Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru angajați **Unitatea 1 Săptămâna 1** **Numele unității: Webinar de introducere**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte**
Responsabil de învățare	• Gabriel Vladut • Valentin Istratie
Obiectivele activității de învățare	1. Introducere despre proiectul Erasmus+ InCyT 2. Obiective 3. Rezultate și produse 4. Cum să te protejezi împotriva atacurilor cibernetice 5. Instruire și mentorat 6. Inginerie sociala 7. Rețea de socializare
Abilități de dobândit	• TS3 Securitatea retelei • TS4 Testare de penetrare (vulnerabilități exploatabile). • SS3 Analiza cognitivă și comportamentală
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Pentru a afla despre proiectul Erasmus+ InCyT / obiective / Rezultate și produse • Cum să te protejezi împotriva atacurilor cibernetice • Instruire și mentorat • Inginerie socială / Rețea socială

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Informații scurte despre modul

Descriere
InCyT este un proiect Erasmus+ care urmărește crearea unui cadru, o metodologie de formare, care oferă un mecanism pentru VET și companii pentru a descrie competențele și abilitățile, necesare în securitate cibernetică pentru profesioniști și nu pentru profesioniști, pentru a evita atacurile cibernetice, precum și lacune digitale și altele. NIST, Inițiativa națională pentru educația în domeniul securității cibernetice (NICE) subliniază că ar trebui făcut un pas crucial pentru remedierea deficitului de „persoane cu cunoștințele, abilitățile și abilitățile necesare pentru a îndeplini sarcinile necesare pentru munca de securitate cibernetică”. O astfel de forță de muncă va include „roluri tehnice și nontehnice care sunt încadrate cu oameni cunoscători și cu experiență”. Proiectul va dori să implementeze câteva soluții în acest context. Are ca obiectiv mai întâi dezvoltarea unui cadru, care oferă un mecanism pentru VET și companii pentru a descrie decalajele digitale și altele necesare în securitatea cibernetică pentru profesioniști și neprofesioniști, pentru a evita atacurile cibernetice și a le ajuta să îmbunătățească această situație. Luând în considerare avantajele programelor de formare interdisciplinară și de mentorat, în special în domeniul securității cibernetice, proiectul va dezvolta și va testa programe de formare interdisciplinară digitală susținute de e-mentorat pentru IMM-uri și le va adapta pentru VET. Colaborarea și comunicarea între educatori, cercetători și persoanele care folosesc tehnologiile informaționale sunt necesare. O problemă este că companiile, în special IMM-urile cu resurse mai puține, au nevoie de ajutor pentru a aprecia competențele și decalajele angajaților lor, metode de evaluare a situației existente, precum și utilizarea posibilităților de formare pentru a-și recalifica angajații. Cursanții ar putea fi informați despre astfel de aspecte citind textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în ritm propriu. Toate aceste documente se află pe platforma digitală interactivă a proiectelor. Cursanții își pot testa răspunsurile prin exerciții de autoevaluare. Răspunsurile la alte exerciții ar trebui salvate pe forumul de discuții corespunzător și discutate cu mentorul la întâlnirea comună organizată o dată pe săptămână. Cursantul poate lucra în cooperare cu ceilalți și poate îndruma în special în timpul întâlnirilor. Aceștia vor fi sprijiniți să dezvolte un portofoliu electronic important pentru reflecția și evaluarea instruirii.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Conținutul materialului de învățare

Cadrul de competențe

Vor fi 3 întâlniri transnaționale în proiectul nostru. A fost planificat în luna a 3-a, a 13-a și a 20-a a proiectului. Vor avea loc câteva întâlniri suplimentare de proiect deoarece credem că 3 întâlniri nu vor fi suficiente pentru a derula un proiect de 24 de luni. Aceste întâlniri sunt online și au loc în mod regulat în fiecare lună. Echipa de management superior al proiectului va organiza aceste proiecte.

Proiectele vor fi conduse de coordonatorul proiectului, liderul WP. Vor fi 7 evenimente multiplicatoare în proiectul nostru. Fiecare instituție parteneră va organiza aceste activități pentru a populariza ideea de proiect în propria țară și pentru a împărtăși produsele dezvoltate. Fiecare instituție parteneră va desfășura Training-ul interdisciplinar pentru angajații IMM-urilor și profesorii în activitatea de securitate cibernetică în propria țară.

