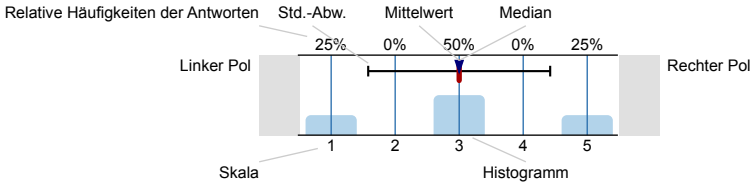
pMOOCs2
WS19/20
Digitaler Selbstschutz ()
Erfasste Fragebögen = 289

Auswertungsteil der geschlossenen Fragen

Legende

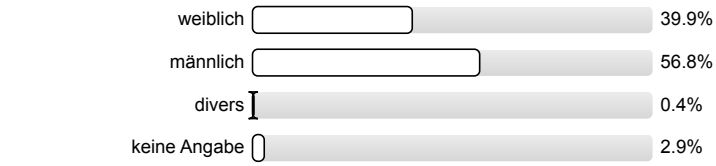
Fragetext



n=Anzahl
mw=Mittelwert
md=Median
s=Std.-Abw.
E.=Enthaltung

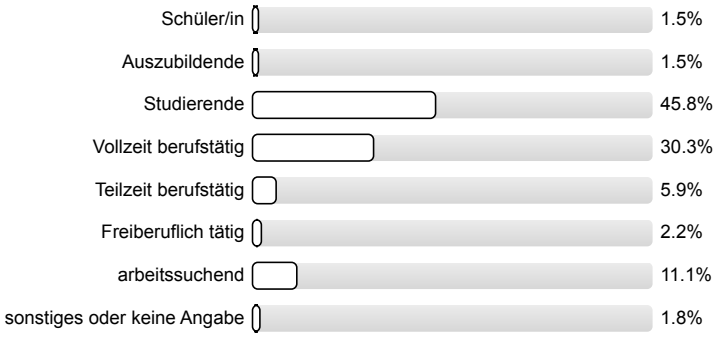
1. Demographische Daten - (Bitte entschuldige, wenn sich die Fragen in diesem Teil mit denen aus der Befragung zu Beginn des Kurses wiederholen. Wie versprochen handelte es sich hierbei um eine anonyme Befragung, sodass wir nicht auf Deine Antworten aus der ersten Befragung zurückgreifen können.)

1.1) **Geschlecht** - Du bist...



n=273

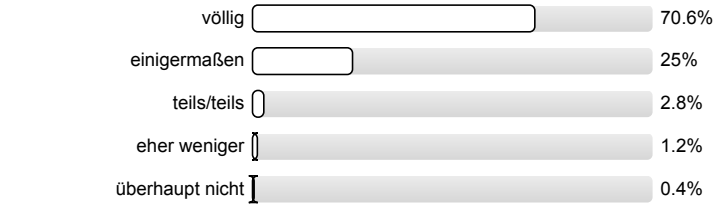
1.4) Was ist Dein beruflicher Hintergrund?



n=271

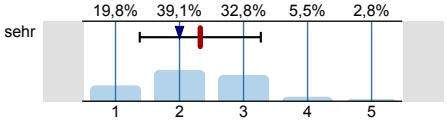
2. Lernen mit und im MOOC

2.2) **Zielrreichung** - Wie sehr konntest Du die Ziele erreichen?



n=248
mw=1,4
s=0,6

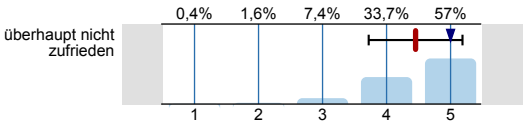
2.4) **Vergleich zu anderen Angeboten** - Wie sehr unterscheidet sich Ihr Lernverhalten im MOOC im Vergleich zum traditionellen Lernen (Schulungen, Seminare, Vorlesungen, etc.)?



n=253
mw=2,3
md=2
s=0,9

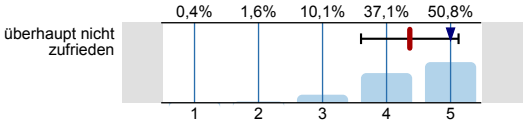
3. Gestaltung des Kurses

3.1) ...mit dem Aufbau des Kurses?



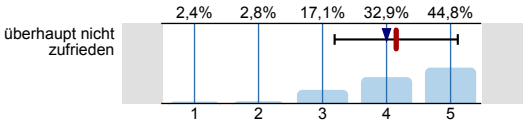
n=258
mw=4,5
md=5
s=0,7
E.=4

3.2) ...mit der Gesamtorganisation?



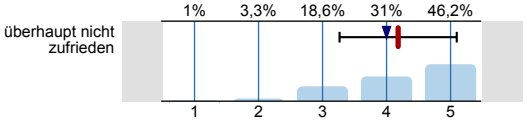
n=248
mw=4,4
md=5
s=0,8
E.=13

3.3) ...mit dem benötigten Zeitaufwand im Vergleich zum angegebenen Umfang?



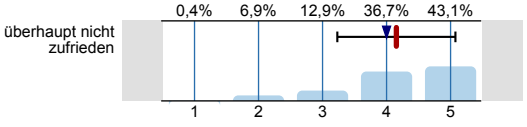
n=252
mw=4,2
md=4
s=1
E.=9

3.4) ...mit der Betreuung im Kurs?



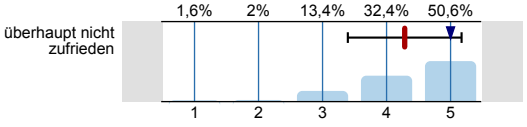
n=210
mw=4,2
md=4
s=0,9
E.=50

3.5) ...mit dem wissenschaftlichen Niveau der Lerninhalte?



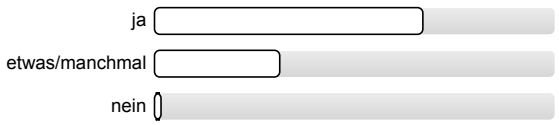
n=248
mw=4,2
md=4
s=0,9
E.=10

3.6) ...mit dem Aufgabenformat?



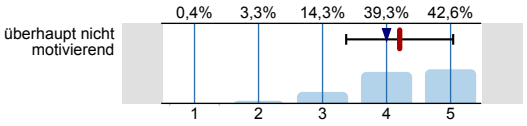
n=247
mw=4,3
md=5
s=0,9
E.=7

3.7) **Motivation -** Hast Du Dich auf das nächste Kapitel gefreut?



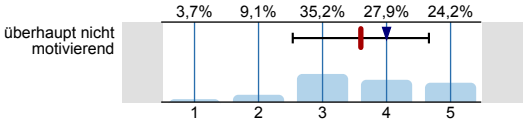
n=246

3.8) die Inhalte im Kurs



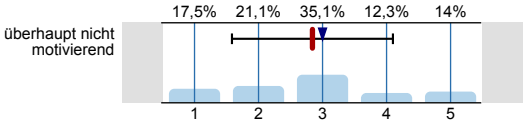
n=244
mw=4,2
md=4
s=0,8
E.=11

3.9) die Benachrichtigung zum Kapitelstart



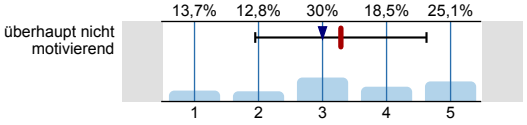
n=219
mw=3,6
md=4
s=1,1
E.=35

3.10) die Diskussionen mit anderen Teilnehmenden im Forum



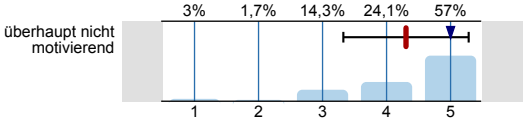
n=171
mw=2,8
md=3
s=1,3
E.=83

3.11) die Badges



n=227
mw=3,3
md=3
s=1,3
E.=24

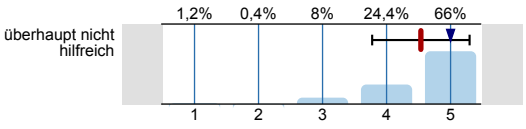
3.12) das Zertifikat am Ende des Kurses



n=237
mw=4,3
md=5
s=1
E.=19

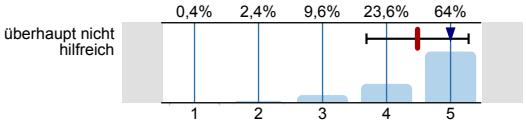
4. Eingesetzte Medien und Plattform

4.1) ...die Videos?



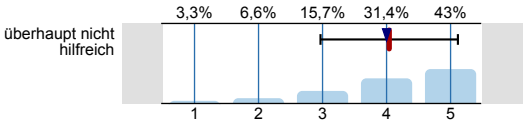
n=250
mw=4,5
md=5
s=0,8
E.=5

4.2) ...die Quizfragen?



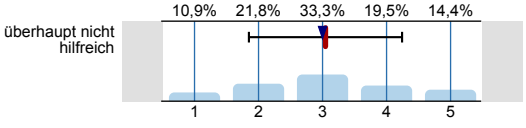
n=250
mw=4,5
md=5
s=0,8
E.=6

4.3) ...die Umfragen?



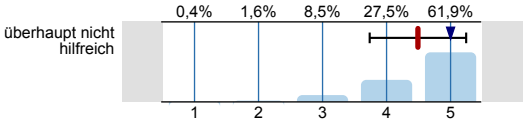
n=242
mw=4
md=4
s=1,1
E.=12

4.4) ...das Forum und die Diskussionen dort?



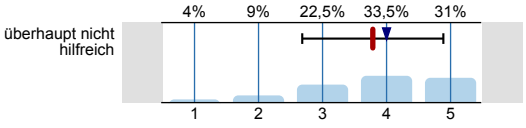
n=174
mw=3
md=3
s=1,2
E.=79

4.5) ...die Praxisbeispiele?



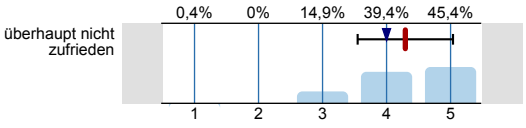
n=247
mw=4,5
md=5
s=0,8
E.=5

4.6) ...die Reportaufgaben?



