Instructie 'Hoe ga ik om met gevoelige bestanden zoals tentamens?'

Wat is er aan de hand?
Bij Avans Hogeschool zijn meerdere zogenaamde keyloggers gevonden op smartboard computers.
Een keylogger is een apparaatje dat tussen de computer en de toetsenbordkabel wordt geplaatst en dat onmerkbaar alle ingevoerde toetsaanslagen opslaat.
Een keylogger is makkelijk te gebruiken en het apparaatje is alleen visueel te ontdekken.
De fraudeur kan de keylogger later op een computer uitlezen en ziet dan alle toetsaanslagen van de gebruiker(s). Denk aan inlog pagina('s), gebruikte accountnaam(-namen) en wachtwoord(en) van Avans en privé bezochte sites.

Hoe herken je een keylogger?
Een keylogger ziet eruit als een USB- stick. In plaats van één USB- poort hebben ze een tweede poort aan de achterkant. Dat komt omdat het apparaatje tussen de computer en de toetsenbord kabel geplaatst wordt. Kijk dus hoe de kabel van het toetsenbord is aangesloten.
Keyloggers zien er zo uit:

Meer voorbeelden van typen keylogger: https://www.keelog.com/keylogger_comparison.html

Waar is de fraudeur op uit?
In het onderwijs zijn vooral tentamengegevens interessant of plaatsen waar je tentamenresultaten kunt invoeren.

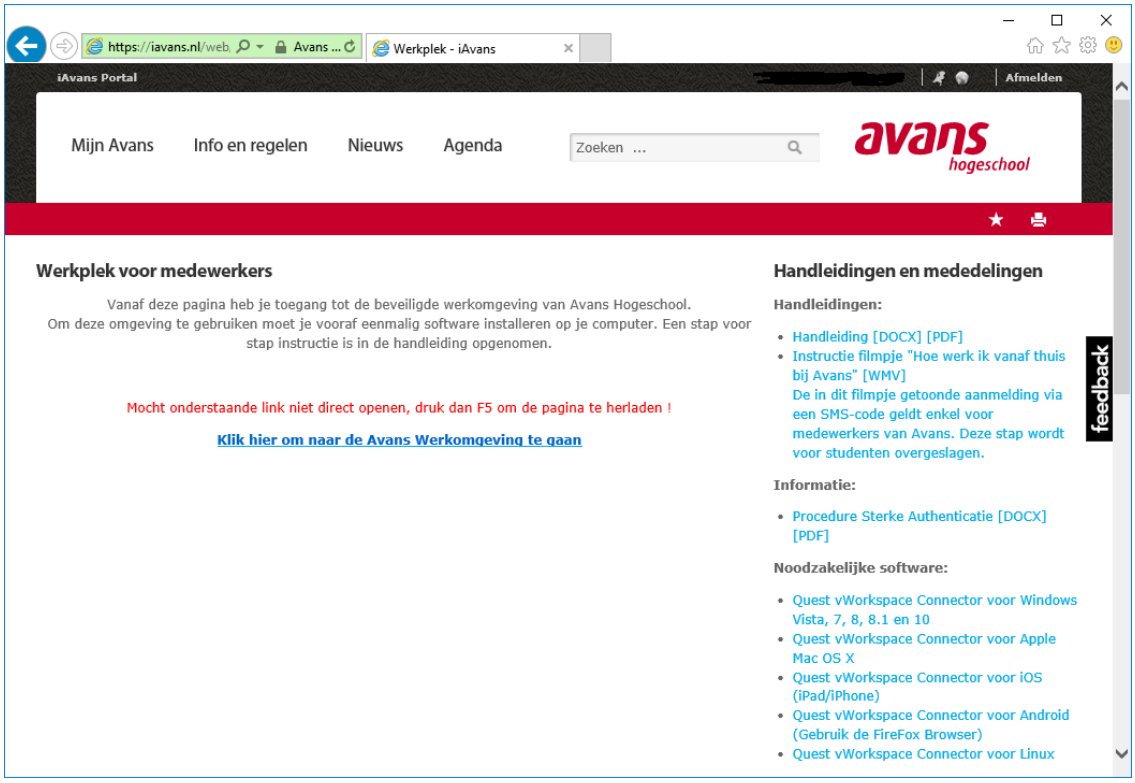
Waarom zijn vooral Smartboard computers gevaarlijk?
Een fraudeur kan heel eenvoudig de gegevens van een specifieke docent achterhalen. In de roosters is te zien waar en wanneer een docent aanwezig is en op welke pc hij/zij inlogt. De fraudeur moet dus op die specifieke pc de keylogger plaatsen.