Figura 1: Activități susținute de proiectul InCyT

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Obiective

Proiectul InCyT va dori să implementeze câteva soluții:

- Dezvoltarea unui cadru, care oferă un mecanism pentru VET și companii pentru a descrie competențele și abilitățile, necesare în securitate cibernetică pentru profesioniști și nu pentru profesioniști, pentru a evita atacurile cibernetice, precum și lacunele digitale și altele.
- Luând în considerare avantajele programelor de instruire și mentorat interdisciplinare, în special în domeniul securității cibernetice, proiectul va dezvolta și va testa programe de formare interdisciplinară digitală susținute și o platformă de e-Learning colaborativă pentru IMM-uri.
- Adaptați-l pentru VET.
- Dezvoltarea unui model european de transferabilitate
- Luând în considerare avantajele programelor de formare interdisciplinară și de mentorat, în special în domeniul securității cibernetice, proiectul va dezvolta și va testa programe de formare interdisciplinară digitală susținute de mentorat electronic pentru IMM-uri și le va adapta pentru VET.

Rezultatele proiectului vor fi:

- Cadrul metodologic de implementare
- Formare existentă și viitoare (cursuri)
- Oportunități de îmbunătățire a acestora prin utilizarea interdisciplinarității și a mentoratului.
- Metodologia de învățare și mentorat

Produse:

1. Framework

2. Un material digital de instruire interdisciplinar în domeniul securității cibernetice pentru IMM-uri, susținut de mentorat și o metodologie adaptată pentru un curs special VET.

3. O platformă digitală pentru a sprijini formarea

4. Rapoarte în care competențele interdisciplinare oferă avantaje pentru IMM-uri și TVA.

5. Model european de transferabilitate pentru formarea și mentorat interdisciplinar testat.

Parteneri din: Germania (coordonator), Turcia, Polonia, Italia, Austria, Danemarca, România.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Activități

- Cadrul metodologic pentru securitate cibernetică - Organizații lider: IAT, Germania, Italia
- Un material de instruire digital interdisciplinar în domeniul securității cibernetice - Organizație lider: Universitatea de Științe Aplicate St. Pölten, Austria
- Platforma ICT pentru Securitate Cibernetică - Organizație lider: IPA, România
- Model metodologic pentru securitate cibernetică - organizație lider: Universitatea Politehnică, Polonia
- Model de transferabilitate - Organizație lider: Centrul European de Formare Copenhaga, Danemarca
- Evenimente - Organizație lider: Turcia

Cum să te protejezi împotriva atacurilor cibernetice

Economia digitală se bazează în primul rând pe date. În epoca Industriei 4.0, a sistemelor ciberfizice și a internetului obiectelor, tot mai multe produse și procese sunt digitalizate. Securitatea cibernetică, adică protecția acestor date și a sistemelor de procesare a informațiilor asociate, este mai relevantă astăzi decât oricând în istoria economică.

Procesele de afaceri pot fi perturbate semnificativ, încetinite sau chiar blocate complet, de exemplu dacă înregistrările de date sunt incorecte, incomplete sau nu sunt disponibile deloc, sincronizarea datelor între sisteme este întreruptă, sistemele IT funcționează incorect sau eșuează complet.

IMM-urile, în special, sunt ținte pentru activități criminale legate de aceste probleme. Spre deosebire de marile corporații, resursele lor sunt limitate - și hackerii știu asta! IMM-urile sunt coloana vertebrală a economiei în Europa, ceea ce înseamnă că peste 99% dintre companiile din Germania sunt IMM-uri.

Mai mult de jumătate din forța de muncă este angajată de IMM-uri. Prin urmare, este necesar să se ajute IMM-urile să evite atacurile cibernetice.

Cyber Security Education Initiative subliniază că ar trebui luat un pas critic pentru a aborda lipsa „persoanelor cu cunoștințele, abilitățile și abilitățile necesare pentru a îndeplini sarcinile necesare pentru activitatea de securitate cibernetică”.

Un astfel de grup include „funcții tehnice și non-tehnice care sunt îndeplinite de angajați cu cunoștințe și experiență”.

Cu toate acestea, este dificil să se creeze o forță de muncă cu abilitățile interdisciplinare necesare și să se rezolve problema comunicării dintre educatori, cercetători și oameni care folosesc

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

tehnologiile informației.

Este necesară cooperarea și comunicarea între aceste grupuri.

O problemă este că companiile, în special IMM-urile cu mai puține resurse, au nevoie de ajutor pentru a evalua competențele și lacunele angajaților lor, folosind metode digitale pentru a îmbunătăți situația existentă și organizând oportunități de formare pentru a-și recalifica angajații.

