

HackShield: Ga toch vissen!

Tijdens deze les gaan de studenten ervaren hoe cybercriminelen via phishingmails, sms-berichten en whatsappberichten persoonlijke gegevens in handen proberen te krijgen. Ook leren de studenten hoe ze phishingberichten kunnen herkennen en hoe ze zichzelf hiertegen kunnen beschermen. Uiteindelijk bedenken en maken ze een tutorial waarmee ze het onderwerp phishing concreet maken voor hun (stage-) praktijk. Deze Digi-doener voor de pabo is een remake van een les uit de lessenserie HackShield over cybercriminaliteit. De student zou deze lessenserie in de (stage)praktijk kunnen geven. Deze les kan gegeven worden in een les over technologie en digitale media op de pabo. Totale duur: 1,5 (tot 2*) uur.

* Optioneel:

Er kan gekozen worden voor het splitsen van de les. In de eerste les wordt dan aandacht besteed aan de theorie en verdieping achter phishing, de opdracht wordt uitgelegd en meegegeven voor de volgende les. In de tweede les worden de tutorials bekeken en beoordeeld. Maak hier vooraf zelf een keuze in.

VERBINDING MET HET ONDERWIJS

De studenten (en later hun leerlingen) kunnen op vele manieren te maken krijgen met cybercriminaliteit. Wachtwoorden, accounts en andere belangrijke gegevens zijn voor cybercriminelen goud waard. Soms is het kinderlijk eenvoudig voor deze criminelen om belangrijke gegevens te achterhalen, met alle gevolgen van dien. Phishing is hier een bekend (en berucht) voorbeeld van. Het sturen van neppe bank- en zelfs whatsappberichten om gegevens te kunnen achterhalen komt steeds vaker voor. Door corona zijn we steeds meer thuis en regelen we ook belangrijke zaken meer vanuit huis. Voor cybercriminelen is dit de ideale situatie om te proberen om belangrijke gegevens te achterhalen. Het is daarom van belang dat vaardigheden zoals het herkennen van phishingmailtjes worden aangeleerd. De studenten van nu voeden de digitale burgers van de toekomst op en ook zij zullen met phishing te maken krijgen. Het is daarom belangrijk dat studenten leren hoe ze hun toekomstige leerlingen bewust en bekwaam kunnen maken in hoe ze hiermee omgaan. De student moet leren welke kansen en gevaren er liggen bij het onderwerp phishing, maar moet het ook concreet kunnen maken voor de (stage)praktijk.

LESOPBOUW

- Introductie: De studenten leren wat phishing betekent en wat het inhoudt.
- Verdieping: De studenten leren hoe phishing in zijn werk gaat en bespreken het ethisch dilemma.
- Doen: De studenten ontwerpen een tutorial rondom phishing.
- Afronding: De studenten bekijken elkaars lesvideo en beoordelen de bruikbaarheid ervan voor hun (stage)praktijk.

ETHIEK EN TECHNOLOGIE

Phishing valt onder cybercriminaliteit en is een vorm van digitale oplichting. Slachtoffers zijn naar een valse website gelokt en hebben vervolgens hun bankgegevens of andere inloggegevens prijsgegeven. Maar wie is nu verantwoordelijk voor de schade die dit oplevert? Het slachtoffer heeft er immers zelf voor gekozen om bepaalde gegevens door te geven aan de crimineel. De cybercrimineel is in vele gevallen niet meer te achterhalen. Maar wie herstelt de schade? Had het slachtoffer zich niet beter moeten laten informeren over cybercriminaliteit en hoe je dit kunt herkennen? Of had het bedrijf achter de banksoftware zijn klant beter moeten beschermen?

