

Vingerafdruk!

Tijdens deze les gaan de studenten ervaren wat een vingerafdruk is en hoe deze gebruikt kan worden voor de veiligheid van jezelf en de samenleving. Ook leren ze over classificatie en databanken. Ze ontdekken wat ethische hackers zijn en hoe ze te werk gaan. Ethische hackers werken in veel gevallen in opdracht van bedrijven, maar gaan soms ook ongevaaragd aan de slag. Wat vinden de studenten van deze werkwijze?

Totale duur: 1-1,5 uur

VERBINDING MET BEROEPEN EN DE ARBEIDSMARKT

Zo zet Defensie, IT- beveiliging, banken, politie en de overheid de skills in deze les ook in om te zorgen voor veiligheid (forensisch onderzoek) en de beveiliging van digitale informatie (bijvoorbeeld het betalingsverkeer).

LESOPBOUW

- Introductie: Waar wordt een vingerafdruk voor gebruikt?
- Verdieping: Eigen vingerafdruk bestuderen en classificeren aan de hand van de lijnen
- Doen: Eigen afdruk tekenen en nadenken over de databank / database van alle afdrucken in de klas
- Afronding: Kijken naar de verschillende manieren waarop smartphones beveiligd zijn en op welke manier hier op dit moment onderzoek naar wordt gedaan door universiteiten en ethische hackers.

VOORBEREIDING & BENODIGDHEDEN

Van tevoren kun je een aantal dingen doen:

- Lees de handleiding en lesbrief
- Klik door de slides voor op het digibord en bekijk het filmpje
- Print de lesbrief uit de PO Digi-doener voor studenten
- Schaar, lijm, inkt of stempelkussens (voor vingerafdrucken)
- Een A3 vel om later alle vingerafdrucken op te plakken
- Optioneel: een vergrootglas voor zoveel mogelijk studenten

Lees het volgende krantenartikel om meer te weten te komen over de gevaren van biometrische technieken.

<https://www.parool.nl/nieuws/liggen-je-biometrische-gegevens-op-straat-dan-ben-je-voorgoed-de-pineut-bfad289f/>

Deze les is een remake van PO Digi-doener 'Vingerafdruk!' (les nummer 28), voor de middenbouw

ETHIEK & TECHNOLOGIE

Op dit moment zijn veel telefoons beveiligd met een vingerafdruk. Dit lijkt een erg goede manier om je telefoon te beveiligen, en om op een veilige en eenvoudige manier bankzaken te regelen. Logisch dat er door veel bedrijven gekeken wordt om andere zaken (zoals inloggen in de Cloud) ook met vingerafdrucken te beveiligen. Op dit moment wordt er nog vaak een wachtwoord gebruikt, en omdat we vaak hetzelfde wachtwoord gebruiken voor verschillende websites, zijn deze makkelijk te kraken. Maar hoe veilig is biometrische beveiliging nu echt?

DOEL VAN DE PABO-LES

Kennisbasis generiek

1. De student is zelf digitaal geletterd, kan leerlingen opvoeden in deze samenleving en digitale middelen benutten in zijn didactiek (2.7):
Mediapedagogiek: kennis van de digitale (leef) wereld van kinderen in een netwerksamenleving, opvoeding in omgang met sociale media en gedragsregels.
2. Natuurwetenschappen & technologie
De student 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.
Het ontwikkelen van een onderzoekende, probleemoplossende en kritische houding.

DOEL VAN DE PO-LES

Domein curriculum.nu	Leerdoelen digitale vaardigheden	Leerdoel (kern)vak	21st century skills
1 Veiligheid & privacy in de digitale wereld DG 2.1 Veiligheid in de digitale wereld. DG 2.2 Privacy in de digitale wereld.	1 Informatievaardigheden De leerling kan de gevonden informatie ordenen.	1 Mens & samenleving De leerling leert zich redzaam te gedragen in sociaal opzicht; als verkeersdeelnemer en als consument.	1 Creatief denken
2 Digitaal burgerschap DG 5.1 De digitale burger. DG 5.2 Digitale identiteit.	2 De leerling kan verbanden tussen variabelen leggen.	2 Natuur & techniek De leerling leert onderzoek doen aan materialen en natuurkundige verschijnselen, zoals: licht, geluid, elektriciteit, kracht, magnetisme en temperatuur. De leerling leert oplossingen voor technische problemen te ontwerpen, deze uit te voeren en te evalueren.	2 Kritisch denken
3 Digitaal burgerschap DG 5.2 Digitale identiteit		3 Rekenen De leerling leert structuur en samenhang van aantallen, gehele getallen, kommagetallen, breuken, procenten en verhoudingen op hoofdlijnen te doorzien en er in praktische situaties mee te rekenen.	

