**Lesontwerp: Awareness Cyber Security & Privacy tijd: 45 min.**

|  |  |
| --- | --- |
| **Doelstelling**  Phishing  Na deze les weten medewerkers en studenten voldoende waaraan ze een phishingmail kunnen herkennen en hoe ze moeten handelen.  Omgaan met data  Na deze les weten medewerkers beter hun verantwoordelijkheid als het aankomt op de  bescherming van persoonlijke gegevens van (toekomstige) studenten en medewerkers.  Wachtwoordgebruik  Na deze les weten medewerkers en leerlingen hoe ze een sterk wachtwoord moeten maken en gebruiken. | **Doelgroep**  • Studenten  Het is onduidelijk hoeveel kennis zij bezitten over de verschillende onderwerpen. Veel van hen zijn waarschijnlijk niet op de hoogte van het privacy- en securitybeleid van onze school.  • Onderwijzend personeel  We verwachten dat ze in enige mate bekend zijn met het privacy- en securitybeleid van de instelling. Onderwijzend personeel heeft veel te maken met persoonlijke gegevens en bestanden van studenten. Denk aan cijferlijsten, examens, verslagen e.d. Veilig omgaan met data en documenten vereist extra aandacht.  • Niet-onderwijzend personeel  We verwachten dat ze in enige mate bekend zijn met het privacy- en securitybeleid van de instelling. Ook niet-onderwijzend personeel heeft te maken met bestanden die vertrouwelijke informatie bevatten, zoals persoonsgegevens met vertrouwelijke informatie voor de instelling.  Veilig omgaan met data vereist om die reden extra aandacht. |
| **Instructie Tijdsduur: 45 min**  *Terugblik:* Bespreken van het voorgaande werk/Voorgaande les: Waar ging het de vorige keer over?  *Voorkennis activeren* van het lesonderwerp  *Doel van de les* benoemen en waarom gaan we dit leren?  *Lesopbouw:* hoe ziet de les er uit? *Instructie op lesinhoud:* | Geen terugblik. Unieke les.    Starten met powerpoint met daarin filmpje  [https://www.youtube.com/watch?v=F7pYH...](https://www.youtube.com/watch?v=F7pYHN9iC9I) Duur: 2 min 20 sec  Inleiding.   * 5 min: Filmpje 2 min 20 Bespreken. Wat zie je. Herken je dit? * Doel van de les om beter om te gaan met phishing mails, je persoonlijke data en met wachtwoorden. * 30 min: Instructie dmv ppt   + Opdrachten uitvoeren gedurende presentatie:   <https://howsecureismypassword.net/>   * + Voorbeelden phishing mail.   <https://haveibeenpwned.com/>   * + Surf filesender uitvoeren   + Kort instructie over AVG en privacy |
| **Evaluatie Tijdsduur:** Les evalueren met studenten op inhoud. Refereren aan genoemde doelen van begin van de les. Hebben wie die behaald?  Docent evalueert voor zichzelf de les en neemt bevindingen mee naar de volgende les. | * 10 min: Afsluiting |
|  |  |

**Doel:**

In 2020 moeten met het awareness-programma de volgende doelen zijn bereikt:

• Studenten en medewerkers zijn op de hoogte van de gevaren van phishingaanvallen. Gebruikers weten wat phishing is, waaraan ze een phishingaanval kunnen herkennen en hoe ze moeten handelen op het moment dat ze met een phishingaanval te maken krijgen.

• Medewerkers weten hoe ze zorgvuldig met de opslag van data moeten omgaan en handelen hiernaar.

• Studenten en medewerkers zijn zich bewust van het belang van sterke wachtwoorden. Ze weten hoe ze een sterk wachtwoord moeten instellen en doen dat ook.

**Aanleiding:**

Phishing

Er heerst te weinig bewustzijn rondom de gevaren van phishing. Medewerkers en studenten weten onvoldoende waaraan ze een phishingmail kunnen herkennen en hoe ze moeten handelen wanneer ze geconfronteerd worden met een phishingmail.

Omgaan met data

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming van toepassing.

Dat betekent extra verantwoordelijkheden voor medewerkers als het aankomt op de bescherming van persoonlijke gegevens van (toekomstige) studenten en medewerkers.

Uit het onderzoek blijkt echter dat medewerkers niet zorgvuldig omgaan met de opslag van data. Er wordt te weinig gebruikgemaakt van de veilige opslagdiensten van de instelling. Data zwerft rond in e-mails, op usb-sticks, of blijft staan op het bureaublad van de desbetreffende medewerker.

Wachtwoordgebruik

Zwakke wachtwoorden veroorzaken regelmatig datalekken. Idealiter zijn wachtwoorden uniek, lang en bestaan ze uit symbolen, cijfers, letters en hoofdletters. In slechts 15% van de gevallen voldoet een wachtwoord aan bovenstaande eisen. Bovendien zien we dat wachtwoorden regelmatig hergebruikt worden.

1. Aan het begin van ieder nieuw studiejaar wordt aan nieuwe studenten en medewerkers informatie uitgedeeld met daarop de contactgegevens van de ICT-helpdesk. Studenten lijken de ICT-helpdesk wel te vinden, maar dat is voornamelijk voor hulp met bijvoorbeeld het installeren van software.

2. Op het moment dat een medewerker in dienst komt van onze school krijgt hij of zij een document toegestuurd met daarin uitleg over hoe binnen onze instelling met data om te gaan. We zien echter dat er met enige regelmaat data zoekraakt, dat docenten veel gebruikmaken van usb-sticks en dat Dropbox en WeTransfer door veel van hen gebruikt worden. Gedrag dat we liever niet terug zouden zien.

**Concreet**

Concreet willen we met het programma in 2020 de volgende gedragsdoelen hebben bereikt:

Phishing

• Op het moment dat er een phishingmail binnenkomt weten onze medewerkers en studenten waaraan ze deze kunnen herkennen.

• Op het moment dat er een phishingmail binnenkomt melden onze medewerkers en studenten dit direct bij de ICT-helpdesk.

• Nadat studenten en medewerkers de phishingmail gemeld hebben bij de ICT-helpdesk verwijderen ze deze permanent uit hun inbox.

Veilig omgaan met data

• Op het moment dat medewerkers data op moeten slaan weten ze hoe én waar ze dit moeten doen (op beveiligde servers).

• Op het moment dat medewerkers data moeten delen weten ze hoe ze dit op een veilige manier kunnen doen (via beveiligd systeem/SURFdrive bijvoorbeeld).

• Op het moment dat medewerkers data op een onveilige manier toegestuurd krijgen van een collega spreken ze hem/haar daarop aan.

Wachtwoorden

• Op het moment dat medewerkers en studenten hun wachtwoord aanpassen weten ze aan welke eisen een wachtwoord moet voldoen om veilig te zijn.

• Medewerkers en studenten maken gebruik van tweefactor-authenticatie waar mogelijk.

• Medewerkers en studenten zijn op de hoogte van de mogelijkheid om een wachtwoordmanager te gebruiken