VOORBEREIDING & BENODIGDHEDEN

Van tevoren kun je een aantal dingen doen:

- Lees de handleiding.
- Digibord met internetverbinding: klik door de slides voor op het digibord.
- Optioneel: bekijk alvast de video's en lees het artikel:
 - Wat is phishing? - <https://youtu.be/z4VOVHE4BNo>
 - Hoe gaat phishing via de telefoon in zijn werk? - <https://youtu.be/w7Jb7hqHZwc>
 - Klokhuus: cyberpesten - <https://www.hetklokhuis.nl/tv-uitzending/4460/Cyberpesten> (vanaf 12:00 min.)
 - Tien tips tegen cyberpesten Dylan Haegens - <https://youtu.be/QglOj5c-1Sk> (tot 1:20 min.)
 - Artikel: <https://nos.nl/artikel/2358390-veel-meer-phishing-fraude-uit-naam-van-de-belastingdienst.html>
- Deze les is een remake van de po-les HackShield 'Ga toch vissen!'. Die les is onderdeel van een lespakket met meerdere lessen. Vraag de studenten om deze les eens op de stageschool te doen! Van dezelfde serie is onlangs ook HackShield les 2 vertaald naar een Digi-doener voor de pabo. Hierin wordt het thema hacken behandeld.

DOEL VAN DE PABO-LES

Kennisbasis generiek

De student is zelf digitaal geletterd, kan leerlingen opvoeden in deze samenleving en digitale middelen benutten in zijn didactiek (2.7). De student heeft voldoende kennis van de digitale (leef)wereld van leerlingen in een netwerksamenleving en is in staat om leerlingen op te voeden in de omgang met (sociale) media en gedragsregels.

Kennisbasis Wetenschap en technologie

Wetenschap en technologie heeft de wereld om ons heen mede vormgegeven. De invloed ervan is niet meer uit ons dagelijks leven weg te denken. Technologie maakt niet alleen ons leven gemakkelijker, maar zorgt er ook voor dat we nieuwe vaardigheden moeten leren. We moeten technologie omarmen, maar ons er ook tegen beschermen.

- De leraar kan verwoorden welke didactische benaderingswijzen hij kan gebruiken om kennisconstructie bij leerlingen te stimuleren door vakbegrippen in relevante contexten en thema's aan de orde te laten komen. Hij illustreert dit met bij de groep passende voorbeelden van leerlingactiviteiten bij natuurwetenschappen en technologie.

De leraar kan beargumenteren dat het vak natuurwetenschappen en technologie bij leerlingen bijdraagt aan:

- Het ontwikkelen van een onderzoekende, probleemoplossende en kritische houding.

- Het stimuleren van aandacht en zorg voor hun eigen en andermans leefomgeving en gezondheid.
- Het ontwikkelen van zelfvertrouwen en zelfredzaamheid in hun eigen leefomgeving.

Kennisbasis Nederlands

Taalbewuste leraren zijn cruciaal om de taalcompetentie te stimuleren (Taalunie, 2017). De leraar grijpt kansen aan en stelt de behoeften van de (taal)lerende leerling centraal. De 21e-eeuwse samenleving kenmerkt zich door diversiteit en meertaligheid. In het onderwijs kunnen de verschillen in taalachtergrond groot zijn. Dat heeft ook gevolgen voor de inrichting van het taalonderwijs Nederlands. De startbekwame leraar moet kunnen inspelen op de onderwijsbehoeften van elke leerling. Dit doet hij door te differentiëren in de mate van instructie, de complexiteit van de taaltaken en de zwaarte van de rollen tijdens het samenwerkend leren. De startbekwame leraar creëert authentieke situaties waarin het voeren van gesprekken, luisteren en spreken centraal staan. Het is daarom belangrijk dat de leraar:

- De leerling leert informatie te verwerven uit gesproken taal en deze informatie schriftelijk en/of mondeling gestructureerd leert weer te geven.
- De leerling leert informatie te beoordelen en beargumenteren: in discussies en in een informatief of opiniërend gesprek.
- De leerling leert informatie en meningen te vergelijken en te beoordelen in verschillende (informatieve) teksten.

DOEL VAN DE PO-LES

Domein curriculum 2021	Leerdoelen digitale vaardigheden	Kerdoel vak	21st century skills
1 Data & informatie DG1.2 Digitale data.	1 Mediawijsheid De leerling start met het ontwikkelen van een strategie om optimaal met media om te gaan.	1 Oriëntatie op jezelf en de wereld De leerling leert zich redzaam te gedragen in sociaal opzicht en als consument.	1 Kritisch denken
2 Veiligheid en privacy in de digitale wereld DG2.1 Veiligheid in de digitale wereld.	2 Mediawijsheid De leerling wordt zich bewust van het belang van persoonlijke mediavaardigheid.	2 Taal De leerling leert informatie en meningen te vergelijken en te beoordelen in verschillende teksten.	2 Communiceren
3 Veiligheid en privacy in de digitale wereld DG2.2 Privacy in de digitale wereld.	3 ICT-basisvaardigheden De leerling leert over de (financiële) waarde van verschillende soorten accounts en content.		