Instruire și mentorat

Antreprenorii, inclusiv cei viitori, au nevoie de moduri complexe de gândire și de capacitatea de a înțelege și integra cunoștințe din diferite sectoare, ceea ce necesită învățare interdisciplinară.

Problemele complexe de inginerie necesită crearea unei situații interdisciplinare într-un mod aproape natural.

Într-o abordare interdisciplinară, cursanții ar trebui să integreze informații din diferite discipline și domenii.

Ei dezvoltă o înțelegere interdisciplinară, învață să integreze domenii de expertiză și moduri de gândire specifice disciplinei.

Acest lucru crește abilitățile cognitive și gândirea critică mai mult decât prin mijloace disciplinare unice.

Inginerie sociala

- înseamnă manipularea ființelor umane, (folosind adesea metode psihologice), pentru a obține acces la date, documente și informații de interes pentru atacator.
- este una dintre principalele amenințări la adresa securității informațiilor în prezent și este o formă eficientă de criminalitate cibernetică.
- ar putea avea repercusiuni periculoase, de exemplu, încălcări ale datelor, mai mult decât orice alt tip de atac.
- atacurile au un scop financiar și astfel organizațiile au pierdut sume considerabile de bani.
- este deosebit de periculos pentru că se bazează mai mult pe eroarea umană decât pe vulnerabilitățile din software și sisteme de operare.

Companiile:

- ar putea suferi pierderi de productivitate, o scădere a moralului angajaților și dificultăți de

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

recuperare.

- au prejudicii reputației deoarece clienții nu sunt convinși că organizația se poate proteja.
- adesea trebuie să declanșeze un răspuns la incident vechi.
- ar trebui să ofere software de securitate pentru a ajuta la prevenirea atacurilor viitoare.
- deseori ar trebui să recalifice angajații pentru a fi pregătiți pentru atacuri.

Formare în inginerie socială (conștientizare cibernetică)

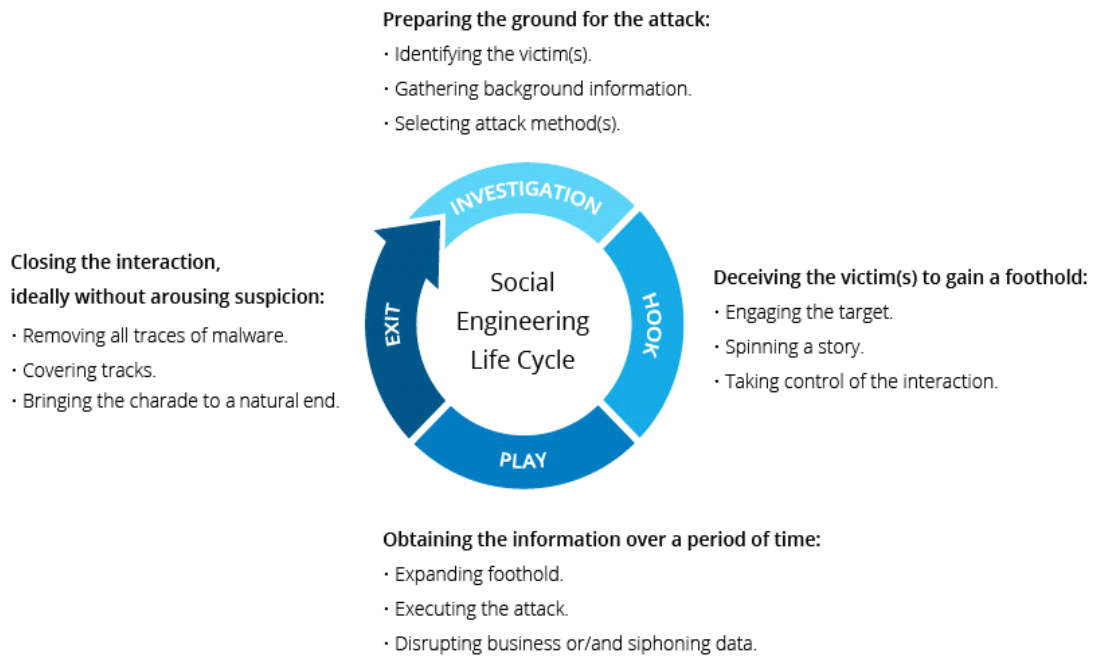
- de angajați și manageri pentru care este important să recunoaștem atacurile de inginerie socială deoarece riscul de a deveni o victimă este mare.
- ar putea fi incluse în programele de conștientizare a securității comunitare, individuale și cetățenești și să protejeze indivizii și organizația acestora.
- lipsește în special IMM-urile care au mai puține resurse, așa că ar trebui ajutate să ia în serios formarea de conștientizare cibernetică și să ofere angajaților oportunități de a o lua.

