Val niet voor vals: Activiteit 1

Bijt niet in de phishinghaak!

Een spel waarbij leerlingen verschillende teksten en e-mails bestuderen en proberen uit te maken welke de echte en valse phishingberichten zijn.

Doelstellingen

- ✓ **De technieken leren** die mensen gebruiken om je identiteit te stelen.
- ✓ **Bekijken** hoe je identiteitsdiefstal voorkomt.
- ✓ **Leren** praten met een vertrouwde volwassene als je denkt dat iemand je gegevens heeft gestolen.
- ✓ De tekenen van een phishingpoging **herkennen**.
- ✓ **Voorzichtig** zijn met hoe en met wie ze persoonlijke informatie delen.

Even praten

Wat is phishing nu eigenlijk?

Phishing gebeurt wanneer iemand informatie probeert te stelen - zoals je login- of accountgegevens - door zich voor te doen als iemand die je vertrouwt in een e-mail, sms of andere onlinecommunicatie. Phishing-e-mails - en de onveilige sites waar ze je naartoe proberen te sturen of de downloads en bijlagen die ze jou proberen te doen openen - kunnen ook virussen op je computer plaatsen die je contactenlijst gebruiken om je vrienden en familie nog meer phishing-e-mails te sturen.

Andere oplichters proberen je te misleiden om malware of ongewenste software te downloaden door je te vertellen dat er iets fout is met je toestel. Let op: een website of advertentie kan onmogelijk zeggen of er iets fout is met je toestel! Sommige phishingaanvallen zijn duidelijk nep. Maar andere kunnen echt lijken en overtuigend zijn. Stuurt een oplichter jou bijvoorbeeld een bericht waarin enkele van je persoonlijke gegevens vermeld staan, dan noemen we dit spearphishing en trap je er misschien wel in.

Het kan heel moeilijk zijn om dit te herkennen, want door je eigen informatie te gebruiken, kan het lijken alsof ze jou echt kennen. Voor je op een link klikt of je paswoord invoert op een site die je nooit eerder hebt bezocht, is het goed jezelf enkele vragen te stellen over die e-mail of webpagina. Deze vragen kun je jezelf stellen:

- Ziet de site er even professioneel uit als andere websites die je kent en vertrouwt, met het gebruikelijke logo van het product of het bedrijf en met tekst zonder spelfouten?
- Stemt de URL van de site overeen met de naam van het product of het bedrijf dat je zoekt? Staan er spelfouten in?
- Zijn er spamachtige pop-ups?
- Begint de URL met https:// met aan de linkerkant een groen hangslotje? (dit betekent dat de verbinding veilig is.)

Vervolg op de volgende pagina →

- Wat staat er in de kleine lettertjes? (Dat is waar het gevaar in schuilt.)
- Biedt de e-mail of site iets aan dat te mooi is om waar te zijn, zoals de kans om veel geld te winnen? (Het is bijna altijd te mooi om waar te zijn.)
- Klinkt de boodschap een beetje vreemd? Alsof ze je kennen, maar je bent toch niet helemaal zeker?

En wat als je toch in de val trapt? Eerst en vooral: geen paniek!

- Vertel het meteen aan een ouder, je leerkracht of een andere volwassene die je vertrouwt. Hoe langer je wacht, hoe erger de dingen kunnen worden.
- Verander de paswoorden van je online-accounts.
- Word je het slachtoffer van oplichters, vertel het dan meteen aan je vrienden en andere contacten, want zij kunnen ook getroffen worden.
- Gebruik de instellingen om het bericht indien mogelijk te melden als spam.

Activiteit

Wat je nodig hebt:

- Hand-out: werkblad "Phishingvoorbeelden"

Antwoorden op het werkblad "Phishingvoorbeelden":

1. **Echt.** De e-mail vraagt de gebruiker naar de website van het bedrijf te surfen en in te loggen op hun account, in plaats van een link te geven in de e-mail of hen te vragen hun paswoord te mailen (links kunnen gebruikers naar twijfelachtige websites loodsen).
2. **Nep.** Verdachte en geen beveiligde URL.
3. **Echt.** Let op de https:// in de URL.
4. **Nep.** Verdacht aanbod in ruil voor bankgegevens.
5. **Nep.** Niet veilig en verdachte URL.