INTRODUCTIE

Openingslide

Vertel de studenten dat we aan de slag gaan met een belangrijk onderdeel binnen het thema cybercriminaliteit, namelijk phishing. In deze les leren ze wat phishing betekent, ze leren phishing herkennen en denken na over een ethisch dilemma rondom phishing. Ook gaan ze aan de slag met het bedenken van een tutorial om hun leerlingen de juiste kennis, vaardigheden en houding aan te leren wat betreft phishing.



Vraag aan de studenten: Waarschijnlijk hebben veel van jullie weleens gehoord van phishing. Zijn er ook studenten die er ervaring mee hebben? Wat gebeurde er? Leverde dit problemen op? Hoe werden deze opgelost en door wie?

VERBINDING MET HET ONDERWIJS

Slide 1, Klassikaal

Vertel de studenten dat zij en hun toekomstige leerlingen te maken kunnen krijgen met cybercriminaliteit. Wachtwoorden, accounts en andere belangrijke data zijn voor cybercriminelen goud waard. Soms is het kinderlijk eenvoudig voor deze criminelen om belangrijke gegevens te achterhalen, met alle gevolgen van dien. Door corona zijn we meer thuis en regelen we belangrijke (bank)zaken veel meer vanuit huis. Voor cybercriminelen is dit de ideale situatie om belangrijke gegevens te kunnen achterhalen. Het is daarom van belang dat er al vroeg begonnen wordt met het aanleren van belangrijke vaardigheden zoals het herkennen van neppe phishingmails. Het is belangrijk dat studenten leren hoe ze hun toekomstige leerlingen bewust en bekwaam kunnen maken in hoe ze hiermee omgaan. De student moet leren welke kansen en gevaren er liggen bij het onderwerp phishing, maar moet het ook concreet kunnen maken voor zijn of haar toekomstige beroep.



PO-LES

Slide 2, Klassikaal / Groepswerk

Vertel de studenten dat deze les een remake is van HackShield les 3 'Ga toch vissen!' van FutureNL. In deze lessenserie maken leerlingen in vijf lessen kennis met het thema cybercriminaliteit. De lessenserie kunnen ze ook gebruiken voor hun (stage)praktijk, het is hier te vinden: <https://www.lessonup.com/nl/lessons/?text=hackshield>. Bij de lessenserie hoort ook een online game. Deze is te vinden op www.joinhackshield.nl, moedig de studenten aan om dit eens te spelen.



Sommige studenten zijn misschien al bekend met de lessenserie, omdat ze HackShield les 2 'Hacker Hoedjes' al gehad hebben. Mocht dit zo zijn, laat deze studenten dan hun ervaringen kort even delen met de rest van

de groep. Laat de studenten vervolgens kort de vijf lesthema's bekijken en met elkaar bespreken.

OPDRACHT

De studenten worden ingehuurd om mee te denken over een zesde les rondom cybercriminaliteit voor HackShield. Voor HackShield is het erg belangrijk dat de les digitale didactiek bevat en dat de drie onderdelen van het TPACK-model (content, didactiek en technologie) verwerkt zijn in alle lessen. Voor de zesde les is al bekend hoe de onderdelen content en technologie worden vormgegeven. Voor het onderdeel didactiek wordt de hulp van de studenten ingeschakeld. Laat de studenten bedenken en bespreken welke vorm van didactiek de zesde les moet bevatten en waarom. Opvallende en bijzondere vormen kunnen later klassikaal genoemd worden. Wanneer nodig, kan de volgende website geraadpleegd worden: <http://training.learnon.nl/tpackgame/>.

Mogelijke antwoorden:

- Toetsen: in de zesde les kan een toetsmoment opgenomen worden om te kijken of de kennis over cybercriminaliteit is verbeterd bij de leerlingen.
- Voorkennis activeren: in de zesde les kan er aan het begin aandacht worden besteed aan wat de leerlingen al weten, zodat nieuwe kennis gekoppeld kan worden aan de reeds bestaande kennis.
- Zelfstandige verwerking: in de zesde les kan er een zelfstandig verwerkingsmoment opgenomen worden, zodat de aangeboden, vooral auditieve, informatie beter verwerkt wordt.