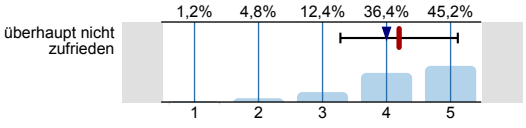
n=200
mw=3,8
md=4
s=1,1
E.=54

4.7) ...mit der oncampus-Plattform insgesamt?



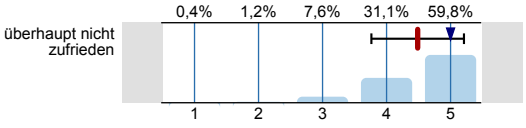
n=249
mw=4,3
md=4
s=0,7
E.=8

4.8) ...mit der Navigation im Kurs?



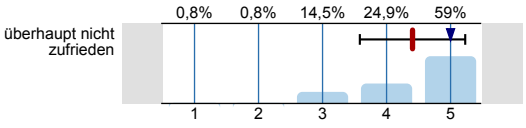
n=250
mw=4,2
md=4
s=0,9
E.=5

4.9) ...mit der (technische) Qualität der Videos?



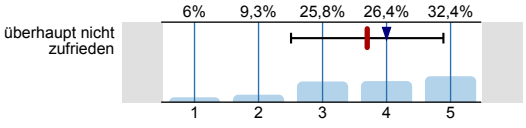
n=251
mw=4,5
md=5
s=0,7
E.=5

4.10) ...mit der Länge der Videos?



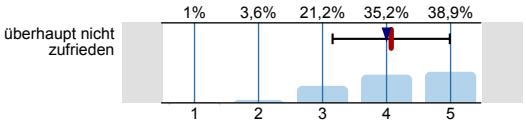
n=249
mw=4,4
md=5
s=0,8
E.=5

4.11) ...mit der offenen Teilnahmeliste und -karte?



n=182
mw=3,7
md=4
s=1,2
E.=69

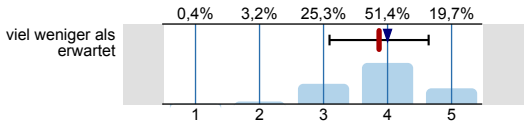
4.12) ...mit den Interkationsmöglichkeiten innerhalb des MOOCs?



n=193
mw=4,1
md=4
s=0,9
E.=54

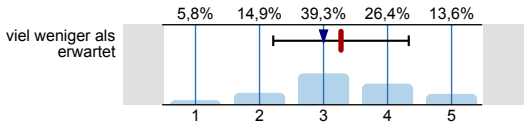
5. Dein persönliches Fazit zu diesem MOOC

5.1) Lernfortschritt, den Du mit dem MOOC erreicht hast



n=249
mw=3,9
md=4
s=0,8
E.=6

5.2) Zeit, die Du für den MOOC aufgewendet hast



n=242
mw=3,3
md=3
s=1,1
E.=12

5.3) **Konsequenzen** - Zu Beginn des MOOCs haben wir Dich nach Deiner Einschätzung gefragt, wie umfangreich Du die Möglichkeiten zum Selbstschutz einschätzt. Wie sieht Deine Meinung dazu nun, nachdem Du diesen MOOC bearbeitet hast, aus? Ist sie gleichgeblieben oder hat sich etwas geändert?

n=247

gleich geblieben	36.8%
umfangreicher: Ich sehe jetzt viel mehr Möglichkeiten für eigene Schutzmaßnahmen.	61.5%
geringer: Ich sehe doch weniger Möglichkeiten als erhofft.	1.6%

5.8) **Kursumfang** - Zum Kurs "Digitaler Selbstschutz 1" gibt es zwei weitere Kurse, die sich mit Daten und Geräten sowie dem Netz befassen. Wie findest Du die Kursaufteilung in kleinere Einheiten?

n=234
mw=1,1
s=0,2

Ich finde eine Aufteilung in kleinere Einheiten gut.	93.6%
Ich hätte lieber einen großen Kurs mit allen Inhalten gehabt.	6.4%

5.9) **Weitere MOOCs** - Denkst Du, dass Du an weiteren MOOCs teilnehmen wirst?

n=230
mw=1,7
s=1,1

ja	54.3%
ja, innerhalb der Digitaler-Selbstschutz-Kurse	37.4%
ja, aber nicht auf oncampus.de	0.4%
nein	0.4%
kann ich nicht einschätzen	7.4%

5.11) **Anrechenbarkeit** - Beabsichtigst Du, Dir die MOOC-Teilnahme in irgendeiner Form anrechnen zu lassen?

n=232

ja, ich bearbeite den Kurs im Rahmen meines Studium an der VFH	45.7%
ja, ich fertige die Reports an und plane, sie zur Beurteilung einzureichen	13.4%
ja, ich fertige keine Reports an, aber plane es auf anderem Weg anrechnen zu lassen	4.3%
nein, ich würde gern, allerdings kommen Termin oder andere Bedingungen so für mich nicht in Frage	0.9%
nein, ich habe kein Interesse an einer Anrechenbarkeit	12.1%
ich bin noch unsicher	9.5%
ich würde gern, mir ist aber keine Anrechnungsmöglichkeit bekannt	3%
sonstiges	11.2%

Profillinie

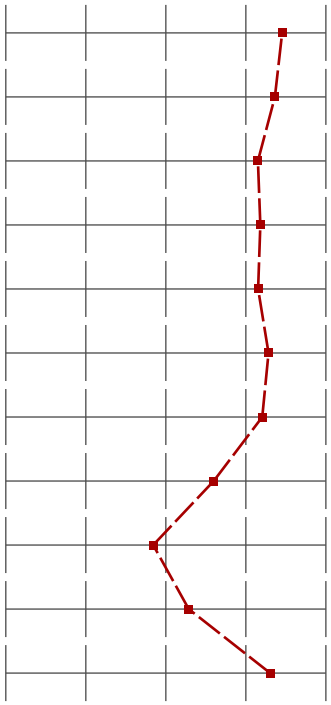
Teilbereich: MOOC
Name der/des Lehrenden: pMOOCs2
Titel der Lehrveranstaltung: (Name der Umfrage) Digitaler Selbstschutz

Verwendete Werte in der Profillinie: Mittelwert

2. Lernen mit und im MOOC

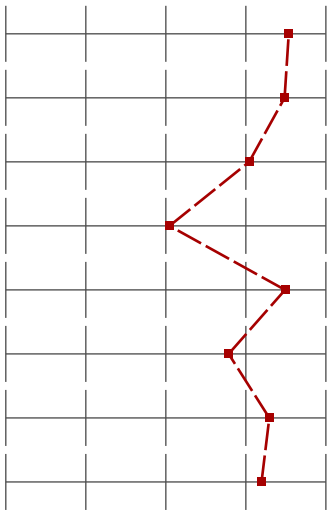
2.4)	**Vergleich zu anderen Angeboten** - Wie sehr unterscheidet sich Ihr Lernverhalten im MOOC im Vergleich zum traditionellen Lernen	sehr	überhaupt nicht	n=253	mw=2,3	md=2,0	s=0,9

3. Gestaltung des Kurses



3.1)	...mit dem Aufbau des Kurses?	überhaupt nicht zufrieden	sehr zufrieden	n=258	mw=4,5	md=5,0	s=0,7
3.2)	...mit der Gesamtorganisation?	überhaupt nicht zufrieden	sehr zufrieden	n=248	mw=4,4	md=5,0	s=0,8
3.3)	...mit dem benötigten Zeitaufwand im Vergleich zum angegebenen Umfang?	überhaupt nicht zufrieden	sehr zufrieden	n=252	mw=4,2	md=4,0	s=1,0
3.4)	...mit der Betreuung im Kurs?	überhaupt nicht zufrieden	sehr zufrieden	n=210	mw=4,2	md=4,0	s=0,9
3.5)	...mit dem wissenschaftlichen Niveau der Lerninhalte?	überhaupt nicht zufrieden	sehr zufrieden	n=248	mw=4,2	md=4,0	s=0,9
3.6)	...mit dem Aufgabenformat?	überhaupt nicht zufrieden	sehr zufrieden	n=247	mw=4,3	md=5,0	s=0,9
3.8)	die Inhalte im Kurs	überhaupt nicht motivierend	sehr motivierend	n=244	mw=4,2	md=4,0	s=0,8
3.9)	die Benachrichtigung zum Kapitelstart	überhaupt nicht motivierend	sehr motivierend	n=219	mw=3,6	md=4,0	s=1,1
3.10)	die Diskussionen mit anderen Teilnehmenden im Forum	überhaupt nicht motivierend	sehr motivierend	n=171	mw=2,8	md=3,0	s=1,3
3.11)	die Badges	überhaupt nicht motivierend	sehr motivierend	n=227	mw=3,3	md=3,0	s=1,3
3.12)	das Zertifikat am Ende des Kurses	überhaupt nicht motivierend	sehr motivierend	n=237	mw=4,3	md=5,0	s=1,0

4. Eingesetzte Medien und Plattform



4.1)	...die Videos?	überhaupt nicht hilfreich	sehr hilfreich	n=250	mw=4,5	md=5,0	s=0,8
4.2)	...die Quizfragen?	überhaupt nicht hilfreich	sehr hilfreich	n=250	mw=4,5	md=5,0	s=0,8
4.3)	...die Umfragen?	überhaupt nicht hilfreich	sehr hilfreich	n=242	mw=4,0	md=4,0	s=1,1
4.4)	...das Forum und die Diskussionen dort?	überhaupt nicht hilfreich	sehr hilfreich	n=174	mw=3,0	md=3,0	s=1,2
4.5)	...die Praxisbeispiele?	überhaupt nicht hilfreich	sehr hilfreich	n=247	mw=4,5	md=5,0	s=0,8
4.6)	...die Reportaufgaben?	überhaupt nicht hilfreich	sehr hilfreich	n=200	mw=3,8	md=4,0	s=1,1
4.7)	...mit der oncampus-Plattform insgesamt?	überhaupt nicht zufrieden	sehr zufrieden	n=249	mw=4,3	md=4,0	s=0,7
4.8)	...mit der Navigation im Kurs?	überhaupt nicht zufrieden	sehr zufrieden	n=250	mw=4,2	md=4,0	s=0,9

