Bijlage 1: script en vragen video’s

Welkom video:

Hallo, ik ben Daan. ik ga samen met een paar vrienden jouw helpen in de leermethode van de gemeente kampen. In deze methode ga je leren hoe je jezelf beter kan beschermen tegen online dreigingen. Toen het internet zoals wij het vandaag de dag kennen in de jaren 60 ontstond, wisten we nog niet wat voor gevaren het kon gaan opleveren. Door het internet kunnen we gemakkelijk dingen opzoeken, maar ook mensen met slechte bedoelingen kunnen makkelijk iets over je te weten komen. In deze methode gaan we je helpen om je te beschermen tegen online gevaren en gaan we zorgen dat zogenaamde hackers niet zomaar al jou gegevens kunnen achterhalen. Doormiddel van video's en vragen gaan we leren over phishing en bankhelpdeskfraude. wat is het? en hoe kan je jezelf er tegen beschermen? laten we maar snel gaan beginnen.

Phishing:

Les 1: wat is phishing?

Hallo, als eerst gaan we het hebben over phishing. In dit eerste onderdeel ga je leren wat phishing is. Vervolgens ga je in het volgende onderdeel leren hoe je erachter kan komen of een website wel echt is. Het laatste onderdeel over phishing gaat over de URL van een website en wat je daar aan hebt.

Phishing is een vorm van online oplichting waarbij criminelen zich voordoen als een betrouwbare organisatie, zoals een bank, om gevoelige informatie van je te stelen. Dit gebeurt vaak via e-mails, sms'jes, sociale media of nepwebsites die eruitzien als officiële communicatie. Ook kan je dit tegenkomen bij nep reclames op echte websites. Door zich voor te doen als betrouwbaar willen ze jou e-mail adres en wachtwoord weten zodat de oplichters ook kunnen inloggen op jouw accounts en bijvoorbeeld dingen met jouw geld gaan bestellen. Dit kan ook gelden voor je naam, adres, telefoonnummer. De reden waarom dit heel bekend is voor oplichters is omdat ze heel erg makkelijk een phishingspakket kunnen kopen. Daarmee kopen ze al voor 150 euro alles wat ze nodig hebben om jou op te lichten.

Bij een e-mail gebeurd het vaak dat je op een link moeten klikken, via deze link kom je op een nep inlogscherm waar je gegevens moet invullen. Door dit te doen kunnen de oplichters die ingevulde gegevens bekijken. Bij sms’jes geld eigenlijk hetzelfde als bij e-mails, via een link kom je op een nep inlogscherm waar je je gegevens moet invullen. Ook op sociale media en reclames kan je makkelijk deze linkjes vinden. Als je via een advertentie ergens op komt kan je best op een nepwebshop komen waar je wel je e-mail in moet vullen.

Al met al wordt je naar nep pagina’s gelokt waar je je gegevens moet invullen die de oplichters vervolgens kunnen bekijken. In de volgende twee delen ga dit soort pagina’s leren herkennen.

Vragen:

1. Als wie doen criminelen zich voor bij phishing?
    - Betrouwbare organisatie
    - Bank
    - School
    - Verkoper
2. Welke gegevens willen criminelen van je hebben?
    - Telefoonnummer
    - Lievelingskleur
    - Adres
    - Wachtwoord
    - Naam
    - Kleur ogen
    - Lengte
3. Is phishing een makkelijke manier van oplichten voor criminelen?
   Ja, nee
4. Waar kom je waarschijnlijk phishing tegen?
    - E-mails
    - Sms'jes
    - Kranten
    - Online advertenties
5. Wat kan je doen om te voorkomen dat je in een phishing link trapt?
    - Op elke link klikken die ik zie,
    - Niet op onbekende linkjes klikken
    - Eerst controleren of de website wel echt is voordat je gegevens invoert
    - Nooit meer op het internet gaan.

Les 2: Wat kopen? Doe onderzoek!