Slide 3, Klassikaal / Groepswerk

Vertel de studenten dat phishing valt onder het thema cybercriminaliteit. Bij cybercriminaliteit wordt een computersysteem aangevallen of misbruikt voor criminele activiteiten. Hierbij kun je denken aan iemand die een computer of software gebruikt voor strafbare handelingen. Oplichting of afpersing via bijvoorbeeld e-mail zijn hier voorbeelden van. Een ander persoon (jij?) is dan het doelwit. Vaak zijn ook computers en systemen zelf het doelwit. Hierbij kun je denken aan het stelen (of 'gijzelen') van bestanden, het verspreiden van computervirussen of het verstoren van computersystemen. Cybercriminaliteit heeft een enorme impact op de Nederlandse samenleving. In 2019 werd ongeveer één op de acht Nederlanders slachtoffer van één of meerdere cybercrimedelicten volgens het Centraal Bureau voor de Statistiek. Vaak zijn vijftigplussers het slachtoffer en is de schade al snel € 2000,- tot € 3000,- per persoon.



OPDRACHT

Vraag aan de studenten welke vormen van cybercriminaliteit zij allemaal kennen. Hoeveel kunnen ze er noemen? Zijn zij zich ervan bewust dat er wel tientallen vormen van cybercriminaliteit bestaan naast phishing? Geef de studenten vijf minuten de tijd en laat ze op het internet op zoek gaan naar verschillende vormen van cybercriminaliteit. Bespreek kort met de studenten: Hoeveel vormen hebben zij gevonden? Zitten er

ook nog vormen bij die ze niet kenden, maar wel belangrijk vonden om bewust van te zijn?

Mogelijke antwoorden:

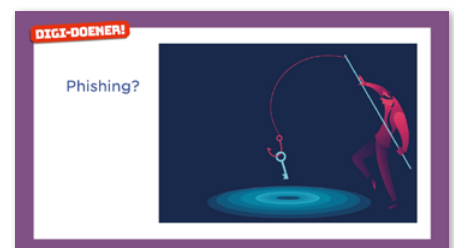
Hacking, kinderporno, ransomware, phishing, virussen, malware, botnets, cryptojacking.

Verder lezen voor meer voorbeelden? Zie: <https://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/>.

VERDIEPING

Slide 4, Klassikaal

Vertel de studenten dat waarschijnlijk veel van hen wel weten wat phishing is. Maar kunnen zij er ook de juiste definitie aan geven zonder te googelen? Welke definitie geven zij aan phishing? Laat de studenten hun eigen definitie opschrijven en delen met de klas. Zijn alle definities gelijk wat betreft de inhoud en beschrijving of zit er nog verschil in? Een voorbeeld van een definitie kan zijn: 'Phishing is het 'vissen' naar persoonlijke gegevens door mensen te misleiden met bijvoorbeeld een neppe website, neppe e-mail of een nep sms- of whatsappbericht'. Bekijk vervolgens samen de video voor een uitleg over phishing: <https://youtu.be/It7qErxa5Qg>.



Slide 5, Klassikaal

Vertel de studenten dat er, volgens een artikel van de NOS, tot november 2020 150.000 meldingen over phishingpraktijken zijn binnengekomen. Dat is ruim vier keer zo veel als de 35.000 meldingen van phishing die de fiscus vorig jaar kreeg. Laat de studenten het artikel op hun device opzoeken: <https://nos.nl/artikel/2358390-veel-meer-phishing-fraude-uit-naam-van-de-belastingdienst.html>. In het artikel wordt geschreven dat de Belastingdienst probeert phishingwebsites zo snel mogelijk te blokkeren en mensen adviseert mogelijke fraude te melden. Bespreek met de studenten welke adviezen er worden gegeven en of ze hier zelf ook aan gedacht zouden hebben.



De volgende adviezen worden gegeven:

- Meld valse en verdachte e-mails via valse-email@belastingdienst.nl.
- Stuur de mailheader door naar Belastingdienst.

Slide 6, Klassikaal

Vertel de studenten dat er verschillende vormen van phishing zijn en dat zij nu de vier meest bekende vormen zien op de slide. Licht elke vorm even kort toe met de tekst hieronder.