4.9)	...mit der (technische) Qualität der Videos?	überhaupt nicht zufrieden		sehr zufrieden	n=251	mw=4,5	md=5,0	s=0,7
4.10)	...mit der Länge der Videos?	überhaupt nicht zufrieden		sehr zufrieden	n=249	mw=4,4	md=5,0	s=0,8
4.11)	...mit der offenen Teilnahmeliste und -karte?	überhaupt nicht zufrieden		sehr zufrieden	n=182	mw=3,7	md=4,0	s=1,2
4.12)	...mit den Interkationsmöglichkeiten innerhalb des MOOCs?	überhaupt nicht zufrieden		sehr zufrieden	n=193	mw=4,1	md=4,0	s=0,9

5. Dein persönliches Fazit zu diesem MOOC

5.1)	Lernfortschritt, den Du mit dem MOOC erreicht hast	viel weniger als erwartet		viel mehr als erwartet	n=249	mw=3,9	md=4,0	s=0,8
5.2)	Zeit, die Du für den MOOC aufgewendet hast	viel weniger als erwartet		viel mehr als erwartet	n=242	mw=3,3	md=3,0	s=1,1

Auswertungsteil der offenen Fragen

1. Demographische Daten - (Bitte entschuldige, wenn sich die Fragen in diesem Teil mit denen aus der Befragung zu Beginn des Kurses wiederholen. Wie versprochen handelte es sich hierbei um eine anonyme Befragung, sodass wir nicht auf Deine Antworten aus der ersten Befragung zurückgreifen können.)

1.2) **Geburtsjahr** - Bitte verrate uns, wann Du geboren wurdest.

- ++++
- 6.4 (5 Nennungen)
- 1954
- 1957
- 1959 (2 Nennungen)
- 1960 (4 Nennungen)
- 1961
- 1962
- 1964 (2 Nennungen)
- 1965
- 1966 (2 Nennungen)
- 1967
- 1968 (2 Nennungen)
- 1969 (5 Nennungen)
- 1970
- 1971 (2 Nennungen)
- 1972 (3 Nennungen)
- 1973 (3 Nennungen)
- 1974
- 1975
- 1976 (3 Nennungen)
- 1977 (2 Nennungen)
- 1978 (2 Nennungen)
- 1979 (2 Nennungen)
- 1980 (4 Nennungen)
- 1981 (9 Nennungen)
- 1982 (5 Nennungen)
- 1983 (7 Nennungen)
- 1984 (6 Nennungen)
- 1985 (7 Nennungen)
- 1986 (7 Nennungen)
- 1987 (6 Nennungen)
- 1988 (12 Nennungen)
- 1989 (9 Nennungen)

- 1990 (9 Nennungen)
- 1991 (3 Nennungen)
- 1992 (2 Nennungen)
- 1993 (7 Nennungen)
- 1994 (7 Nennungen)
- 1995 (12 Nennungen)
- 1996 (21 Nennungen)
- 1997 (18 Nennungen)
- 1998 (14 Nennungen)
- 1999 (13 Nennungen)
- 2000 (16 Nennungen)
- 2001 (15 Nennungen)
- 2002 (5 Nennungen)
- 2003
- 2004 (2 Nennungen)

1.3) **Land -** In welchem Land wohnst Du?

- ++
- BED
- Baden Württemberg
- Brandenburg
- Burgenland (4 Nennungen)
- D (5 Nennungen)
- DE (2 Nennungen)
- DEutschland
- Deustchland
- Deutschalnd
- Deutschland (200 Nennungen)
- Deutschland - NRW
- Deutschland-Niedersachsen
- Europäische Union
- France
- Marokko
- Ostereich
- Polen
- Schleswig-Holstein
- Schleswig-Holstein, Deutschland
- Schweiz
- Vietnam
- de

- deutschland (6 Nennungen)
- Österreich (29 Nennungen)
- österreich (2 Nennungen)

2. Lernen mit und im MOOC

2.1) **Deine Lernziele** - Welche Zielen hast Du Dir zu Beginn des Kurses gesetzt?

- ++++++++++++++++++++++++++++++
- - Validieren bestehender Kenntnisse über den digitalen Selbstschutz
  - Zusätzliches Wissen, das über den bisherigen Stand hinaus geht
- - Was kann man machen, wenn man die Zugangsdaten anderer Personen kennt (Gefahrenpotential)?
  - Welche Strategien gibt es Zugangsdaten zu schützen?
  - Welche Schutzmöglichkeiten gibt es bei der Nutzung von Hardware zu beachten?
- .
- 100%
- Alle MOOCs vollständig durcharbeiten und mich mit dem Thema gut auseinander setzen
- Alles verstehen.
- An Sicherheit zu gewinnen.
- Auffrischung und Erweiterung von bereits erworbenen Wissen
- Aufgeklärter Umgang mit Passwörten
- Aufmerksamkeit schärfen
- Ausbau des bisherigen Wissensstand und Vertiefung der Thematik
- Ausbildung zu neuen Job suchen
- Bekannte Dinge auffrischen, und noch unbekannte Details lernen.
- Besserer Selbstschutz und eine bessere Selbstreflektion
- Besserer Umgang mit Passwörtern
  Mehr Informieren über Sicherheitsmassnahmen im Internet
- Besserer Umgang mit Sicherheit beim Computer
- Besserer Umgang mit Zugangsdaten
  Besseres Bewusstsein über die Wichtigkeit des Digitalen Selbstschutzes
- Bestehen
- Bewusster mit Daten umgehen zu können
- Bewusstsein schaffen für Gefahren gegenüber der eigenen digitalen Identität und wie man diese effektiv schützen kann.
- Bisheriges WIssen stärken und eventuell neues lernen
- Damit ich mehr über denn Digitalen Selbstschutz erfahre.
- Das Zertifikat erarbeiten
- Datenschutzkenntnisse
- Dem MOOC konzentriert zu folgen
- Den Kurs abzuschließen.
- Den Kurs bestehen und etwas im eigenen Interesse lernen.
- Den Kurs zu bestehen
- Die Grundlagen des digitalen Selbstschutzes zu verinnerlichen und auch bestmöglich umzusetzen.
- Die eigenen Sicherheitsmaßnahmen überprüfen und Mooc-Inhalte Kollegen*innen vermitteln können.

- Digitalen Selbstschutz lernen
- Digitaler Selbstschutz
- Digitaler Selbstschutz, Teilnahmebescheinigung
- Digitaler Selbstschutz, souveräner Umgang mit Zugangsdaten. Ich wollte meiner Kenntnisse im IT-Bereich vertiefen.
- Durcharbeitung des MOOCs wegen des Studiums
- Eigene Kenntnisse in IT-Sicherheit zu vertiefen
- Ein noch besserer Umgang mit meinen eigenen Daten und Passwörtern
- Einblick in grundlegende Mechanismen persönliche Daten zu sichern, Erlangen von Wissen und Kompetenzen um eine hinterfragende Haltung einnehmen sowie begründet entscheiden zu können.
- Eine Arbeit finden
- Eine Ausbildung machen
- Eine Sensibilisierung zu erreichen und meine Strategien zu hinterfragen.
- Eine allgemeine Übersicht zu Risiken in der Handhabung von Zugangsdaten im besonderen mit Onlinediensten. Passend dazu wie man damit umgehen kann
- Eine größere Achtsamkeit und Kompetenz im Umgang mit Passwörter benötigenden Diensten zu erlangen.
- Einen bewussten Umgang mit Zugangsdaten und dessen Sicherheit zu erlangen
- Einen gewissenhafteren Umgang mit meinen Daten zu lernen.
- Einen sicheren Umgang mit persönlichen Daten zu erlernen und Methoden kennenzulernen wie man Gefahren entgegenwirken kann.
- Erfahren, welche Lerninhalte für Studienanfänger im Bereich IT-Sicherheit angeboten werden und wie sie vermittelt werden.
- Erlangen von Kenntnissen über Passwort-Sicherheit, genutzte Hacking- Methoden und Gegenmaßnahmen.
- Erlangung des Zertifikats und Erstellung des Reports
- Erlangung umfassender Selbstschutzkenntnisse
- Etwas neues lernen und Arbeit finden
- Etwas neues zu lernen.
- Etwas über Sicherheit zu lernen.
- Festzustellen, wie ich mit den mir gegebenen Möglichkeiten möglichst sicher im Netz unterwegs sein kann.
- Grundlagen
- Grundsätzliche Informationen zum Thema Sicherheit erhalten. Eigenes Verhalten reflektieren und Anregungen für einen anderen Umgang mit dem Thema IT Sicherheit lernen.
- Hintergründe erfahren über Datensicherheit, neue Impulse bekommen für die eigene Sicherheit.
- Ich habe meine Lehrausbildung als EDV - Kauffrau (Teilqualifizierung) abgeschlossen, in diesem Kurs möchte ich mir noch mehr Erfahrung sammeln.
- Ich hatte mir vorgenommen neues über die Passwörter und anderen Authentifizierungsmethoden und deren Sicherheitsaspekte zu lernen.
- Ich hatte vor, mein eigenes Verhalten im Rahmen meines Studiums fundiert zu hinterfragen eventuell zu verbessern.
- Ich möchte mehr über digitale Sicherheit erfahren. Bislang bin ich in diesem Themengebiet nicht bewandert.
- Ich möchte möglichst viel über IT-Sicherheit lernen.
- Ich möchte über alle Gefahren im Netz bescheid wissen und wie ich mich bestmöglich davor schützen kann.
- Ich will mein Wissen im It, rum um Informatik, erweitern und An meinen Fähigkeiten und Perspektiven arbeiten
- Ich wollte Lernen wie ich mich sicher im Internetverkehr bewegen kann.
- Ich wollte den nötigen Stoff für das Modul mir erarbeiten.
- Ich wollte mehr über den Selbstschutz lernen und besseres Verhalten damit erlernen.