Ciclul de viață al atacului de inginerie socială

Atacatorul:

- mai întâi investighează victima vizată pentru a aduna informațiile de bază necesare, cum ar fi punctele de intrare și protocoalele de securitate slabe, care sunt necesare pentru atac.
- apoi încercă, câștigă încrederea victimei și oferă stimulente pentru acțiuni care nu sunt de obicei practici de securitate, cum ar fi devenirea informațiilor sensibile sau acordarea accesului la resurse critice.

Figura 2 explică ciclul de viață al unui atac.



Funde and
do not e
Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Figura 2: Ciclul de viață al unui atac

Rețea socială

- a devenit foarte popular în ultimii ani, oferind utilizatorilor o platformă pentru a comunica cu familia, prietenii și colegii lor.
- iar rețelele sociale se referă la utilizarea site-urilor de rețele sociale bazate pe Internet pentru a se conecta și a comunica cu prietenii, familia, colegii, clienții sau clienții.
- au serverele lor în centre de date amplasate împreună cu principalele puncte de acces la rețea de pe Internet.

Rolurile rețelelor sociale (Figura 3) arată câteva domenii în care rețelele sociale joacă un rol:

- divertisment
- construirea de oportunitati de afaceri
- a face carieră
- îmbunătățirea abilităților sociale
- dezvoltarea relațiilor cu alți indivizi

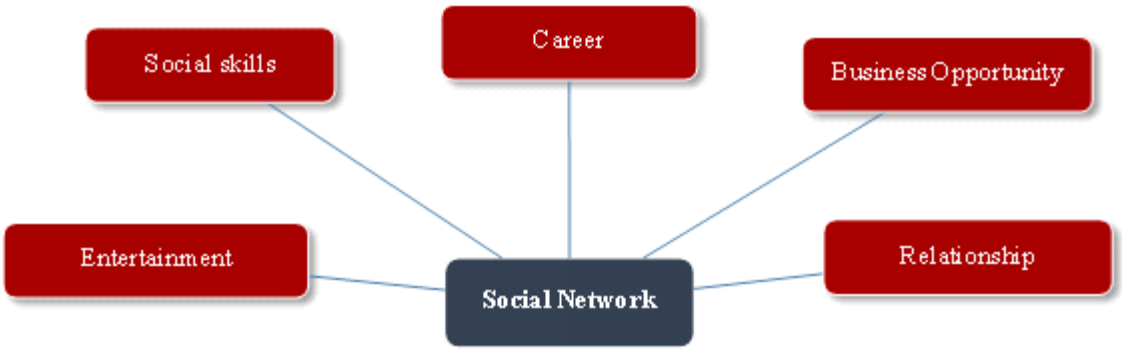


Figura 3: Roluri în rețeaua socială

Rețeaua socială:

- este o fundație pentru agenții de marketing care caută clienți pentru a crește recunoașterea mărcii, pentru a stimula loialitatea mărcii, pentru a îmbunătăți ratele de

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

conversie, pentru a oferi acces și implicare cu clienții noi, recenți și vechi.

- face posibil, prin partajarea postărilor de blog, imagini, videoclipuri sau comentarii pe rețelele de socializare, ca mai mulți oameni să viziteze site-ul companiei și să devină clienți.
- face dificilă ținerea pasului cu schimbările și afectează, de asemenea, rata de succes în marketing a unei companii.

Cele mai populare site-uri de rețele sociale (social media) din Statele Unite și Europa sunt:

- Facebook
- Instagram
- Twitter
- YouTube
- WhatsApp
- LinkedIn care ajută la conectarea profesioniștilor cu colegii de muncă, contactele de afaceri și angajatorii.

Rețelele sociale se bazează pe dezvoltarea și menținerea relațiilor personale și de afaceri folosind tehnologia și site-urile de rețele sociale (Social Media) care permit oamenilor și companiilor să se conecteze între ele, dezvoltând relații, partajând informații, idei și mesaje..

Membrii familiei ar putea rămâne conectați prin intermediul rețelelor sociale personale precum Facebook, să partajeze fotografii și să trimită alte mesaje despre viața lor.

