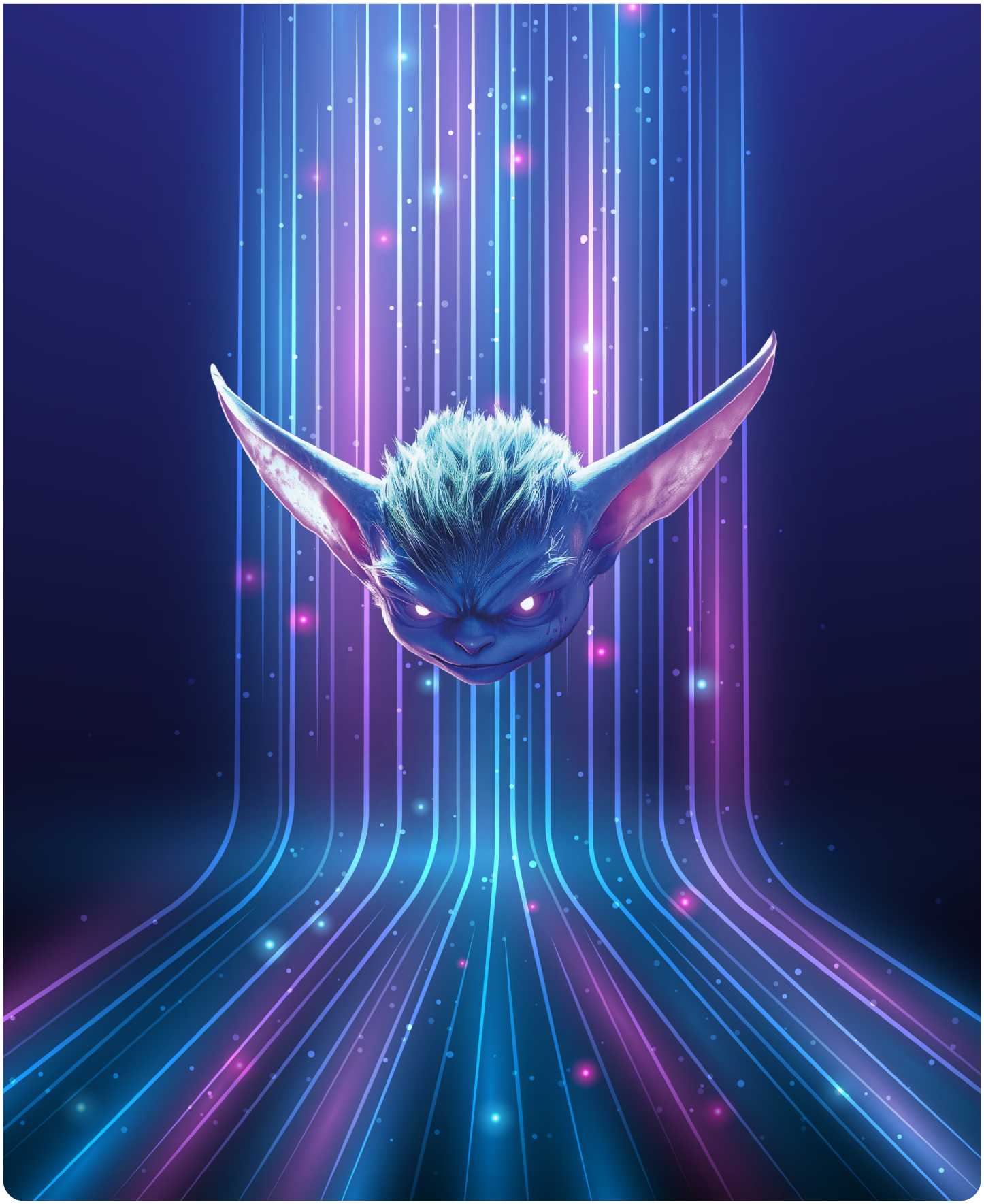
SCHOLENWORKSHOP: CYBER(S)PIONNEN

WORKSHOP CYBER COMMAND x TECHNOPOLIS - 1STE GRAAD SECUNDAIR ONDERWIJS



EXTRA INFORMATIE: PHISHING

Wat houdt phishing precies in?

Phishing is één van de meest voorkomende internetoplichting waarbij criminelen proberen persoonlijke informatie, zoals wachtwoorden, bankgegevens en identiteitsgegevens, te bemachtigen. Dit doen ze door zich voor te doen als betrouwbare organisaties zoals banken, webshops of overheidsinstanties. Met deze gestolen gegevens kunnen ze geld van je rekening halen, aankopen doen of zelfs je identiteit misbruiken.

Waarom is phishing een belangrijk aandachtspunt voor jongeren?

Veel jongeren zijn elke dag online actief. Ze chatten, spelen games, doen aankopen of regelen hun bankzaken via internet. Door hun intensieve online aanwezigheid zijn jongeren aantrekkelijk voor cybercriminelen. Hoewel jongeren vaak denken dat ze veilig zijn, lopen ze vaker risico slachtoffer te worden omdat ze de gevaren net onderschatten.

Volgens onderzoek van Febelfin (2023) werd 12% van de jongeren in België slachtoffer van phishing, wat hoger ligt dan het gemiddelde bij volwassenen. Dit komt doordat jongeren vaak minder ervaring hebben met online fraude en sneller reageren onder druk. Bovendien worden phishing-technieken steeds geavanceerder, waardoor het moeilijker is om ze te herkennen. Daarom is het essentieel dat jongeren leren hoe ze phishing-berichten kunnen herkennen en voorkomen.

Hoe herken je phishing?

Phishingberichten kun je ontvangen via e-mail, sms, whatsapp, sociale media, telefoonoproepen, … Deze berichten zien er vaak heel geloofwaardig uit en lijken afkomstig te zijn van bekende instanties. Er wordt meestal gevraagd om een actie uit te voeren, zoals het klikken op een link of het invullen van gegevens op een website. Phishing-berichten zetten vaak druk op jou, bijvoorbeeld door te melden dat je account zal worden geblokkeerd als je niet snel reageert.

Tips om phishing effectief te herkennen:

- Controleer zorgvuldig de afzender en URL (websiteadres) voordat je persoonlijke gegevens invult. Kleine foutjes kunnen wijzen op fraude.
- Wees kritisch bij onverwachte berichten die vragen om snel te reageren of persoonlijke informatie te delen.
- Let op vreemde taal, taalfouten en onprofessionele vormgeving.
- Klik nooit zomaar op links in onverwachte berichten. Controleer altijd zelf via de officiële website of het bericht authentiek is.

Praktische voorbeelden van phishing-berichten:

- Een bericht waarin staat dat je bankrekening wordt geblokkeerd tenzij je onmiddellijk via een link jouw gegevens controleert.
- Een e-mail van een zogenaamd betrouwbare webshop met een tijdelijke kortingsactie, waarvoor je via een verdachte link gegevens moet invoeren.
- Een WhatsApp-bericht van iemand die zich voordoet als een familielid en dringend financiële hulp vraagt.
- Een sms waarin wordt beweerd dat je een prijs hebt gewonnen en persoonlijke gegevens moet verstrekken om deze prijs te kunnen claimen.