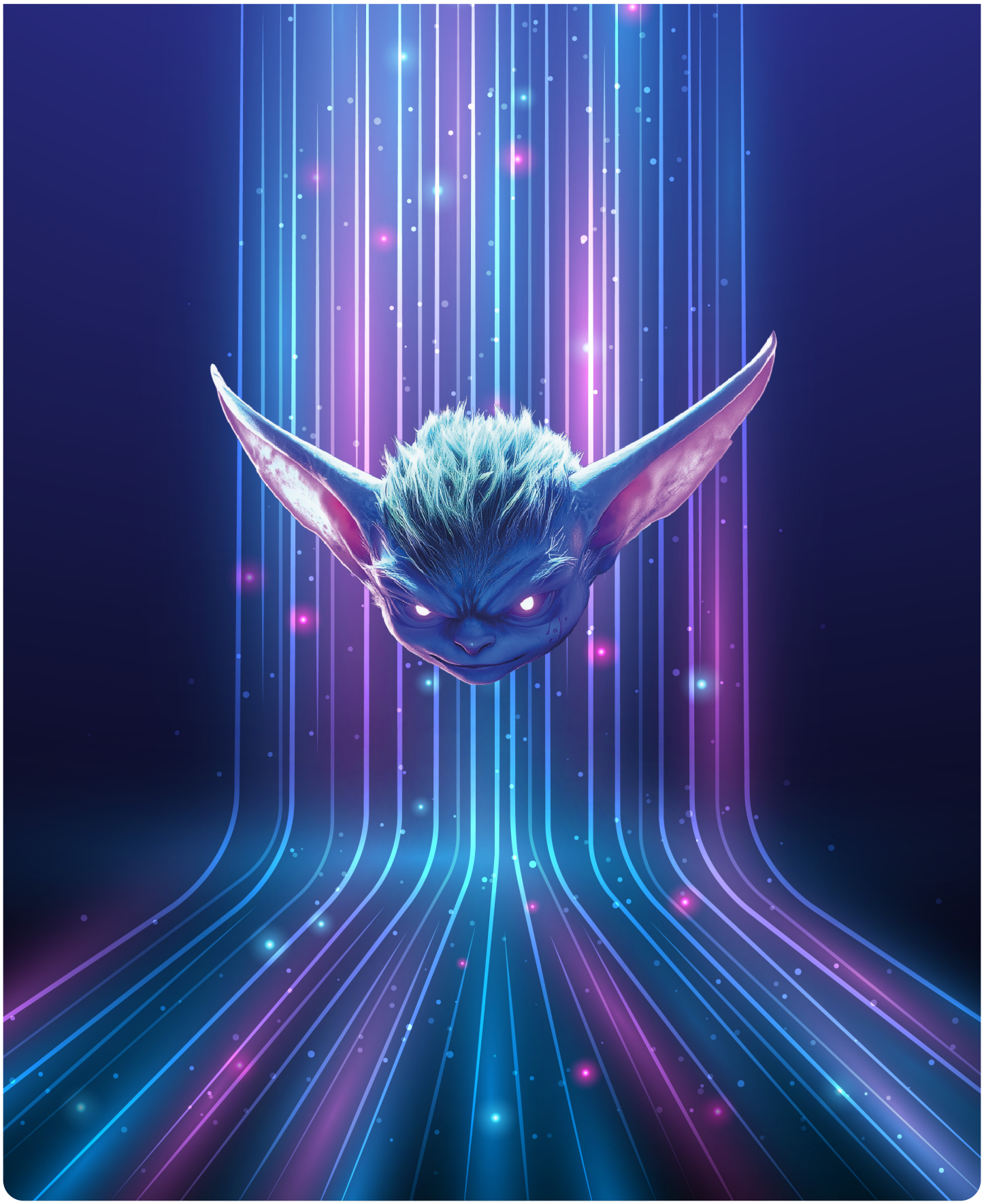
SCHOLENWORKSHOP: CYBER(S)PIONNEN

WORKSHOP CYBER COMMAND x TECHNOPOLIS - 1STE GRAAD SECUNDAIR ONDERWIJS



EXTRA INFORMATIE: CYBERCRIMINALITEIT

Wat houdt cybercriminaliteit precies in?