DIGITALE DIDACTIEK

TPACK	SAMR
Didactiek: Tijdens een klassikaal leergesprek leren de studenten over de opbouw van vingerafdrukken en waarom ze uniek zijn. Daarna gaan ze samen aan de slag met hun eigen vingerafdruk (ontdekkend leren). Aan het eind van de les volgt een klassikale discussie over de veiligheid van vingerafdrukscanners.	Aanpassing: Technologie heeft een meerwaarde. We gaan deze les kijken hoe eigenschappen van het menselijk lichaam (biometrie) gebruikt kunnen worden ter identificatie voor computers. Hiermee hoeven we geen wachtwoorden of pincodes meer te onthouden.
Technologie: In deze les wordt er gebruik gemaakt van het digi-bord voor de presentatie waarin foto's en filmpjes te zien zijn.	
Content: De les gaat in op natuurwetenschappen en techniek en behandelt biometrische beveiligingsmethodes en wat dat betekent voor je privacy.	

INTRODUCTIE

Slide 1, klassikaal

Vertel de studenten dat deze les over vingerafdrukken gaat. We gaan kijken hoe een vingerafdruk is opgebouwd, waar ze op dit moment voor gebruikt worden en hoe je ze kan classificeren. Ook gaan we het hebben over mediawijsheid. We kijken op welke verschillende manieren je kan inloggen op je telefoon. We bekijken hoe hier door universiteiten, maar ook door ethische hackers onderzoek naar wordt gedaan.

Slide 2, praten met de klas

Laat de studenten reageren op de slide. Weten ze wat dit voor een apparaat is? Dit is een vingerafdrukscanner. Je kan met een simpele scanner je laptop beveiligen, maar ze worden ook gebruikt door bijvoorbeeld bedrijven en sportscholen om mensen toegang te geven tot een gebouw.



Hebben de studenten nog andere voorbeelden? Denk aan:

- Identificatie (betalen, toegang tot telefoon / computer)
- Opsporingsmiddel (recherche, paspoort)

Vertel dat vingerafdrukken als identificatie in 1858 voor het eerst werden gebruikt. Een Engelsman kreeg het idee om vingerafdrukken te gebruiken op loonzakjes van plaatselijke arbeiders. Het kwam namelijk regelmatig voor dat arbeiders voor een tweede keer in de rij gingen staan om nogmaals een loonzakje te ontvangen.

Inventariseer bij de studenten op welke manier ze hun telefoon vergrendeld hebben. Wie doet dit via een cijfercode, een patroon tekenen of met een vingerafdruk? Welke manier van beveiligen is volgens studenten het veiligst? Ga hier verder nog niet uitgebreid op in, we komen hier later op terug!

VERDIEPING

Slide 3, klassikaal

De studenten gaan straks een vingerafdruk maken. Ze gaan het patroon van de lijnen goed bestuderen en natekenen op hun lesbrief. Daarna maken ze een database van alle vingerafdrukken van de klas, verdeeld in drie groepen.

Bekijk samen met de studenten het filmpje om erachter te komen waarom je vingertoppen uniek zijn. Laat studenten dit kort in hun eigen woorden herhalen.

De vingertoppen bevatten dunne lijntjes die lussen, kringen of bogen vormen. Die lijntjes op je vingers, bestaan uit nauwe dalen (dit noem je **groeven**) en heuveltjes (dit noem je **huidlijsten** of **papillairlijnen**). Als je dus naar een vingerafdruk in inkt kijk, kijk je eigenlijk naar het patroon van de huidlijsten.



Slide 4, klassikaal

Laat de studenten opdracht 1 van de lesbrief maken. Leg daarna uit dat we gaan kijken naar drie lijn patronen. In het echt houdt de recherche (en vooral de software die ze gebruiken) rekening met nog meer kenmerken. Dit zijn de drie patronen waarin ze de vingerafdrukken gaan classificeren:

1. Boogpatroon: De lijnen gaan langs een zijde binnen. Ze vormen lijnen, lopen naar het midden en gaan via de andere zijde terug naar de andere kant van je vinger.
2. Lusp patroon: De lijnen komen aan een kant binnen, maken een lus en gaan naar dezelfde kant van de vinger weer terug.
3. Draaiingspatroon: De lijnen vormen een cirkel in het midden van de vingerafdruk.