Daar ben ik weer, nu je weet wat phishing is gaan we leren hoe je het kan herkennen. Het leren herkennen gaan we doen aan de hand van 5 verschillende onderdelen. Het eerste onderdeel is reviews. Als je iets wilt gaan kopen op een wat minder bekende website is het handig om reviews over de webshop te gaan vinden. Dit zijn recensies van andere klanten die iets op de webshop hebben gekocht. Als je leest dat vele mensen het hebben over oplichting, phishing en dat de site niet betrouwbaar is kan je er beter niks kopen.

Het volgende is om te kijken of je het product ook op een bekende webshop kan kopen. Hierdoor is de kans een stuk lager dat je met het invullen van de gegevens hackers geven wat ze willen.

Ook is dat je beter niet direct iets haalt van een advertentielink. Zie je op het internet een mooie advertentie met een link naar de webshop? Zoek dan handmatig de webshop op via het internet. Doordat je zelf naar de website gaat is de kans kleiner dat je op een nep versie van de website komt. Hierdoor kan je alsnog het mooi product halen maar geef je de hackers niet al jou informatie.

Nog iets waar je bij webshops op moet letten: is het product niet te goedkoop. Dit kan voor hackers een vorm van overhalen zijn waardoor jij gemakkelijker het product gaat halen. Doordat je het wilt bestellen moet je eerst je gegevens invullen die de hacker vervolgens kunnen gebruiken.

Het laatste waar je bij het online shoppen op moet letten is de betalingsmogelijkheid. Moet je via bitcoin, een online munt, of zelf het bedrag overboeken? Dan moet je extra alert zijn. De meeste echte webshop geven je de mogelijkheid om dat iDeal of PayPal te betalen. Het betekend niet gelijk dat de website niet betrouwbaar is als dit niet kan, maar je moet dan wel extra goed controleren of de website legitiem is voordat je gegevens gaat invullen.

Met deze 5 tips kan je jezelf beter beschermen bij je volgende digitale aankoop. Maak nu een aantal vragen om te kijken of je het hebt gegrepen.

Vragen:

Bij welke reviews moet je extra goed opletten of de site wel echt is?

- Een review over hoe goed het product is,
- Een review over de lange levertijd
- Een review dat het product nooit is aangekomen
- Een review over het constant gebeld worden na wat kopen op de webshop

Welke van de volgende websites zijn het meest verdacht?

- Amazon
- Bul.com
- AlibabaShop
- Zalando

Je ziet een mooi advertentie van iets wat je wilt kopen, wat doe je niet?

- Klikt op de advertentie om het gelijk te kunnen kopen
- Zoek het product op bij een bekende webshop

U wilt een nieuwe tv kopen, u heeft een model gevonden die past bij uw eisen, wat doet u niet?

- Ik koopt de tv op webshop Emazon, hier was het heel erg goedkoop
- Ik zoek op een aantal bekende webshops voor de tv die ik zoek
- Ik vind via een advertentie de tv die ik wil en klik gelijk op de link om het te gaan kopen.

U wilt u tv gaan betalen, op de webshop staat dat u een creditcard moet kopen en daar de pincode en bankadres van moet invullen, als zij bij de creditcard kunnen krijgt u uw product, wat doet u nu?

- Ik koop de creditcard en vul de gegevens in op de webshop
- Ik ga gelijk van de webshop af omdat hij nep is
- Ik stuur de helpdesk de vraag of ik op een andere manier kan betalen
- Ik rapporteer de website als gevaarlijk

Les 3: de URL kan je helpen!

Daar ben ik weer, nu je een aantal dingen hebt geleerd over phishing gaan we het nog hebben over de URL van een website. Een URL zie je als je op het internet zit bovenaan de pagina en begint met https:// of http://. Hier heb jij normaal niet heel mee te maken, dit is er zodat de computer weet op welke website je zit. Aan deze URL kan je best wel een aantal dingen aflezen om je te helpen niet in phishing te trappen. Op het moment dat je op de website bent gaan we nu eerst kijken waar daar allemaal wel niet staat voordat je verder gaat kijken op de site.