Cybercriminaliteit is een verzamelnaam voor misdrijven die plaatsvinden online, met als doel persoonlijke gegevens te verkrijgen, geld te bemachtigen, of schade toe te brengen aan andere mediagebruikers. Het kan zowel gaan om misdrijven tegen bedrijven, organisaties of individuele personen.

Waarom plegen mensen cybercriminaliteit?

Cybercriminalietiet ontstaat hoofzalelijk voor *finacieel gewin*, maar kan ook ingegeven zijn door *politieke motieven* of uit *persoonlijke redenen*.

- *Financieel Gewin*
  Een oplichter stuurt een e-mail die lijkt te komen van je bank. In het bericht staat dat er "onregelmatigheden" zijn op je persoonlijke rekening en dat je snel moet inloggen via onderstaande link. Die link leidt naar een valse website waar je je bankgegevens invult. De oplichter gebruikt vervolgens deze gegevens om geld van je rekening te halen.
- *Politieke Motieven*
  Hackers dringen tijdens verkiezingstijd binnen in de servers van een oppositiepartij. Ze stelen vertrouwelijke documenten en lekken die naar de pers om de partij schade te berokkenen en stemmenverlies te veroorzaken.
- *Persoonlijke Redenen*
  Na een ruzie hackt een tiener het Instagramaccount van een klasgenoot. Hij plaatst gênante foto's en beledigende berichten om die persoon publiekelijk belachelijk te maken.

Hoe herken je cybercriminaliteit?

Opzich kan iederéén slachtofer worden van cybercriminaliteit. In meeste gevallen gebeurt het via verdachte e-mails, sms of whats-app berichten. Let vooral op volgende waarschuwingssignalen:

- Het bericht bevat vreemd taalgebruik en/of spelfouten (Let wel: niet altijd het geval).
- De afzender doet zich voor als een bekende persoon of organisatie, zoals je bank of de overheid.
- Er wordt gevraagd om vertrouwelijke gegevens en/of informatie te delen.
- Er is tijdsdruk, waardoor je snel moet handelen.
- Er staat een link in waarop je moet klikken.
- Er wordt beweerd dat je geld tegoed hebt of een prijs hebt gewonnen.
- Er wordt gevraagd om een betaling te doen.

Welke soorten cybercriminalitait bestaan er allemaal?

Door de immer snelle vooruitgang van technologie en innovatie wordt ons leven makkelijker, maar ook het werkterrein van cybercriminelen wordt groter. Ze vinden telkens nieuwe manieren en technieken om mensen en organisaties om de tuin te leiden. Toch zijn er een aantal vormen die het vaakst voorkomen:

- *Phishing*

  Oplichters sturen online valse berichten die lijken te komen van een vertrouwde organisatie om persoonlijke (bank) gegevens te ontfutselen. Ze 'vissen' naar je gegevens.
- *Ransomware*

  Kwaadaardige software die je computer of bestanden vergrendelt. Je krijgt pas terug toegang na het betalen van losgeld.
- *Factuurfraude*

  Echte facturen worden onderschept en aangepast, meestal met een nieuw rekeningnummer dat naar de oplichters leidt.
- *Hulpvraagfraude*

  Criminelen doen zich voor als een vriend of familielid met een nieuw telefoonnummer en vragen dringend om geld.
- *Hacking*

  Het ongeoorloofd binnendringen in computersystemen of accounts om informatie te stelen, te wijzigen of te vernietigen.
- *Geldezelpraktijken*

  Jongeren of volwassenen laten hun bankrekening gebruiken om illegaal geld door te sluizen in ruil voor een vergoeding, vaak zonder te beseffen dat dit strafbaar is.