1. Bestudeer enkele voorbeelden

Laat uw kinderen deze voorbeelden van berichten en websites bestudere.

2. Geef keuzes aan

Selecteer "Echt" of "Nep" voor elk voorbeeld en zeg daaronder waarom.

3. Bespreek de keuzes

Welke voorbeelden lijken betrouwbaar en welke lijken verdacht?
Hebben sommige antwoorden je verrast?

4. Verdere discussie

Dit zijn enkele vragen die je jezelf kan stellen bij het beoordelen van berichten en sites die je online vindt:

- **Ziet dit bericht er goed uit?**
  Wat is je eerste indruk? Vallen jou onbetrouwbare aspecten op?

- **Biedt de e-mail jou iets gratis aan?**
  Gratis aanbiedingen zijn meestal niet echt gratis (ook al is het echt).

- **Vraagt het bericht je persoonlijke gegevens?**
  Sommige websites zullen jou persoonlijke informatie vragen, zodat ze jou nog meer bedrieglijke berichten kunnen sturen. Bijvoorbeeld een 'persoonlijkheidstest' waarin je informatie prijsgeeft op basis waarvan je paswoord of andere geheime informatie makkelijker kunnen raden. De meeste echte bedrijven zullen geen persoonlijke informatie via e-mail vragen.

- **Is het een kettingmail of post op sociale media?**
  E-mails en posts die je vragen iets door te sturen naar iedereen die je kent, kunnen jou en anderen in gevaar brengen. Doe het niet, tenzij je zeker bent van de bron en zeker weet dat je het bericht veilig kan doorgeven.

Vervolg op de volgende pagina →

- **Lees de kleine lettertjes**
  Onderaan de meeste documenten vind je de kleine lettertjes. Deze tekst is klein en bevat vaak de dingen waarvan ze willen dat je ze over het hoofd ziet. Een kop bovenaan de tekst vertelt bijvoorbeeld dat je een gratis telefoon hebt gewonnen, maar in de kleine lettertjes staat dat je dat bedrijf eigenlijk 200 euro per maand moet betalen.

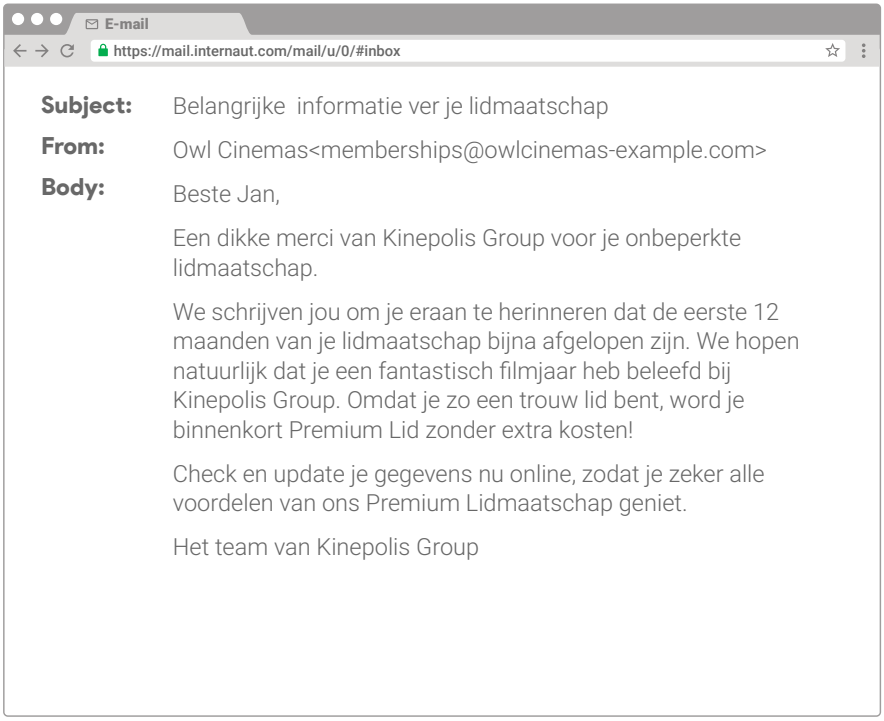
Opmerking: in deze oefening gaan we ervan uit dat 'Internaut Mail' een echte, vertrouwde service is.