- Ich wollte meinen eigenen Umgang mit Daten reflektieren und gegebenenfalls anpassen, um meine Daten mehr zu schützen
- Information
- Keine, einfach schauen, was angeboten wird
- Kennenlernen von sicherer Erstellung und Verwaltung von Passwörtern
- Kenntnisse an wie ich meine Daten, bzw. Person von Fremden auf dem Net schutzen kann, als auch weitere Themen bzw. Angriffe, Phishing, usw.
- Kenntnisse vertiefen, wieder in Erinnerung bringen
- Kurs abschließen
- Lernen
- Lernen, wie ich meine Daten im Internet besser schütze.
- MIch tieferlegend mit der Materie Digitaler Selbstschutz zu beschäftigen.
- MOOC bestehen für ITS Studium
- Medienkompetenzen im Bereich Sicherheit vertiefen
- Mehr Erfahrung anzueignen mit diesem Thema
- Mehr Selbstbewustsein mit Passwörtern
- Mehr Sicherheit
- Mehr Sicherheit im Umgang mit Daten zu erlernen.
- Mehr Sicherheit in der digitalen Welt bekommen und meinen Stand verifizieren.
- Mehr Wissen
- Mehr darüber erfahren, wie ich meine Daten besser sichern kann
- Mehr lernen
- Mehr wissen
- Mehr zum Thema "digitaler Selbstschutz" zu erfahren.
- Mehr zum Thema Datenschutz erfahren
- Mehr über Datennutzung und Sicherheit zu erfahren
- Mehr über Datensicherheit herauszufinden
- Mehr über Digitalen Schutz zu wissen
- Mehr über Digitalen Selbstschutz zu lernen
- Mehr über Passwörter und allgemeine Sicherheit zu erfahren
- Mehr über das Thema erfahren
- Mehr über den Bereich Sicherheit zu erfahren und einen angemessenen Umgang mit vertraulichen Daten erlernen.
- Mehr über den Digitalen Selbstschutz zu lernen und sich zu informieren, um sich im Privaten besser zu schützen und über Sachen aufmerksam zu werden, auf die man im Alltag oder allgemein gar nicht kommt.
- Mehr über den Digitalen Selbstschutzt zu lernen
- Mehr über den sicheren Umgang von Daten im digitalen Leben zu lernen
- Mehr über die Sicherheit und den Umgang mit Passwörtern zu lernen
- Mehr über die Sicherheit von Passwörtern zu erfahren, um selbst sicherer zu werden
- Mehr über die Sicherheit von Passwörtern zu lernen
- Mehr über dieses Thema zu lernen
- Mehr über digitalen Selbstschutz zu lernen.

- Mehr über sicherheit im netz zu erfahren
- Mein Verhalten über das Thema digitaler Selbstschutz zu reflektieren
- Mein Wissen zum Thema Datenschutz zu verbessern.
- Mein bereits vorhandenes Wissen zu vertiefen und zu erweitern und über die dargestellten Inhalte zu reflektieren
- Meine Daten besser schützen zu können
- Meine Daten sicherer zu verwahren
- Meine Frage war - Wie steht es um meine Sicherheit - Mache ich etwas falsch? Ja - eine ganze Menge...
- Meine Sicherheit im Internet zu überprüfen und ggf. zu updaten.
- Mich auf den Kurs einzulassen und etwas dazuzulernen
- Mich gut zu konzentrieren
- Mich im Bereich Datenschutz weiterbilden.
- Mich im Internet mehr selbst schützen zu können.
- Mich informieren und für mein Leben und Sicherheit was dazu lernen
- Mich weiterbilden
- Mit mehr Eigenverantwortung im internet Accounts und Passwörter zu verwalten.

  Neue methoden Kennen zu lernen.

  5 CP zu bekommen
- Neue Erkenntnisse zum Digitalen Selbstschutz.
- Neue Erkenntnisse über wie sicher Ich mit meinen Persönlichen Daten umgehe. Und eventuelle Anpassungen an meine derzeitigen Tätigkeiten treffen.
- Neues Entdecken
- Neues Lernen
- Neues Wissen erzielen und Impulse erhalten, um mich vor Sicherheitsbedrohungen gezielter schützen zu können.
- Neues im Umgang mit Zugangsdaten zu lernen und vorhandenes Wissen zu reflektieren
- Neues lernen
- Oberflächliche Kenntnisse Über IT-Sicherheit
- Pro und Contra verschiedener Methoden kennen. Refklektion über eigenes Verhalten. Kurs bestehen
- Prüfen ob es verbesserungen bei meinem Sicherheitsverhalten gibt
- Reflexionen zu IT-Sicherheit, Auseinandersetzung mit Sicherheitsaspekten von Zugangsdaten, Authentifizierung und Identifikationsüberprüfung im Digitalen
- Richtigen Umgang mit Passwörtern lernen.
- Schutz in der eigenen IT optimieren
- Selbstbestimmter mit meinen Daten sein
- Selbstschutz, Verständnis von digitaler Sicherheit, Passwort-Management
- Sich die Thematik in Erinnerung rufen.
- Sicherheit (3 Nennungen)
- Sicherheit Umgang mit Passwörtern
- Sicherheit im Internet
- Sicherheit im Web und mit Endgeräten.
- Sicherheit meiner Passwörter erhöhen

- Souveräner und besonnener Umgang mit meinen Zugangsdaten.
- Studium (2 Nennungen)
- Tag für Tag weiter die Skripte bearbeiten, Aufgaben lösen und am Ball bleiben
- Tools im Umgang mit Datenschutz verstehen und nutzen zu können.
- Umgang mit Daten sicherer zu gestalten
- Update bzw. Upgrade für eigene Datensicherheit - und Tipps an Familie, Freunde und Bekannte. Sensibilisierung für das Thema + eine gewisse Souveränitätb im Umgang mit Passwörtern, Accounts und nicht zu vergessen Social-Media Publicity
- Verständnis und Fachwissen aufzubauen
- Verständnis über Datensicherheit im Internet zu erhalten
- Vertiefende Infos über den Schutz.
- Vertieften Einblick in das Thema Digitaler Selbstschutz
- Vertiefung im Umgang mit sicherheitsrelevanten Daten, insbesondere umgang mit Passwörtern.
- WPM bestehen
- Weiterbildung (2 Nennungen)
- Weitere Ausbildung machen
- Weitere Ideen für eigene eLearning-Angebote
- Weitere Infos
- Wie ich meine Passwörter sicherer gestalten kann.
- Wiederholung von bereits Bekanntem -- ich bin selbst im Bereich IT-Sicherheit tätig und auch bei Chaos macht Schule aktiv.
- Wissen erweitern und vertiefen
- Wissen über Datensicherheit erweitern
- Wissen über digitalen Selbstschutz zu vertiefen und ggfs. neue Erkenntnisse direkt für mich umzusetzen.
- Wissen über sicheren Umgang mit Daten im Internet
- Wissen, wie man die eigenen Daten und Geräte besser schützen kann.
- Zu lernen, wie ich meine Daten und meine digitale Identität besser schützen kann.
- Zumindest Grundwissen
- aufklärung Datennutzung
- aus dem Kurs etwas zu lernen
- bewussterer Umgang mit Zugangsdaten
- den kurs bestehen
- etwas dazulernen
- etwas neues zu erlernen und es zu verstehen.
- ist nicht wirklich mein thema
- keine
- keines
- kenntnisse und sicherheit erlangen
- lernen sicherer mit digitalen Medien umzugehen
- mehr Selbstschutz in der digitalen Welt
- mehr sicherheit
- mehr zu Daten- und Gerätesicherheit wissen

- mehr zu wissen
- mehr über Sicherheitsmaßnahmen erfahren
- mehr über dieses Thema zu verstehen
- mehr über digitalen Selbstschutz erfahren für Beruf und privat
- mein eigenes Verhalten zu reflektieren und ggf anzupassen
- mich besser zu schützen
- persönliche Sicherheit im Umgang mit meinen Daten und Passwörtern
- sensibilisierung
- sicheres surfen im Netz erlernen, wissen vertiefen
- weitere Sicherheitserkenntnisse
- Überblick verschaffen wie es um die verschiedenen Authentifizierungmöglichkeiten bestellt ist und welche Vor- und Nachteile die verschiedenen Dienste und Programme haben

2.3) **Weitere Unterstützung** - Was könnte getan werden, um Dich besser bei der Erreichung Deiner Zielerreichung zu unterstützen?

- - (12 Nennungen)
- --
- .
- Alles bestens
- Alles gut, sehr gutes Konzept!
- Alles verstanden
- An meiner Konzentration arbeiten
- Analyse wie und wo ich mich im WWW bewege und welche Spuren ich hinterlasse, Wie kann ich das auch über einfache Mittel (Browserverlauf, PW Speicher etc.) auslesen, bzw. abrufen.
- Bei diesem MOOC kann in meinen Augen nicht viel verbessert werden außer hier und da die Tippfehler zu korrigieren und kaputte Links zu anderen Webseiten zu entfernen oder zu aktualisiseren.
- Bessere Erklärung plan
- Bessere erklärt werden (2 Nennungen)
- Das Niveau anheben und einzelne Themen vertiefen
- Den nächsten Kurs machen!
- Der Stoff wird gut vermittelt, habe keine verbesserungsvorschläge.
- Die Maßnahmen fand ich gut.
- Die komplizierte Navigation auf oncampus.de lenkt sehr vom Thema ab, man könnte stark vereinfachen, anstatt nur anfangs zu erklären.
- Eigentlich passt alles.
- Es hätte mich gefreut, wenn noch auf die Addons und der gebrauch und Sicherheitsfaktoren von lokalen Passwortmanagern wie beispielsweiße Keepass eingegangen worden wäre.
- Es war alles perfekt, ich hätte mir nichts anderes wünschen können.
- Es wurden mit umfangreichen Angebote gemacht um alle Ziele zu erreichen.
- Gut so
- Hier im MOOC nichts weiter.
- How-To-Videos zu den verschiedenen Maßnahmen wie PWM.
- Ich bin mit dem Kurs so zufrieden, wie er ist. Außerdem bin ich motiviert, weitere Kurse zu machen.