- **Spear phishing:** spear phishing werkt gericht op één persoon of organisatie. Spear phishing valt een specifiek persoon of organisatie aan, vaak met inhoud die is toegesneden op het slachtoffer of de slachtoffers. Vooraf heeft er een verkenning plaatsgevonden van namen, functietitels, e-mailadressen en dergelijke. Met al deze



informatie creëert de phisher een geloofwaardige e-mail. Wanneer de phishing is gelukt, kan de phisher bijvoorbeeld een betalingsmail omleiden naar zijn eigen bankrekening.

- **Clone phishing:** bij deze aanval maken criminelen een kopie of kloon van eerder bezorgde en legitieme e-mails die een koppeling of bijlage bevatten. Nietsvermoedende gebruikers klikken op de koppeling of bijlage waardoor hun systeem in veel gevallen wordt overgenomen. Vervolgens kan de phisher de identiteit van het slachtoffer nabootsen om zich als vertrouwde afzender voor te doen.
- **419/Nigeriaanse zwendel:** bij de Nigeriaanse zwendel krijg je een langdradige phishingmail van iemand die beweert dat hij een Nigeriaanse prins is. Deze vorm is één van de eerste en langstlopende zwendels op het internet. De e-mail is gemarkeerd als 'dringend' of 'privé' en de afzender vraagt de ontvanger om een bankrekening op te geven waarop gelden in bewaring kunnen worden gegeven. Het getal 419 verwijst naar de sectie van de Nigeriaanse strafwet die handelt over fraude en straffen voor de plegers.
- **Phone phishing:** bij phone phishing (ook wel voice phishing of vishing genoemd) belt de phisher op en beweert hij namens de bank, politie of de Belastingdienst te handelen. Ze vragen doorgaans om een gedwongen overboeking of betaling via prepaidkaarten, zodat ze onmogelijk op te sporen zijn. Een andere vorm van phone phishing is sms-phishing, hierbij wordt via sms-berichten dezelfde soort zwendel gedreven. Via een ingebouwde, kwaadaardige koppeling wordt er ingebroken in je gegevens.

Slide 7, Klassikaal

Vertel de studenten dat ze met een beetje kennis, gezond verstand en wat tips phishing snel kunnen herkennen. Op de slide staan een aantal tips die ze goed kunnen gebruiken voor het herkennen van phishing en tevens bij het toepassen van eerste hulp bij phishing.

- Phishingaanvallen maken vaak gebruik van angst om het oordeelsvermogen te beïnvloeden. Vertrouw daarom op je intuïtie, maar laat je niet bang maken. **Tip 1:** Volg je verstand.
- Is het aanbod in de e-mail te mooi om waar te zijn? Dan is dit het vaak ook. Herken je de afzender, maar is het iemand met wie je geen contact hebt gehad? **Tip 2:** Wees achterdochtig en beoordeel de inhoud kritisch. Bij twijfel: verwijder het bericht.
- Is het bericht schrik aanjagend? Bevat de e-mail alarmerende taal om je snel tot actie (klikken op snelkoppelingen of bijlagen) over te laten gaan? **Tip 3:** Bedenk dat verantwoordelijke organisaties nooit via het internet om persoonlijke gegevens vragen. Meld het eventueel bij het desbetreffende bedrijf.
- Bevat het bericht onverwachte of ongewone bijlagen? Deze bijlagen kunnen malware, ransomware of een andere bedreiging bevatten. **Tip 4:** Open de bijlagen niet en verwijder ze.
- Bevat het bericht koppelingen die er wat onwaarschijnlijk uitzien? **Tip 5:** Vertrouw hyperlinks niet blindelings en klik er niet zomaar op.



Slide 8, Klassikaal

 Ondertussen hebben de studenten behoorlijk wat kennis opgedaan over phishing en andere vormen van cybercriminaliteit. Ze weten dat phishing veel (financiële) schade kan opleveren bij verkeerd handelen van het slachtoffer. Maar wie is er nu eigenlijk verantwoordelijk voor de schade? Het geld is weg, de dader is niet meer te achterhalen en de schade is soms erg groot. Had de burger niet zijn eigen verantwoordelijkheid moeten nemen en zichzelf moeten laten voorlichten? Of had het bedrijf waar de phishing plaatsgevonden heeft zichzelf beter moeten beschermen met digitale certificaten, ingebouwde waarschuwingsberichten of een dubbele check? Bespreek met de studenten dit dilemma.