Als eerst gaan we kijken of de website wel beveiligd is. dit kan je zien aan het begin van de URL. Bij een beveiligde website staat er voor de URL een slotje, ook begint de URL met https. Begint de website het http, dan is deze niet beveiligd. Dit betekend niet dat het gelijk een phishing pagina is maar geeft wel aan of je extra scherp moet opletten. Alle grote websites zijn beveiligd.

Het volgende waar je op gaat letten is op typfouten, staat er in https://www.bul.com in plaats van https://www.bol.com dan kunt u de website als gevaarlijk beschouwen.

Het kan ook zijn dat er te veel woorden worden gebruikt in de URL. Een voorbeeld hiervan is: https://www.debelastingdiest.nl in plaats van wat de belastingdienst echt gebruikt: https://www.belastingdienst.nl. In deze gevallen is er ook vaak sprake van phishing.

Ook kan je letten op de aantal punten in de URL. Staat er https://www.rabo.bank.nl dan kan je verwachten dat je te maken hebt met een phishing pagina, dit komt doordat de Rabobank geen punt en zijn naam heeft en je dus verwacht er https://www.rabobank.nl. Een uitzondering op deze regel is iets met ‘mijn’; een voorbeeld hiervan is: https://www.mijn.rabobank.nl

Het laatste waar je op moet letten zijn dubbele dingen in de URL. Staat er bijvoorbeeld https://www.trouw.nl.detrouw.nl dan kan je ook verwachten dat je met een nepwebsite te maken hebt. De echte URL van Trouw is: https://www.trouw.nl

Nu heb je een aantal handvaten om phishing websites te herkennen aan de hand van de URL.

Vragen:

Waar kan je de URL van een website vinden?

- Onderaan je scherm
- Rechts op je scherm
- Links op je scherm
- Bovenaan je scherm

Wanneer is een website beveiligd?

- Als er een open slotje te zien is bij de URL
- Als er geen slotje te zien is bij een URL
- Als er een dicht slotje te zien is bij de URL
- Als de URL begint met http://
- Als de website begint met https://

Op welke dingen kan je allemaal letten bij de URL om te kijken of de website betrouwbaar is?

- Op spelfouten
- Op lange namen
- Op extra woorden
- Op dingen die dubbel staan
- Op de kleur van de letters

Is deze website aan de hand van de URL betrouwbaar? http://www.de.telegraav.com

- Ja
- Nee

Is deze website aan de hand van de URL betrouwbaar? https://www.youtube.com ?

- Ja
- Nee

Is deze website aan de hand van de URL betrouwbaar? https://www.netflx.com ?

- Ja
- Nee

Bankhelpdeskfraude

Les 4: Wat is bankhelpdeskfraude?

Gefeliciteerd, je hebt het onderdeel over phishing nu af. De komende drie lessen gaan we het hebben over wat bankhelpdeskfraude is. Bankhelpdeskfraude is een bekende vorm van fraude. Mensen doen zich voor als iemand die voor een bank werkt om zo geld van je te kunnen stelen. Dit doen ze door gebruik te maken social engineering. Dit klinkt misschien moeilijk maar het betekend dat mensen jouw emoties zoals vertrouwen en angst misbruiken. De nepmedewerker van de bank belt je op en zegt dat je geld in gevaar is. Vervolgens willen ze je helpen door het geld vaar een 'veilige rekening' over te maken. Het kan ook zijn dat de nepmedewerker aangeeft dat uw bankpas onveilig is en zal worden opgehaald. Kortom, iemand belt u op en doet zich voor als een bankmedewerker die op verschillende manieren u geld wilt hebben. In de volgende les ga je leren hoe je bankhelpdeskfraude kan herkennen. Heel veel succes.

Les 5: Hoe herken ik het?