- Ich fand die Lektion sehr lehrreich. Ich weiß leider nicht, ob die Informationen manchmal etwas veraltet sind.
- Ich finde, dass der MOOC so schon sehr gut aufgebaut und durch Videos, Texte, Quizfragen und weiterführende Links unterstützt wird.
- Ich sollte nur nicht so Faul mit meinen Passwörtern umgehen.
- Integration der Report Teilbereiche direkt in die einzelnen Lektionen.
- Keine
- Kleine zusammenfassungen in stichpunkten wurde mir helfen
- Mehr Dienste vorstellen, welche beim sicheren Umgang mit Daten Unterstützung bieten
- Mehr Neuigkeiten in IT-Sicherheitssphäre, aktuelle Häker-Möglichkeiten.
- Mehr Zusatzmaterial. Videos vom CCC fand ich super!
- Mehr erklären (2 Nennungen)
- N/A
- Nicht so kompliziert
- Nichts (4 Nennungen)
- Nichts wirklich.
- Noch mehr Material bereitgestellt werden
- Noch spezifischere Themenbereiche und noch mehr Einblicke in verschiedene Programme bzgl. Bruteforce bspw. Man sollte es aus beiden Perspektiven kennen. Ich habe mir scheinbar schon vor dem Kurs ca. 90% des Kurses autodidaktisch erarbeitet
- Schadsoftware erkennen und Malware entfernen
- Schwierig gerade an dieser Stelle zu beantworten, da dieser Kurs die Grundlagen behandelt hat. Wenn man viele Dienste nutzt, ist es zwar ein wichtiger Aufwand alles zu ändern, um sicherer zu sein. Aber es kostet schon Zeit und Nerven. Vielleicht kann man da darauf hinweisen.
- Sich mehr zu informieren und auszutauschen
- Sichere Websiteprotokolle und Gesichtserkennung besprechen.
- Tutorial zur Einrichtung eines bestimmten Passwort-Managers
- Vertiefte Inhalte
- Vielen Dank!!!! Digitaler Selbstschutz 1 - Onlinekurs ist für mich sehr nützlich gewesen.
- War alles gut so
- Weiter informieren und andere Kursebesuchen
- Weitere Empfehlungen zu sicheren Providern, Mail-Anbietern und Co.
- Weitere Informationen zu Profiling und Datenschutzrecht, Nutzungbedingungen
- Weiteres OER-Material, das Angebot die H5P Aktivitäten herunterzuladen finde ich äußerst hilfreich. Danke!
- Weiterführende Links verfolgt
- alles gut
- evtl. ab und an aktuelle Link-Listen
- genauere Erklärungen bei den Englischsprachigen dingen
- ich hab mich null ausgekannt war sehr kompliziert
- kein Bedarf
- keine
- keine Verbesserungsvorschläge, war alles klar zu verstehen.
- keine lückentexte
  zu viel geschwafel

- mehr Inhalte von Dritten
- mehr Praxisbeispiele
- nicht nötig
- nichts (5 Nennungen)
- nix (2 Nennungen)
- noch ein Mooc über dieses Thema
- weitere Informationen

5. Dein persönliches Fazit zu diesem MOOC

5.4) **Praktischer Nutzen** - Ziehst Du aus dem MOOC einen praktischen Nutzen für Dich, d.h. machst Du in Zukunft etwas anders?

- -
- - Passwörter werden abgeändert und sicherer gestaltet
- .
- Auf jeden Fall dass ich meine Passwörter ändere und die mehr einzigartig pro Dienst machen
- Besserer Umgang mit Daten und deren Verknüpfung zu anderen Diensten.
- Da ich die meisten Tipps aus diesem Kurs zum Datenschutz schon befolge, werde ich nicht viel ändern. Ich habe jedoch alle Dienste etc. grob nach Datenschutz nochmals durchleuchtet.
- Dienste auf den Prüfstand stellen, vermehrt 2-Faktor verwenden und Webseiten entkoppeln
- Es hat mir auf jeden Fall gezeigt, dass ich schon einiges intuitiv so angewendet habe, wie ich sollte. Ich werde wohl in Zukunft etwas mehr auf Dinge achten, jedoch kann ich vieles beibehalten.
- Für jeden Dienst einen anderen E_Mail Account, Passwortlänge erhöhen, die Speicherung von Passwörter im Browser hinterfragen,
- Für mich heißt es am Ball bleiben. Da ich in der Berufsorientierung freiberuflich arbeite (EDV ;-)) ist das Thema sehr wichtig.
- Ich achte verstärkt auf den sicheren Umgang mit Zugangsdaten.
- Ich habe mehrere Verhaltensweisen geändert und mir viele neue sichere Passwörter zuglegt.
  Auch habe ich Sicherheitsrisiken kennengelernt, derer ich mir vorher nicht bewusst war. Außerdem überlege ich, ob ich mich bei der "Facebook-Datenschleuder" abmelde.
- Ich habe meine Passwörter verstärkt und fühle mich dadurch auch sicherer und aufgeklärter.
- Ich habe meine Sicherheitsvorkehrungen definitiv verbessert.
- Ich habe viele Tips bekommen mich selbst noch besser zu schützen
- Ich habe über meine Passwortsicherheit nachgedacht und Änderungen gemacht wo notwendig
- Ich hatte wohl schon zu viel Vorwissen - ich kannte fast alle Inhalte. Daher fühle ich mich in mein Vorgehen etwas bestärkt.
- Ich nutze bereits einen Passwortmanager.
- Ich nutze einen Password Manager und nehme bei wichtigeren Diensten Passsätze
- Ich nutze einen Passwortmanager
- Ich nutze nun privat einen Passwort Manager
- Ich nutze zwar mehrere E-Mail-Adressen, diese sind sich aber recht ähnlich. Ich überlege nun, ob es sich lohnt, dies zu "verbessern".
- Ich werde auf jeden Fall die Nutzung eines PWM in betracht ziehen und sehr wahrscheinlich schon heute anwenden.
- Ich werde definitiv sicherer und selbstbestimmter im Umgang mit meinen Daten sein, denn jetzt weiß ich endlich, worauf es ankommt.
- Ich werde eventuell meine Passwörter länger und komplizierter setzen und darauf achten wenn jemand Fremdes mich nach persönlichen Angaben fragt.
- Ich werde mein Verhalten mit gewissen Anbietern und Dienste mehr hinterfragen
- Ich werde meine Daten anders und komplexer schützen wie bisher

- Ich werde meinen Passwortmanager konsequenter nutzen, und eventuell auf einen lokalen PWM umsteigen. Außerdem habe ich zumindest für den PWM jetzt ein besseres Passwort vergeben sowie 2FA eingerichtet.
- Ich werde mich zukünftig mehr mit Passwörtern und Passwortmanagern beschäftigen
- Ich werde versuchen einen Passwortmanager einzurichten um mich besser vor Angriffen zu schützen.
- Ich werde zukünftig meine Passwörter durch generierte Passwörter meines PW-Managers ersetzen.
- Ich ziehe einen Nutzen daraus, in der Hinsicht, einen Passwortmanager und schwerere unterschiedliche Passwörter zu verwenden.
- Ich ändere in Zukunft so einiges
- Impuls nochmal meine Stragien zu prüfen und zu verbessern.
- In jedem Thema
- Intensiver den Passwortmanager zu nutzen.
- JA
- Ja (13 Nennungen)
- Ja etwas, Passwörter auf 16 stellen erhöhen, da die Rechenleistung immer besser wird.
- Ja ich werde einen Passwortmanager nutzen
- Ja schon, für das Lernen in der Zukunft
- Ja, Passwort Manager einführen und Passwörter anders wählen. Außerdem keinen zentralen Login-Dienst benutzen.
- Ja, auf jeden Fall
- Ja, auf jeden Fall, ich werde mein Handeln in Bezug auf Passwörter, Passwortmanager, etc. nochmal überdenken.
- Ja, das Handling von Mail-konten und die Nutzung div. bek. Dienste.
- Ja, das wird geschehen!
- Ja, durch mein täglich tun und meiner Beratung konnte ich sozusagen viel mehr in die Tiefe arbeiten, und jetzt nicht mehr nur oberflächlich, sondern diversifiziert.
  Auch die Privatperson wurde von mir viel mehr angesprochen und nicht nur die Beratung des Unternehmens fokussiert. Das gibt immer Pluspunkte im B2B! ;-)
- Ja, eine ganze Reihe von Änderungen werde ich vornehmen.
- Ja, einige veraltete Passwörter sicherer machen und Passwortmanager nutzen.
- Ja, ich habe bereits die verwendeten Login-Dienste entfernt, mir eine neue Passwortstrategie überlegt und einen Passwortmanager installiert
- Ja, ich habe viel gelernt und das gelernte bereits zum großen Teil umgesetzt.
- Ja, ich werde auf weniger Verknüpfungen zwischen Online - Diensten achten und mir ein anderes Verhalten anlegen was E-Mails/ Benutzernamen und Passwörter betrifft.
- Ja, ich werde die Passwörter abändern / anpassen.
- Ja, ich werde einen Passwort Manager verwenden.
- Ja, ich werde größeres Augenmerk auf Passwort-Zurücksetzen-Funktionen und Cross-Plattform-Nutzung legen. Zusätzlich werde ich auch meine privaten Passwörter lieber einem lokalen Passwortdienst anvertrauen.
- Ja, ich werde im Umgang mit Zugangsdaten vorsichtiger sein
- Ja, ich werde meine Passwortverwaltung konsequenter einsetzen
- Ja, ich ziehe praktischen Nutzen daraus -- aber nicht, indem ich etwas anders machen werde, sondern indem ich den Kurs Teilnehmenden von Chaos macht Schule Workshops empfehlen kann.
- Ja, mache ich
- Ja, passwortmanager ist schon eingerichtet
- Ja, schöne Praxistipps.
- Ja, sichere Passwörter verwenden und soviel wie möglich offline machen.