Lessen

Ben je online, wees dan altijd op je hoede voor phishingaanvallen in e-mails, sms-berichten en posts - en zorg ervoor dat je de juiste mensen hierover aanspreekt als iemand je voor de gek houdt.

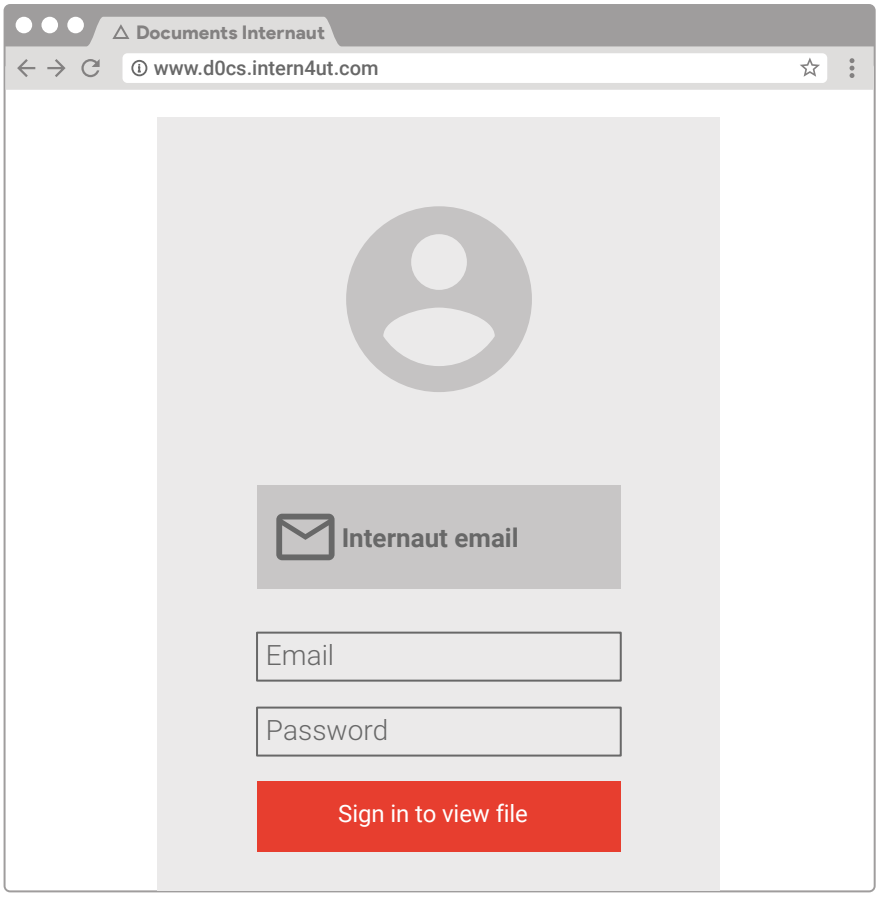
Werkblad: Activiteit 1

Voorbeelden van phishing