Oamenii se pot conecta și cu alții (străini) care împărtășesc aceleași interese.

Există, de asemenea, dezavantaje ale rețelelor sociale, inclusiv răspândirea dezinformării și costul ridicat al utilizării și menținerii profilurilor de rețele sociale..

Funcționalitatea platformelor sociale poate fi clasificată în:

Funcțiile de rețea servesc la stimularea relațiilor sociale între utilizatori în cadrul platformelor virtuale și oferă funcționalitate pentru construirea și întreținerea graficului rețelei sociale.

Funcțiile de date sunt responsabile pentru gestionarea conținutului furnizat de utilizator și a comunicării între utilizatori, ajutând la îmbunătățirea (extinderea) interacțiunii utilizatorilor și pentru a face platforma mai atractivă

Funcțiile de control al accesului urmăresc să implementeze măsuri de confidențialitate definite de utilizator și să restricționeze accesul neautorizat la datele și informațiile furnizate de utilizator.

Avantajele și dezavantajele rețelelor sociale

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Beneficii

Rețelele de socializare le permit companiilor să:

- pentru a intra în legătură cu clienții noi și existenți.
- pentru a putea crea, promova și crește gradul de conștientizare a mărcii.
- să se bazeze pe recenzii și comentarii făcute de clientela lor importante pentru a crește vânzările mărcii și a clasamentului mai ridicat în motoarele de căutare.
- pentru a putea stabili un nou brand. pentru a demonstra clienților săi un nivel înalt de servicii.
- pentru a putea îmbunătăți produsele și relațiile cu consumatorii.

Dezavantaj

- pot contribui la răspândirea dezinformării.
- poate avea un impact negativ asupra companiilor deoarece critica la adresa unui brand s-a răspândit foarte repede pe rețelele de socializare.
- necesită ore de lucru și costuri în fiecare săptămână pentru a construi și menține un profil al companiei.

Securitate și confidențialitate în rețelele sociale

- Informațiile partajate în rețelele sociale și media se răspândesc foarte repede, ceea ce face atractivă pentru atacatori să le câștige.
- Problemele de securitate și confidențialitate legate de informațiile partajate de utilizator atunci când un utilizator încarcă conținut personal, cum ar fi fotografii, videoclipuri și sunet, ar trebui respectate, deoarece atacatorul poate folosi cu răutate informațiile partajate în scopuri nelegitime..
- Lipsa de conștientizare a utilizatorilor cu privire la securitate și confidențialitate are potențialul de a duce la diferite atacuri cibernetice prin intermediul rețelelor sociale.

Amenințările pot fi împărțite în trei categorii:

- Amenințările convenționale includ amenințările pe care utilizatorii le-au întâlnit încă de la începutul rețelei sociale.
- Amenințările moderne sunt atacuri care folosesc tehnici avansate pentru a compromite conturile de utilizator.
- Atacurile direcționate sunt atacuri care vizează un anumit utilizator, care pot fi comise de orice utilizator pentru diverse vendete personale.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Soluții pentru operatorii de rețele sociale

- Au fost propuse proceduri de autentificare precum CAPTCHA, autentificare cu mai mulți factori și identificarea cu fotografie a prietenilor..
- Setări de securitate și confidențialitate pentru a permite clientului să introducă informații personale din acces nedorit de către persoane din afara sau aplicații.

Utilizatorii raportează orice formă de abuz sau încălcări ale politicii de către orice utilizator din rețeaua lor, adică atunci când Facebook primește un raport de utilizator, acesta este revizuit și eliminat conform standardelor comunității Facebook.

Întrebări:

Să se răspundă cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

1. Care sunt așteptările tale cu privire la proiectul InCyT
2. Cum să te protejezi împotriva atacurilor cibernetice
3. Ce este o inginerie socială
4. Rețea de socializare

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

- Cum să te protejezi împotriva atacurilor cibernetice
- Ce este o inginerie socială
- Rețea de socializare

Atasamente

Prezentare PowerPoint
Filme video

Referințe:

- InCyT – Interdisciplinary Cyber Training

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Cyber Incident Recovery
- Minimize Cyber Attacks - Cyber Resiliency Strategy
- How to Prevent Cyberattacks: Top Ways to Protect Yourself
- Social Media Security: How Safe is Your Information?
- Internal Controls Over Information Systems
- Social Media Adoption Brings New Risks
- Social Media Security – 5 Security Tips
- 19 Social Media Security Best Practices

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.