Laat de studenten opdracht 2 van de lesbrief maken. Daarna gaan ze de (drie verschillende) lijnpatronen goed bestuderen.

Slide 5, doen

Laat de studenten opdracht 3A van de lesbrief maken. De studenten kunnen op de slide kijken voor een voorbeeld.

Slide 6, doen en praten met de klas

Tijdens opdracht 3B zetten de studenten hun naam onder hun vingerafdruk en welk lijnenpatroon het is.

Slide 7, Klassikaal

De studenten gaan samen een databank maken. We gaan kijken welk patroon het vaakst voorkomt. Komt dit overeen met 'Henry-classificatiesysteem'? Een boogpatroon komt bij 5% van de mensen voor, een luspatroon bij 30% en het patroon met draaiingen bij 65%.

Slide 8, praten met de klas

Kom terug op de vraag die aan het begin van de les aan studenten gesteld is. Op welke manier hebben de studenten hun telefoon vergrendeld? Wat was volgens hen de veiligste manier? Vertel dat er door verschillende universiteiten onderzoek wordt gedaan naar de veiligheid van telefoonbeveiliging. Hiervoor schrijven ze speciale algoritmes. Weten studenten nog wat algoritmes zijn?

Viercijferige pincode

Onderzoekers van de universiteit van Newcastle konden in 70% van de gevallen een pincode van vier cijfers in één keer raden! Ze hadden maximaal vijf pogingen nodig om de overige codes te kraken. De onderzoekers hebben hiervoor een algoritme geschreven. Het algoritme maakt gebruik van verschillende sensoren die in de nieuwste smartphones zitten. Aan de hand van die sensoren konden ze bewegingen meten en daarmee de pincode makkelijk achterhalen. Stel dat je een foute app of website op je telefoon opent, dan kunnen hackers toegang krijgen tot deze bewegingssensoren. Hiermee kunnen ze alles zien wat je doet (scrollen, inzoomen, typen). Deze bewegingssensoren kunnen de kleinste bewegingen waarnemen.

Tekenen van een patroon

Bij deze manier wordt de telefoon ontgrendeld door een patroon te tekenen op het scherm. Er verschijnen stippen op het scherm en via een lijn wordt er een patroon getekend. Uit onderzoek van verschillende universiteiten is gebleken dat deze manier van ontgrendelen vaak binnen vijf pogingen te kraken is. Hiervoor maakten ze gebruik van een camera en een speciaal algoritme dat beeld kan interpreteren. De onderzoekers namen via de camera het beeld van een 'slachtoffer' op. Het algoritme komt vervolgens met een paar mogelijke patronen. Een hacker zou op deze manier (bijvoorbeeld in een café) achter de

DIGI-DOENER!



Schematisch tekenen voor onze databank:

1. Teken eerst met je linkerhand de omtrek van jouw rechterwijsvinger in het vak in de lesbrief.
2. Teken jouw patroon erin.

DIGI-DOENER!

Schrijf nu je naam onderaan de omtrek en welk patroon het is:

1. boog,
2. lus of
3. draaiing.



DIGI-DOENER!

We gaan nu een **databank** (verzameling) maken met de drie groepen. Als je iets in groepen indeelt heet dat **classificeren**.

Naam leerling	Boog	Lus	Draaiing

DIGI-DOENER!

Beveiliging van je telefoon



patronen van andere mensen kunnen komen.

Slide 9, praten met de klas

De beste manier lijkt dan toch de vingerafdrukscanner. Welke voordelen heeft een vingerafdrukscanner volgens studenten?

- Iedere vingerafdruk is uniek, dus niet makkelijk te hacken.
- Je hoeft geen moeilijk wachtwoord of pincode te onthouden.

Inmiddels is er ook onderzoek gedaan naar vingerafdrukscanners (en vooral naar die op smartphones) door universiteiten in Amerika. Ze hebben geprobeerd om een soort super vingerafdruk in elkaar te knutselen, waarmee je een groot deel van alle smartphones kunt ontgrendelen en dit lukte nog ook!

Je **hele** vingerafdruk is uniek, maar het probleem met scanners op telefoons is dat ze maar een klein deel van je vinger scannen (meer laat de grootte van de scanner niet toe). Je slaat ook nooit één vingerafdruk op, maar je maakt vaak tientallen afdrukken.