- Ja, verschiedene und sicherere Passwörter nutzen
- Ja, zukünftig werde ich mich intensiver mit der Verknüpfung meiner Konten und der Wahl meiner Passwörter auseinandersetzen.
- Ja. Ich werde auf eine längere und komplexere Passwortauswahl setzen.
- Ja. Konsequent PWM nutzen, unterschiedliche E-Mail-Adressen anlegen.
- Ja. Passwortmanager nutzen ^^
- Ja. Z.B. Nutzung von Passwortmanagern
- Kritischer Hinterfragen, im allgemeinen noch vorsichtiger zu sein im Umgang mit den eigenen Daten sowie deren Nutzung von Dritten noch weiter einzuschränken so weit möglich.
- LÄNGERE PASSWÖRTER
- Längere Passwörter (min. 12 Zeichen) nutzen!
- Man geht definitiv mit offeneren Augen durch das Netz. Definitiv wird von PINs und Mustern, dort wo es möglich ist, auf Passwörter umgesteigen. Es werden E-Mailadressen verändert und komplexere Passwörter definiert, die in der Folge für die Dienste individuell sein werden. Ein Passwortmanager scheint eine gute Idee - wenn auch nicht für die wichtigsten Passwörter..diese behält man nun doch lieber im Kopf.
- Mein Passwörter komplexer gestalten
- Meine Handy-Tastensperre habe ich schon von Pin-Muster zu einer 6-stelligen Pin geändert. Weiterhin werde ich wohl darauf verzichten Dienste miteinander zu verknöpfen.
- NEin werde mein Verhalten beibehalten
- Nein
- Nein, da ich den MOOC zwar interessant fand, aber für mich nichts Neues dabei war.
- Nein, da mir schon viele Sachen bewusst waren, aber vielleicht werde ich mal einen Passwortmanager nutzen.
- Nein.
- Nicht wirklich.
- Obgleich man vieles von dem MOOC schon vorher, wenn auch detailärmer, einmal gehört hat, so ist es doch gut immerwieder einmal auf die Aspekte der Sicherheit von Authentifizierungsmethoden aufmerksam gemacht zu werden. Mir hat das MOOC auf jeden Fall näher gebracht wirklich auf die länge meiner Passwörter zu achten und diese in jedem Fall immer unterschiedlich zu wählen.
- Passwort Manager wird genutzt. Ich habe mich von einigen Diensten abgemeldet. Datensparsamkeit.
- PasswortManager werden weiter getestet und fließen in meinen Alltag mit ein
- Passwortlänge vor -komplexität;
  tw. 2-Faktor-Authetifizierung und EInschätzung, wo das nicht sinnvoll ist;
  keine Login-Dienste;
  unterschiedliche Mailadressen für unterschiedlich vertrauenswürdige Plattformen;
  Passwort-Manager in meinem Fall nicht nötig;
- Passwortlänge ändern, PWM nutzen
- Passwortmanager nutzen
  effektivere Passwörter wählen
- Passwortmanager nutzen,
- Passwortmanager zulegen
- Passwörter (2 Nennungen)
- Passwörter und Dienste viel strenger trennen.
- Passwörter ändern/überdenken
- Sehr wahrscheinlich
- Sensiblisierung für Zusammenhänge und differenzierte Zugangsdaten
- Sicheres Surfen
- Sicherlich.

- Situation verdeutlicht
- Verschiedene Emailadressen nutzen
  Bank-PW nicht im lokalen PWM speichern
- Verwendung anderer Technischer möglichkeiten und Sensibilisierterer Umgang mit Daten im Netz.
- Vielen Dank! Ich freue mich darüber, dass den Kurs kostenfrei ist. Ja, das ist für mich sehr nützlich gewesen. Die frisch gelernte Kennfinesse / Information kann ich nicht nur für digitaler Selbstschutz verwenden, sondern auch in meinem Beruf weiter umsetzen. (als Call-Center Agent, First-Level-Support)
- Vielleicht die Verwendung eines Passwortmanagers
- Zugang zu Webdiensten überarbeiten, nach einer Risikoabschätzung die Absicherung der Mobile Devices verbessert.
- auf jeden Fall
- besser Passwörter
- bessere PW, mehrere E-Mails-Accounts
- bessere Passwörter benutzen
- in Details vermutlich schon, man wird noch ein bisschen paranoider
- ja (7 Nennungen)
- ja aufjedefall
- ja ich werde viele ändern
- ja,mail adressen und längere Passwörter
- ja.
- komplexere Passwörter
- nein (3 Nennungen)
- nicht nur verschiedene Passwörter, sondern auch verschiedene Mails
- noch bewusster mit den eigenen Daten bei den Diensten umgehen
- selber mehr fürSicherheit sorgen
- sicherere Passwörter
- viel werde ich nicht anders machen
- weiterhin kein Konto bei Google und Facebook
- werde mein Smartphone jetzt via pin sperren nicht muster
- yes...unbedingt

5.5) **Begeisterung -** Hat Dir etwas besonders gut gefallen? Lass es uns wissen, damit wir es in jedem Fall beibehalten:

- - (2 Nennungen)
- .
- /
- Aktuell würde ich es genau so lassen.
- Alles gleich gefallen
- Alles war gut und interessant :)
- Begeisterung hat bei mir jetzt niichts ausgelöst, ich würde den Aufbau trotzallem so belassen, da mir die Struktur und der vermittelte Inhalt schon sehr gefallen haben.
- Beispiele
- Berichte von realen Geschehnissen, zum Beispiel der Indentitätsdiebstahl des Reporters oder die Passanten, die ihr Passwort beim Interview verraten.

- Besonderes gut waren die Videos und die darin integrierten Fragen, bei denen man sofort überprüft ob man das erzählte auch verstanden hat.
- CCC
- Das Format an sich ist echt super und macht Spaß!
- Das Format.
- Das Jimmy Kimmel Video, soweit allgemein die Interviews sowie die Quizzes.
- Das Lernformat war schon nicht verkehrt
- Das Video und die Erklärung zum dem Fingerabdruck.
- Das Video von Jimmy Kimmel.
- Das Video über die Rekonstruktion von Fingerabdrücken.
- Das die Kurse für alle offen sind, und nicht nur die eingeschriebenen Studenten.
- Das es immer wieder unterschiedliche Arten zum lernen waren
- Der Aufbau des Kurses und die Kombi aus Video, Quiz und Text
- Der Informationsgehalt war genau richtig, wichtige Infos wurden noch einmal zusammengefasst, unterschieldiche Methoden zum Selbstlernen wurden angeboten
- Der enorme Praxisbezug. Im Vergleich zu anderen Modulen empfinde ich dieses MOOC als am nächsten an der (ggf. beruflichen) Praxis. Es hat sehr viel Spaß gemacht von Seite zu Seite und Video zu Video neue Sachen zu lernen, sein Wissen direkt in Quizzes testen zu können und anhand der Beispiele sowie Praxisaufgaben das gelernte an sich selbst überprüfen zu können. Man konnte mit jeder Lektion direkt Fortschritt und Praxis-/Lebensrelevanz feststellen.
- Der gute Praxisbezug des MOOC
- Die Umfragen und Statistiken, die vielen Möglichkeiten zur Reflexion
- Die Anzahl verschiedener Medien (Umfragen, Videos etc.)
- Die Ausgewogenheit aus Machbarkeit, Schwierigkeit und Reflexion/Selbstreflexion.
- Die Auswahlmöglichkeit zwischen Video und Text
- Die Befragungen und die hilfreichen Videos
- Die Beschreibung, wie Bruteforce Programme arbeiten.
- Die Einbindung von Videos verschiedener Leute/Formate war sehr abwechslungsreich und informativ.
- Die Erläuterung zu den Passwortmanagern, das Empfehlungen gegeben worden sind und worauf man bei Passwörtern achten sollte.
- Die Fragen zwischen Videos!
- Die Geschichte über den Hack des Journalisten. Das öffnet einem die Augen.
- Die Interviews
- Die Lehrvideos von unabhängigen Kanälen
  (Sempervideo)
- Die Logik hinter Passwörtern zu erkennen
  Die H5P Aktivitäten zum download
  Die Videos mit "CCC-Hacker-Feeling" :)
- Die Mischung aus Videos, Texten, externen Inhalten, Praxisbeispielen. Das sorgt für Abwechslung, verbessert die Motivation und macht einfach Spaß
- Die Multiple-Choice Test haben mir sehr gefallen.
- Die Möglichkeit diese Plattfrom zu nutzen ist das angenehmste Format seit beginn meines Studiums. Normalerweise tue ich mich mit Berichtschreiben schwer, aber dies fiel mir hier garnicht allzuschwer, da man im Kapitel auch immer direkt angezeigt bekommt, dass man jetzt besser die dazugehörige Aufgabe bearbeiten sollte.
- Die Quizze
- Die Schilderung des mehrstufigen Angriffs auf den Twitter-Account.
- Die Umfrage in Gestaltung eines Chatverlaufs und das Jimmy Kimmel Interview.