Welk gevaar dreigt?
Identiteitsfraude: de fraudeur doet zich voor als iemand anders en heeft op basis daarvan ongemerkt toegang tot diverse Avans- en privé gebruikte systemen.

Wat niet te doen
Gebruik geen e-mail, Home drive of Xythos om (concept)tentamens of andere gevoelige bestanden uit te werken of uit te wisselen. Deze omgevingen zijn hiervoor niet veilig genoeg.

Wat dan wel?
Gebruik de AVANS 'Werkplek voor medewerkers' omgeving hiervoor. Zie de afbeelding hieronder. Deze is te vinden via: iAvans, Info en regelen, Werkplek. Een fraudeur krijgt daar geen toegang toe omdat dit systeem extra beveiligd is met een sms-code.

Je krijgt de beschikking over een computerscherm dat lijkt op de standaard Avanswerkomgeving. Plaats bestanden op de gedeelde groepsschijven (O:, R:, S: en U:) van je academie of dienst. Daar staan ze veilig.



Wat kun je zelf doen om:

A) Je inloggegevens te beschermen?

Als dat mogelijk is controleer dan in publiek toegankelijke ruimtes en vooral in Smartboard lokalen altijd de computer die je wilt gebruiken op keyloggers. Vind je een keylogger op een pc, bel dan direct de Avans servicelijn 088 – 525 8888.
Tip: ben je in het bezit van een door Avans beheerde notebook? Gebruik deze dan in plaats van de aanwezige vaste computer om het smartboard aan te sturen.

B) Je bestanden te beschermen?

Plaats je bestanden op de juiste plek:

- Niet vertrouwelijke documenten kun je op je Homedrive (H:) of Xythos plaatsen.
- Vertrouwelijke bestanden, zoals (concept)tentamens, bestanden met persoonsgegevens, horen thuis op de gedeelde schijf van je Academie of Dienst (O:, R:, S:en U:) en dus niet op je Homedrive (H:) of Xythos .
- Lock je vaste werkplek of notebook wanneer je deze verlaat. Dit kan met de sneltoets (+L).

Waarom kan ik mijn bestanden niet gewoon overal plaatsen?

- Omdat een fraudeur met jouw wachtwoord (naast keyloggers zijn daar ook andere manieren voor) onopgemerkt toegang binnen en buiten Avans kan krijgen tot je bestanden wanneer alleen een wachtwoord nodig is voor de toegang.
  Denk aan Homedrive: e-mail, Xythos, Home drive, Osiris- docent, Blackboard, Mijn HR, … maar ook aan niet Avansomgevingen zoals Dropbox en dergelijke.

- Wanneer je je bestanden op de gedeelde schijf van je academie of dienst (O:, R:, S:en U:) zet:
  - dan zijn deze bestanden op een standaard vaste werkplek alleen toegankelijk met een wachtwoord binnen de Avansmuren én binnen de medewerkersdomeinen/- ruimtes.
  - en je hebt een managed notebook van Avans dan zijn de bestanden binnen de muren van Avans altijd beschikbaar op dat notebook. Bij vermissing van een notebook moet meteen de helpdesk/servicedesk gewaarschuwd worden.
- Ook andere Avanssystemen, waarvoor je een sms- code of een code via een app nodig hebt voor toegang (zoals Corsa en binnenkort Remindo toets), zijn veilig. Buiten de medewerkersdomeinen en via internet kun je daar nog steeds bij. Toegang daarvoor krijg je alleen met de extra authenticatie(code). En daar kan een fraudeur niet over beschikken.

Wat gaat DIF doen?
DIF treft zo snel mogelijk technische maatregelen zodat het niet meer mogelijk is om het toetsenbord los te maken en er een apparaat tussen te plaatsen. Dit vergt nog wat onderzoek en ook de uitvoering hiervan zal nog wat tijd in beslag nemen.