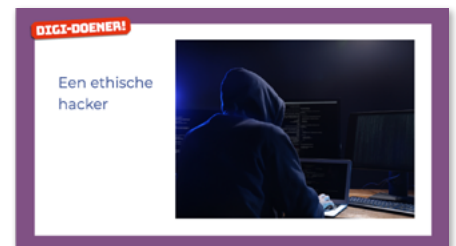
De onderzoekers hebben gekeken welke kenmerken het meest voorkomen bij vingerafdrukken en vervolgens hebben ze een aantal 'masterprints' gemaakt. Met deze masterprints zijn ze er in geslaagd om 40% tot 50% van de smartphones te unlocken.



Slide 10, Klassikaal

Vraag aan de studenten of ze weten wat een ethische hacker is en wat hij of zij doet. Bekijk daarna het filmpje.

Naast universiteiten die onderzoek doen naar beveiliging, kunnen bedrijven of overheden dus ook hackers inhuren om te kijken naar de veiligheid.



Slide 11, Klassikaal

Jan Krissler, een bekende Duitse hacker is er al meerdere keren in geslaagd om diverse veiligheidssystemen die gebruik maken van biometrie te hacken. Dit is technologie die fysieke eigenschappen (zoals vingerafdrukken, handafdrukken en irissen) gebruiken ter identificatie.

Met behulp van foto's kon hij scanners voor irissen en vingerafdrukken hacken. Hij is er zelfs in geslaagd om vingerafdrukken van Duitse ministers na te maken.

Zelfs één van de meest recente scanners voor handafdrukken is door hem al gehackt. Het voordeel van handafdruk scanners is, dat ze naast vingerafdrukken, ook de lijnen in je handpalm en aders scannen. Toch is de Duitse hacker met behulp van foto's en een nagemaakte handafdruk erin geslaagd om deze scanner te hacken.

icoon ethiek

De hacker deed dit niet in opdracht van de Duitse overheid, maar op eigen initiatief. Wat vinden de studenten hiervan? Vinden ze dat het doel hier de middelen heiligt?



AFRONDING

Slide 12, Klassikaal

Bekijk ter afsluiting van de les het filmpje.

 In het filmpje is te horen dat Het College Bescherming Persoonsgegevens een voorkeur heeft voor het gebruik van een pasje ter identificatie. We hebben deze les geleerd dat vingerafdrukken uniek zijn, maar desondanks kunnen vingerafdrukscanners toch gekraakt worden.

Waarom moeten bedrijven en overheden zorgvuldig(er) omgaan met het gebruik van deze biometrische gegevens?

Vraag aan de studenten wie wel eens zijn bankpas kwijtgeraakt is. Wat hebben studenten toen gedaan? In zo'n geval zullen studenten hun bank gebeld hebben om het pasje te laten blokkeren en een nieuwe pas aangevraagd hebben.

Hetzelfde geldt voor wachtwoorden en pincodes. Worden deze gekraakt, dan is dat vervelend en kunnen er nare dingen gebeuren, maar je kan aan het eind altijd weer een nieuw wachtwoord of pincode aanvragen.

Met biometrische gegevens ligt dit anders. Mocht je gezichtsscan of vingerafdruk in verkeerde handen belanden, dan ben je eigenlijk voorgoed de pineut. Je kan namelijk nergens een andere vingerafdruk aanvragen.

Vorig jaar bleek dat bij een groot beveiligingsbedrijf, waar miljoenen vingerafdrukken en ander biometrisch materiaal opgeslagen is, (zoals van sportscholen, maar ook de Londense politie) niet goed beveiligd was. Als zo'n databank eenmaal gekraakt wordt en bij de verkeerde mensen terecht komt, zou er dus op grote schaal identiteitsfraude gepleegd kunnen worden.

Wat hebben studenten deze les geleerd? Gaan ze anders kijken naar hun eigen beveiliging? Gaan ze voorzichtiger om met het verstrekken van hun biometrische gegevens? Vinden ze dat biometrische gegevens niet meer gebruikt zouden moeten worden? Waarom wel/niet?

Voor meer informatie kan eventueel dit krantenartikel gelezen worden:

<https://www.parool.nl/nieuws/liggen-je-biometrische-gegevens-op-sstraat-dan-ben-je-voorgoed-de-pineut-bfad289f/>