- Die Videos
- Die Videos mit den Quizfragen zwischendurch haben dafür gesorgt, dass meine Konzentration nicht zu schnell flöten gegangen ist.
- Die Videos und interaktionen waren sehr angenehm und abwechslungsreich.
- Die Videos.
- Die anschaulichen Beispiele über Sicherheiten von Passwörtern, das Video in dem gezeigt wird, das man Fingerabdrücke rekonstruieren kann, die Aufklärungen über Gefahren im Umgang mit Passwörtern
- Die beispiele aus echten gegebenheiten
- Die informativen Videos
- Die lehrreichen Videos
- Die praktischen Beispiele waren super! Gerade der Fall mit dem Journalisten.
- Die praktischen Beispiele, aktuellen Artikel und Gedankenspiele waren sehr hilfreich/motivierend.
- Die praktischen Beispiele, wie Angreifer bei zu einfacher Authentifizierung an die Accounts ran kommen. Dies führt einem die Dringlichkeit von der ganzen Problematik wunderbar vor Augen.
- Die unterschiedlichen Inhalte und die Abwechsllung (Quiz, Lesen, Film, ...)
- Forumdiskussionen
- Gefahren von Kameras für biometrische Authentifizierungsverfahren
- Gesamtpaket gut.
- Guter Kurs. Thema ist je nach Person natürlich spannender (oder nicht).
- Handwerkszeug, Impulse und Alternativen gezeigt bekommen und der Freiraum, die eigene Haltung im Umgang mit digitalen Medien reflektiert weiter zu entwickeln und ins Handeln zu kommen. Kriterien für Entscheidungen zu finden.
- Ich fand das Niveau durchgängig sehr gut.
- Ich fand die Kombination aus Videos und optionalem Text sehr gut. Die Videos lockerten das Ganze etwas auf und den Text habe ich zum Nachlesen beim Notizen machen verwendet.
  Dieses Konzept sollte auf jeden Fall beibehalten werden.
- Ich fand die Lektion mit den Passwort-Managern sehr gut
- Ich fand die Quizzes sehr gut um die Kenntnisse zu erweitern, als auch die möglichkeit für Wiederholung derren Fragen. Das MOOC ist sehr interaktiv, und hilft besonders gut meine Aufmerksamkeit zu unterstützen - zwar beim Online Studium
- Ich fand die unterschiedlichen Arten der Videos sehr gut, und die Erklärungen waren so, dass ich sie als teilweise Laie noch gut verstehe.
- Ich finde es sehr gut, dass nicht nur die Inhalte präsentiert werden, sondern das auch eine Interaktion stattfindet, wie z.B. die Quizzes während der Videos.
- Insgesamt freut mich einfach, dass ich jetzt selber wirklich weiß, worauf zu achten ist und wie man auch wirklich sein Verhalten verbessert.
- Interessante Artikel und tatsächliche Beispiele
- Jimmy Kimmel Video lockert sehr auf!
- Konkrete Beispiele
- Kurze Videos, die das Thema auf den Punkt bringen.
- Mir gefällt der Wechsel aus Video, Quizze, Roboterchats und praktischen Aufgaben sehr ausgeglichen und sehr gut :)
- Mir haben die Videos sehr gut gefallen.
- Möglichkeiten sich im Internet zu schützen
- Passworthacker
- Praxisbeispiele
- Quizzes und Umfragen
- Qzizfragen, Dialog zum Anklicken

- Tolle Beispiele zur Selbstreflexion
- Video mit Fingerabdruck
- Videos aus verschiedenen Formaten
- Videos mit den Fragen
- Vielen Dank! Heutzutage das Thema digitaler Selbstschutz sehr relevant ist. Ich freue mich darüber, dass den Kurs kostenfrei ist, weil nicht jeder Teilnehmer solcher Kurs sich leisten könnte.
- War toll! Interaktiv, motivierend!
- Wenn man einmal dort angekommen ist, war der Aufbau des Kurses mit seinen "Erfolgen" sehr motivierend. Auch das Layout ist sehr einladend.
- besonders die Videos und Quizfragen
- die Aufdröselung und grafische Darstellung hierzu zum Fall des Journalisten Mat Honan
- die informativen Videos und externen Artikel
- interaktiven Videos z.B.
- ja sehr hilfreich
- keine Angabe
- nein
- nein nicht so ganz
- unterschiedliche Videos und Quellen
- viele Beispiele
- war alles top

5.6) **Probleme** - Hattest Du größere Probleme in diesem Kurs oder der oncampus-Plattform? Oder hätten Sie auf etwas im Kurs verzichten können? Bitte beschreibe uns das kurz, damit wir daran arbeiten können;

- - (9 Nennungen)
- .
- Alles fine
- Alles gut
- Alles lief einwandfrei.
- Alles super
- Auf Facebook, Google Analytics, Google Tagmanager und deren Tracking hätte ich getrost verzichten können ;)
- Das Scollen der Maus wurde sowohl im Browser (Oben Unten) als auch in dem Lektionen genutzt. War unpraktisch!
- Das Video zu den beliebtesten Passwörtern in Deutschland finde ich einfach nicht gut. Die Informationen waren schon ganz gut, aber die Aufmachung des Videos nicht.
- Das Zusammenspiel von oncampus, Lernraum und Moodle fand ich etwas verwirrend.
- Das abschließende Quiz ist fehlerhaft - auch bei mehrmaligem Ausprobieren konnte eine der Fragen nie als "richtig" beantwortet werden.
- Den Weg über den Lernraum fand ich recht umständlich. Damit ging ja mal wieder ein neuer Account inkl. Passwort und somit ein möglicher Angriffspunkt mehr einher ;o)
- Die Chat-Funktion - ich wusste auch nicht gleich was das soll. Hier hätte auch eine Zusammenfassung in Stichpun kten gereicht.
- Die Reporterstellung war anfangs nicht ganz eindeutig, da die Reports etwas anders als im onlineformat sind.
- Ein Video von Semper Video war leider von YouTube gesperrt worden.
- Eine Erklärung zu den Navigationselementen/ dem technischen Aufbau des MOOCs wäre gut gewesen.
- Eingabe des Wörtbuchangriffs als Lösung ;-)

- Einige Videos funktionierten nicht.
- Es gab eine Stelle, wo ich etwas verärgert war:
  Beim Lückentext wo nach "brute force" gefagt wurde hatte ich "Brute Force" eingegeben und das war falsch. Hier sollten verschiedenen Antwortmöglichkeiten hinterlegt werden. (https://www.oncampus.de/course/weiterbildung/moocs/ds1-zugangsdaten?chapter=3&selected_week=22)
- Fragen sind teilweise schwer, aber machbar
- Freischaltung der Module anfangs.
- Für Report-Aufgaben private Accounts bei anderen Diensten einzubeziehen - ob bereits vorhanden oder neu erstellt - ist in meinen Augen ein NoGo.
  Das anfängliche Interview-Format erzeugt bei mir keinen Eindruck vom wissenschaftlichen Lernen und Arbeiten, wie ich es bei einem Studium erwarte und mir auch wünsche.
- Hatte keine Probleme. Vielleicht hätte ich mir mehr Videos gewünscht, aber das ist nur mein persönliches Empfinden.
- Hatte keine großen Probleme.
- Hier fällt mir leider kein Punkt ein.
- Ich bin nicht so der Fan von Vorstellrunden und Kommunikation, dementsprechend viel habe ich mich auch im Forum mit anderen unterhalten.
- Ich finde die nötigen Aufgabenblöcke offenbar nicht. Nach 5 Badges und der Bearbeitung aller Kapitel, hätte ich ein Zertifikat erwartet. Die Report Aufgaben werden ja nicht im MOCC bewertet, sondern vom Dozenten.
  Etwas schwierig finde ich auch die Option des Textes neben dem Video, wo im Video dann auf einmal die multiple choice Aufgaben aufpoppen, die man sonst gar nicht sehen könnte, wenn man einfach nur den Text lesen möchte. Warum gibt es nicht nach jedem kapitel einen Aufgabenblock, und einen Fortschrittsbalken für das Zertifikat? Ich sehe nirgendwo ob ich Aufgaben übersehen haben könnte. Die Badges sind unpraktisch, da sie auch keine Auskunft erteilen, ob daraus jetzt das benötgte Zertifikat erwächst. Der MOOC ist fertig bearbeitet, aber kein Zertifikat sichtbar. Und nirgends kann man prüfen, ob man Aufgaben übersehen haben könnte, da diese erratisch irgendwo zwischen Videos auftauchen. Das ist völlig unpraktisch. Man weiß nichtmal, ob diese kleinen Tests eigentlich die Aufgaben darstellen, die das Zertifikat braucht. Ich bin verwirrt.
  Außerdem sind mir das zuviele Umfragen.
- Ich finde, dass der Kurs sowohl für Einsteiger als auch für Amateure und Profis genau den richtigen Umfang hat.
- Ich finde, dass der Kurs zu lange ging.
- Ich hatte keine Probleme mit diesem Kurs.
- Ich hatte keine Probleme.
- Ich hatte keine großen Probleme
- Ich hätte mir gewünscht tiefer in die Inhalte einzusteigen. Ich fand es fast zu leicht...
- Ich würde mich freuen, wenn mein Klarname nicht öffentlich sichtbar ist.
- Ja mit verstanden
- Kannte mich gar nicht aus wie was wo
- Kaputte Links zu anderen Webseiten Prüfen und korrigieren
- Kein Problem. Alles ist TIP-TOP gewesen. Der oncampus-Plattform ist für mich deutlich gewesen. Ich war völlig zufrieden.
- Keine
- Keine.
- Manche Artikel, die verlinkt werden oder als Beispiel dienen, sind veraltet. Ich hätte es besser gefunden, wenn man auf aktuellere Themen Bezug genommen hätte
- Meine einzelne Kritik wäre die ziemlich lange Wartezeit wenn ich zwischen Lektionen, als auch Kapitalen navigiere. Allerdings weiß ich nicht genau ob es dann an meiner IPS liegt oder der Server der On Campus Webhost
- Mit Verständnis die deutsche sprache
- Nach dem Kurs läuft auf meinem PC alles nicht mehr so wie gewohnt, und der Alltag erweist sich als deutlich schwieriger.
  Ich arbeite am Tag mit mind. 4 Endgeräten sowohl beruflich als auch Privat. Die Umstellung von Windowsrechnern, Android und Apple gleichermaßen und gleichzeitig erwies sich als äußerst schwierig.
- Nein (6 Nennungen)
- Nein hatte ich nicht
- Nein, alles gut.

- Nein. (2 Nennungen)
- Nichts
- Rechtschreibung ist verbesserbar
- Sie vermischen bei dieser Fragestellung Du und Sie ;)
- Teils teils
- Teilweise waren Weblinks nicht mehr aktuell.
- Video im Kapitel 4.3 Methoden zum Durchtesten von Passwörtern steht nicht mehr zur Verfügung.
- Videos hätten durchaus kürzer sein können oder entsprechende Texte nicht dabei sein, die den Inhalt des Videos erneut wiedergeben.
- War alles perfekt.
- Zertifikat
- alles super
- die doppelte moodle Thematik verwirrte mich etwas.
- die praktischen Aufgaben für den Report sind z.T. zeitaufwändig, was für ein nebenberufliches Studium demotivieren kann. Man muss ja den Kontext des Lesens wechseln und nun eine Aufgabe am PC erledigen, die man von sich aus nicht machen würde.
- eigentlich nicht
- ja hab mich nicht ausgekannt und verstehe den sinn noch immer nicht
- keine Angabe
- keine Probleme
- keine änderungen notwendig
- nein (7 Nennungen)
- oncampus ist super. nur mit dem TH-Lübeck Account überblick bezüglich des Kurses war ich etwas unzufrieden. Könnte weniger einzelne Seiten haben.