1. Is dit echt of nep?

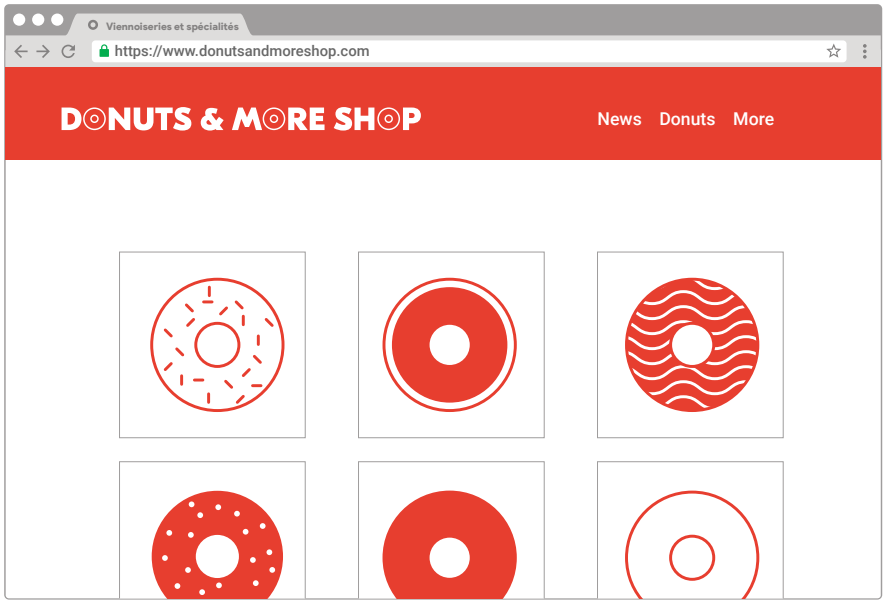
.....



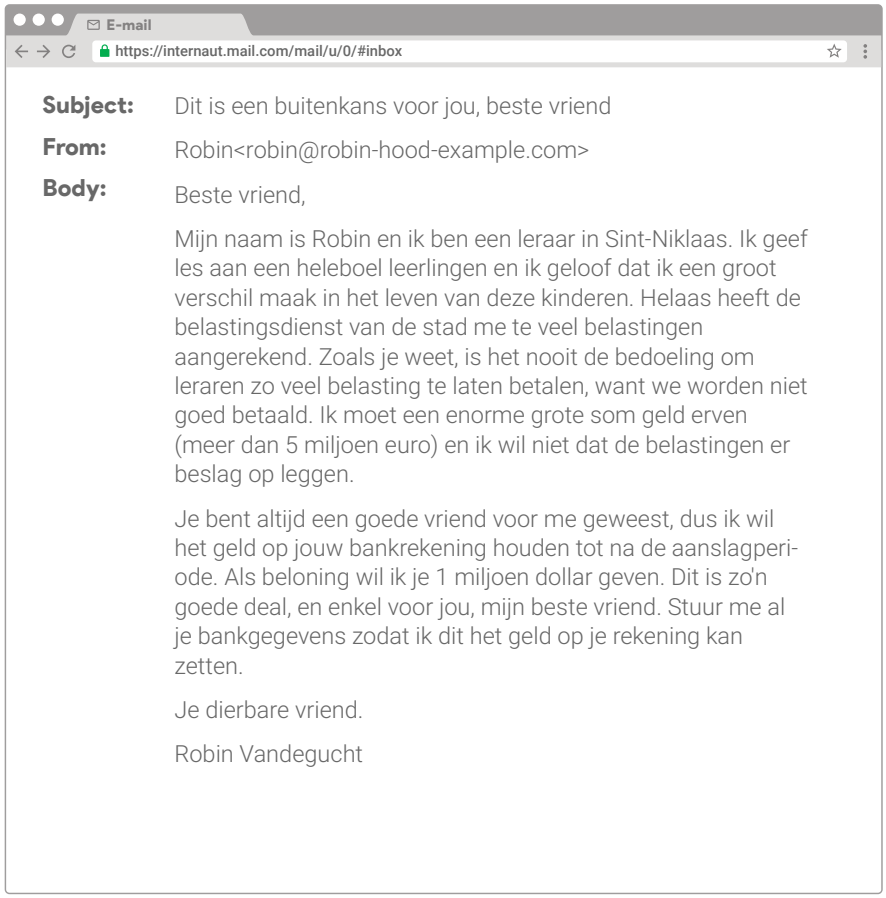
2. Is dit echt of nep?

.....

Vervolg op de volgende pagina →



3. Is dit echt of nep?



4. Is dit echt of nep?

Vervolg op de volgende pagina →

5. Is dit echt of nep?