Daar ben ik weer. Nu je weet wat bankhelpdeskfraude is gaan we het leren herkennen. Dit bestaat uit best veel onderdelen dus let goed op! We beginnen met het gebeld worden; Op het moment dat je niet verwacht dat je gebeld gaat worden door de bank is het al gelijk verdacht. Een bank belt u nooit uit het niets. Op het moment dat de bankwedewerker begint over dat er fraudeurs geld van je rekening proberen te halen gaat er nog een alarmbel af. De medewerker vraagt u om op een gestuurde link te klikken om uw geld naar een veilige kluisrekening over te maken. Dit vertrouwt u ook niet omdat u ziet dat het geen betrouwbare link is. De bankmedewerker vraagt u iets op uw computer te zetten omdat hij dat even met u mee kan kijken. Dit vertrouwt u niet omdat u niet zomaar iemand toegang geeft tot uw computer. Het kan ook zijn dat u via een sms een link krijgt van de bank omdat uw geld in gevaar is; ook dit zal een bank nooit doen. Trap hier dus niet in. In het volgende onderdeel ga je leren wat je hier tegen kunt doen. Heel veel succes met het maken van de vragen.

Vragen:

Wat zal een bank nooit vragen om te doen?

- Je betaalpas opsturen
- Je betaalpas meenemen
- Je pincode vragen
- Via een specifieke link laten inloggen op internetbankieren
- Iets laten downloaden zodat ze kunnen mee kijken met je telefoon
- Je geld over te maken naar een kluisrekening
- Je pincode geven.

Les 6: kan je er wat tegen doen?

Daar ben ik weer. Nu je weet wat een bank je nooit zal vragen is het goed om te weten of je hier niet iets tegen kan doen. Het antwoord op deze vraag nee, nou ja; bijna nee. Het kan iedereen overkomen dat je gebeld wordt door een oplichter die zich voordoet als een bankmedewerker. Ook kan het iedereen overkomen dat je een sms'je krijgt wat niet echt van je bank is. Je kan wel goed controleren of het wel echt is met alle tips die we je hebben gegeven. Het kan zijn dat er op het moment van opnemen de naam van u bank ik beeld staat, dit betekend automatisch dat het echt de bank is, fraudeurs kunnen dit nadoen. Als je het niet helemaal vertrouwt dat je bank je belt kan je altijd zeggen dat je zelf even terug belt. De bank vind dit niet erg en raden dit ook aan op hun websites. Op deze manier kan je zelf het echte telefoonnummer van je bank bellen en vervolgens je vragen stellen. Ook als je een mailtje of sms'je niet helemaal vertrouwd kunt u naar uw bank bellen om te vragen of de mail of sms van de bank is. Op het moment dat u ontdekt dat iemand een fraudeur is hang gelijk de telefoon op en meld het bij uw bank. Dit kan vaak via de website en anders kunt u altijd bellen. Succes met het maken van de opgaven.

Vragen:

Is het uw schuld als u wordt gebeld door een fraudeur?

- Ja
- Nee

Iemand van de bank belt maar u vertrouwd het niet helemaal, wat doet u nu?

- Ik hang het gesprek op en bel zelf de bank terug
- Ik volg precies de stappen van de medewerker van de bank
- Ik hang in paniek op,

Er komt iemand bij de deur die zegt dat hij van de bank is en uw bankpas komt ophalen omdat uw bankpas onveilig is, wat doet u?

- Ik geef hem mijn bankpas en pincode
- Ik geef hem mijn bankpas
- Ik doe de deur dicht
- Ik vraag of hij kan bewijzen dat hij van de bank is
- Ik nodig heb binnen uit omdat ik ook nog een vraag over internetbankieren had

U krijgt een sms'je van de bank waarin staat dat uw geld in gevaar is en dat u via de link in het sms'je het geld kunt veilig stellen, wat doet u?

- Ik bel de bank om te vragen of het sms'je wel echt van de bank komt
- Ik klik op de link om te kijken wat het is
- Ik verwijder het bericht omdat het er net uitziet en meld dit bij de bank
- Ik bel het telefoonnummer wat bij het sms'je staat om te vragen of het wel echt is

Outro video:

Nu we aan het einde van deze courses zijn gekomen hopen wij dat je nu hebt geleerd wat phishing en bankheldeskfraude is en hoe je jezelf hiertegen kan beschermen. Heel veel veilige uren op het internet gewenst.