DOEN

Slide 9, Groepswerk

In de afgelopen slides hebben de studenten geleerd wat phishing is, welke vormen van phishing er zijn, hoe je het kunt herkennen en wat je kunt doen als er bij jou gephisht wordt. Al deze kennis gaan ze nu gebruiken om een tutorial te maken voor een les over phishing. Aan de slag!



Stap 1

Vertel de studenten dat zij aan de slag gaan met het maken van een tutorial die zij kunnen gebruiken bij een les over cybercriminaliteit en phishing. Door een video(tutorial) toe te passen in hun onderwijspraktijk, maken ze bewust (of onbewust) gebruik van digitale didactiek in de les en maken ze hun eigen educatieve content. Door verschillende soorten content toe te passen in de les, worden hun toekomstige leerlingen gestimuleerd en gemotiveerd om meer te willen leren. Dit zijn de eisen waar de tutorial aan moet voldoen:

- De studenten hebben ongeveer 45 minuten de tijd: van het schrijven van het script tot het opnemen van de video.
- De video mag maximaal vijf minuten duren.
- De video moet het onderwerp phishing begrijpbaar en concreet maken voor groep 7 en 8.
- Taal, teksten en voorbeelden moeten afgestemd zijn op groep 7 en 8.
- In de video moet uitgelegd worden wat phishing is, hoe de leerlingen het kunnen herkennen en wat ze zouden kunnen doen als ze in aanraking komen met phishing.

Stap 2

Bekijk met de studenten de volgende video's ter inspiratie:

- Hoe gaat phishing via de telefoon in zijn werk? - <https://youtu.be/w7Jb7hqHZwc>
- Klokhuus: cyberpesten - <https://www.hetklokhuis.nl/tv-uitzending/4460/Cyberpesten> (vanaf 12:00 min.)
- Tien tips tegen cyberpesten Dylan Haegens - <https://youtu.be/Qgl0j5c-1Sk> (tot 1:20 min.)

Stap 3

Bespreek na het bekijken van de video's wat de studenten gezien hebben. Op welke manier worden belangrijke onderwerpen concreet en bespreekbaar gemaakt? Hoe zouden zij dit kunnen doen voor hun eigen tutorial?

Stap 4

Verdeel de studenten in groepjes en laat ze bedenken wat ze hun leerlingen willen leren met hun tutorial. Wat wordt het doel van de tutorial?

Stap 5

Laat de studenten een (simpel) storyboard van de tutorial maken. Welke opbouw hanteren ze in de tutorial en hoe verwerken ze hun doel van stap 4?

Stap 6

Laat de studenten afspreken waar en wanneer ze gaan filmen en wat ze nog meer nodig hebben om tot een succesvol product te komen.

Stap 7

Alles duidelijk en geregeld? Filmen maar!

Slide 10, Klassikaal

Vertel de studenten: Met deze laatste opdracht ronden we de les over phishing af. We gaan de tutorials bekijken en beoordelen aan de hand van een aantal kijkvragen. Is het gelukt om een tutorial te maken? We gaan het nu zien!

★ TIP

Er kan gekozen worden voor het delen van de tutorials via WhatsApp, YouTube of ander platform, maar hier moet wel eerst toestemming voor gegeven worden door alle 'acteurs'. Mochten er bezwaren zijn, dan worden de tutorials vooraf naar de docent gestuurd en uiteindelijk verwijderd.



Na het bekijken van de tutorials worden onderstaande vragen ter beoordeling gesteld:

- Heeft de tutorial een duidelijke inleiding, kern en slot?
- Is het begrip phishing voldoende concreet gemaakt voor groep 7 en 8?
- Zijn er tips verwerkt in de tutorial waardoor de leerlingen phishing leren herkennen en weren?
- Zijn het taalgebruik, de voorbeelden en tekst afgestemd op groep 7 en 8?
- Hoeveel sterren krijgt de tutorial? (1 t/m 5)
- Na het bekijken van alle tutorials: welke tutorial zouden jullie morgen gelijk gebruiken?