5.7) **Weitere Themen** - Zu welchen Themen hättest Du gern mehr erfahren?

- - (11 Nennungen)
- --
- .
- /
- Alle wurden gut wiedergegeben.
- Angriffsmethoden
- Da es für einen Großteil der Studierende ein Modul im ersten Semester ist, wäre ich vielleicht auch auf die on-premisis PWM Lösungen eingegangen. Ich habe diese zum Teil im Forum erläutert.
- Das große Thema IAM (Identity Acces Management) noch etwas weiter beleuchten, open source Entwicklungen wie KeePass, vertieft Cloud contra lokales Netzwerk
- Das kommt evtl später noch, aber als Passwörter besprochen wurden habe ich ein wenig auf Verschlüsselung oder Salting gehofft
- Eine generelle Vertiefung wäre interessant
- Einzelheiten zu den Passwort-Managern.
- Es war ausführlich und ausreichend, so, wie es war.
- Firewall, Anti-Virus (es gab ja einen Abschnitt mit Bezug auf Trojaner) - falls es nicht in den beiden weiteren Kursen Thema sind
- Gerade freue ich mich nur die Inhalte zu lernen. Das Thema Digital Selbstschutz ist mir nur "umgangsprächlich" bekannt und ich finde die Realisierung der komplexeren Problema des Themas spaß
- Gesichtserkennung, Verschlüsslung, verschlüsselte Internetkommunikation.

- Hacking
- Hardware Sicherheit wie z. B. Yubi Key etc.
- Homebanking
- Ich finde Social Engeneering besonders spannend und wünsche mir noch mehr Infos dazu.
- Ich hätte gerne noch mehr theoretisches Hintergrundwissen erlangt, wobei das sicherlich den Kurs gesprängt hätte.
  Die Ziele, auf die der Kurz abzielte, wurden voll erreicht.
- Ich hätte mir ein paar mehr Passwort-Manager-Vergleiche direkt im Kurs gewünscht. Besonders zu lokalen Passwort-Managern.
- Ich interessiere mich auch an Medieninformatik. Das Thema "Digitaler Selbstschutz" war auch sehr wichtig und interessant für mich.
- Ich wurde für mein Empfinden gut informiert.
- Ich wurde weites gehend gut informiert.
- Kapitel 6.1 fand ich besonders spannend da es genau zeigt wie verwoben einzelne Accounts und Sicherheitsmechanismen sein können. Hier hätte ich mir noch mehr (anschauliche) Beispiele gewünscht, anstelle von Artikeln.
- Länge von Passwörtern mit Gleichbleibenden Symbolen u.ä.
- MFA, Keys als zusätzlicher Schutz
- Passwort
- Penetration testing, aber da greife ich thematisch vermutlich schon etwas vor.
- Phishing
- Rechtliche Sachen
  (Was droht bei Verletzung)
  Woran kann man sich wenden (wie lange dauert ein gerichtsverfahren - kosten,...)
  welche rechte kann man einklagen bei verletzungen?
  Inwieweit kann man klagen (Bund, EU, UN)?

  Zukunftsinteraktionen und Anregungen:
  sichere mechanismen in der Programmierung (codes)
  sicheres Betriebssystem vorstellen oder lücken und tücken aufzeigen (von anderen)
- Sichere Provider, Trakting
- Social Engineering
- Social-Engineering
- Technologien wie z.B. Passwörter oder andere Daten verschlüsselt werden
- Teil zwei kommt ja noch :-)
- Tourismus
- VPN, Home LAN Schutz, mobile devices schützen (e2e Verschlüsselung bspw.)
- War eigentlich alles gut ausbalanciert
- Welche Organisationen befassen sich mit diesen Themen? Was sind aktuelle Diskussionspunkte?
- Wie Geheimdienste Nutzer hacken
- Wie bereits beschrieben, Keepass und dessen Addons.
- Wie funktioniert ein Hasch mit Salt bei der Passwortdatenbank?
- Würmer, Trojaner und andere Schadsoftware
  Netzprotokoll, Router konfigurieren
- Zu den einzelnen konkreten Fällen von Datenmissbrauch.
- Zu keinen
- Zum Beispiel die produktion. Mitarbeiter
- Zum Thema Indentitätsdiebstahl
- habe mich für die Folge-moocs angemeldet und bin hinreichend sensibilisiert, nach weiterem moocs-input Ausschau zun halten

- keine Angabe
- nichts
- social engineering / brute Force methoden aber ich denke das kommt alles noch
- war genau richtig
- weiß ich nicht

5.10) **Monetarisierung** - Welchen Preis wärst Du ggf. bereit, für einen solchen MOOC samt Betreuungsangebot zu zahlen? (Angabe in EURO. Falls Du nicht bereit wärst, hierfür Geld zu bezahlen, trage bitte "0" ein.)

- -
- 0 (47 Nennungen)
- "0"
- .
- 0 euro
- 5 (6 Nennungen)
- 10 (5 Nennungen)
- 10 Euro
- 10,00 €
- 10€ einmalig
- 5 Euro
- 12
- 13
- 14,99
- 15 (3 Nennungen)
- 20 (7 Nennungen)
- 30 (3 Nennungen)
- 150 €
- 150-200€
- 150€
- 20,00
- 25 (4 Nennungen)
- 150€ aber je günstiger desto besser^^
- 299,-
- 30 Euro
- 40
- 50 Euro
- 50 €
- 50,00 €
- 50€
- 78€ (analog zu den anderen Kursen)
- 80,- Euro

- Da das MOOC1 - MOOC3 Teil des Moduls sind, sprich das Modul hier auch schon 80€ kostet und ab dem kommenden Wintersemester sogar 100€, bin ich froh das diese Themen / Aufgaben keine Zusatzkosten verursachen - dennoch wären hier 30€ die, aus meiner Sicht, zu vertreten wären. Aber da beim Onlinesudium ohnehin schon höhere Kosten auf der Rechnung stehen - wäre das in jedem Fall ein Ärgernis.
  FH Brandenburg...
- Da der Kurs neu ist und die Begleitung sehr gut ist, na das was man beim Studium bezahlen muss. 78€
- Da es hier eher um eine Sensibilisierung geht würde ich es als Einführungskurs verstehen. Somit 0 €, aber ein digitaler Strauß Blumen an die Professorin, die das Kursformat auf ein neues Level gehoben hat. Weiter so!
- Das hängt vom Umfang des Kurses ab. Ich bin sehr froh, dass dieser Kurs kostenlos angeboten wird, sonst hätte ich ihn vermutlich nicht gemacht, da ich erst mal reinschnuppern wollte.
  Da dieser Kurs vom Umfang her recht klein ist, würde ich sagen bis 25€.
- Für alle 3 Teil ca. 100 Euro
- Ich finde das sehr nützlich könnte sein, beim Schulungen im Call-Center, Providern auch in der Schulen. Damit die Sicherheitskenntnisse man gleich umsetzt.
- Ich mache diesen Kurs aufgrund eines Kurses an meiner Hochschule und würde unter diesen Umständen keinesfalls nochmal "obendrauf" etwas zahlen wollen. Als normaler Bürger würde ich aber sagen, dass man auch gerne 10/15 Euro oder so für diesen Kurs nehmen könnte.
- Im Rahmen des Studiums an der TH 0 Euro. Hier erwarte ich, dass alle Kurse wie gewohnt kostenlos sind. Andernfalls kommen mir die Kosten von 139 Euro für Personen von außerhalb zu hoch vor.
- Kann ich nicht pauschal sagen, je nach zu erwartender Qualität und Umfang 0-1000€ (gerade IT-Sicherheitskurse sind ja häufig wahnwitzig teuer und kaum von Privatpersonen zu bezahlen -- 1000€ für einen wirklich guten Kurs hielte ich jedenfalls nicht für zu hoch).
- Max. 50-60 Euro
- Mit kostenlosen Angeboten bekommt man mehr Teilnehmer, die sich dann ggf. auch für kostenpflichtige Angebote (bis 50 EUR) interessieren und anmelden.
- Wenn bei der Hochschule den MOOC nicht Gratis ist, wurde ich mir wahrscheinlich 5-12 Euro pro Kurs bezahlen.
- Wenn ich für etwas gerne bezahle, dann ist das Wissen. Den Preis kann man dementsprechend etwas höher ansetzen, als es bei guter Fachliteratur der Fall ist, sprich zwischen 50 und 100 Euro.
- ca. 100€
- da teils die Links und deren Inhalte teils etwas veraltet sind, das grundsätzliche Vorgehen der Hacker-Kaperer wohl noch relativ ähnlich ist, würde ich für alle drei Kurse etwa 149,-€ zahlen...

  insgsamt nutze ich die Corona-Phase zum Tuning meiner Lebensinhalte und -ziele, moocs sind ein großer Anreiz und eine Chance, sich Know-how anzueigenen ohne das eigene schmale Budget zu belasten
- den üblichen Preis für ein Modul, sofern die Betreuung ggf aufwändiger würde, weil Zusatzinhalte dazu kämen, allerdings wünschte ich mir klarere Zusammenfassungen in größeren Blöcken, als verfügbar, und systematischeren Aufbau Z.B. Welche Angriffsarten gibt es an welchen Stellen? Bei der Authentifizierung, bei single sign in, aber auch im Browser, Angriffe über Datenbanken etc pp. - bisher fand ich das IT Sicherheit Skript aus dem online Medieninformatik Studium gehaltvoller ;). Aber ich belege den Kurs als WPF im 4. - 5. Semester und habe ja erst den ersten Teil gesehen.
- kann ich nicht einschätzen, das ist mein erster Kurs..
- keine Angabe (2 Nennungen)
- keine ahnung
- weiß nicht
- 50 (11 Nennungen)
- 78
- 99
- 100 (2 Nennungen)
- 200
- 1000