

ABILITĂȚI DE SECURITATE IT

**PROTEJÂNDU-VĂ COPIII, VIAȚA PERSONALĂ ȘI
AFACERILE**

Cuprins

Introducere	3
Viața privată trebuie protejată	4
Copiii și tinerii sunt în mod special vulnerabili online	5
Pentru a preveni pierderile, afacerile trebuie să se adapteze	6
Oamenii sunt mai vulnerabili decât sistemele IT	7
Abilitățile de securitate IT sunt esențiale pentru a fi în siguranță online	8
Dezvoltarea competențelor de securitate IT – Perspectiva ECDL Foundation.....	8
Concluzii	10
Despre ECDL Foundation	11



INTRODUCERE

Pe măsură ce numărul de încălcări ale securității cibernetice crește în fiecare an, amploarea și costurile aferente acestora se măresc exponențial¹. Metode de a obține informații ilegal, precum phishing, spam și hacking, devin mai sofisticate și, ca urmare, protejarea informațiilor devine din ce în ce mai importantă. Acest document de poziție pune în discuție nevoile de securitate IT în ariile private sau profesionale și oferă exemple de cazuri în care principiile de securitate cibernetică nu au fost respectate. Lucrarea sugerează că, până și cele mai avansate produse de securitate IT nu sunt capabile să rezolve singure problema: oamenii trebuie să devină mai conștienți și să dețină abilitățile potrivite pentru a-și proteja propriile date și pe cele ale companiilor.

1 ENISA, Cyber 7, 2015, <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/cyber-7-seven-messages-to-the-edge-of-cyber-space>

1. Viața privată trebuie să fie protejată

Viața cotidiană devine din ce în ce mai digitalizată. În Europa, 65% dintre utilizatorii de Internet deja comandă online bunuri și servicii, 63% participă la rețele sociale, 57% folosesc online banking și 13% își fac programările la doctor online¹. Aceste activități le ușurează viața, dar ridică și preocupări suplimentare de securitate. Conștientizarea posibilelor amenințări și o înțelegere a felului în care protejăm datele personale și suntem în siguranță online devin cruciale. Totuși, doar sub jumătate dintre cetățenii UE se consideră foarte bine informați cu privire la riscurile criminalității informatice². Așa cum arată cazul Mat Honan, neglijarea principiilor simple de securitate cibernetică din viața personală poate fi dezastruasă.

Lui Mat Honan, un jurnalist pe tehnologie din San Francisco, i s-au spart și i-au fost compromise toate conturile digitale în decurs de numai o oră¹. Mai întâi, hackerii i-au spart contul de Amazon și i-au denaturat detaliile personale, ceea ce le-a dat posibilitatea să îi acceseze contul Apple ID. Ca urmare, au șters toate datele lui. Honan din iPad-ul, iPhone-ul și MacBook-ul personal, incluzând fotografii de neînlocuit, cu familia sau din primii ani de viață ai copilului. Apoi, infractorii s-au conectat la contul Google al lui. Honan și l-au șters. În final, i-au resetat parola Twitter și au propagat mesaje rasiste și homofobe.

Mat Honan admite că parțial a fost vina lui, toate conturile lui fiind în strânsă legătură unele cu altele. Consecințe grave ar fi putut fi prevenite, dacă ar fi urmat câțiva pași simpli de securitate, precum copierea pozelor pe care le stoca online (back-up) și utilizarea unui proces de autentificare cu doi factori pentru contul său Google.

1 Mat Honan "How Apple and Amazon Security Flaws Led Me to My Epic Hacking", <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>



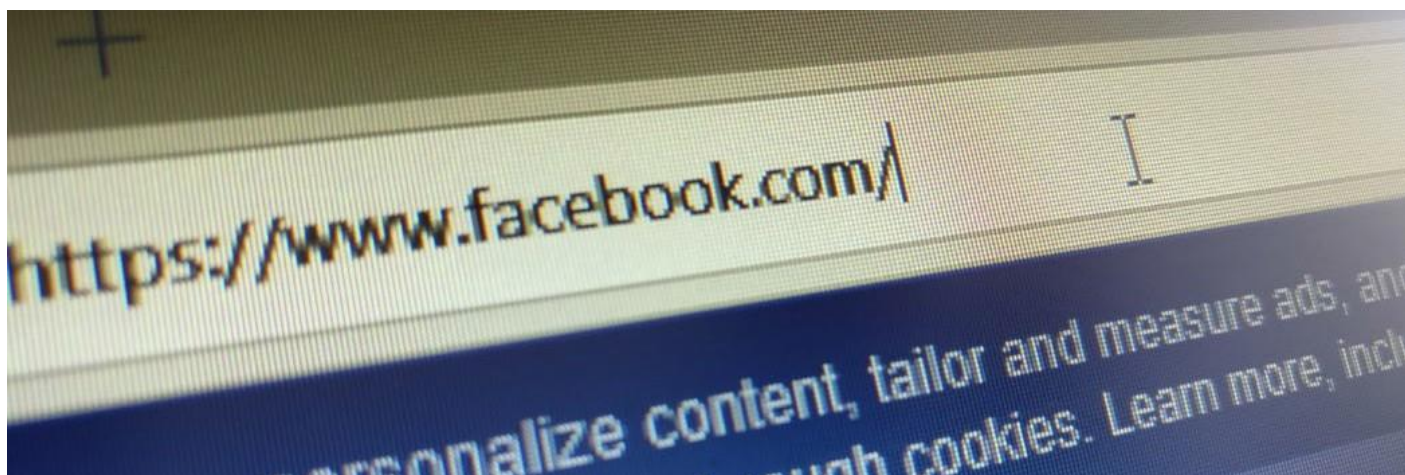
1 European Commission, Digital Scoreboard, <https://ec.europa.eu/digital-single-market/en/create-graphs>

2 Eurobarometer "Cyber Security", 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

2. Copiii și tinerii sunt în mod special vulnerabili online

Copiii și tinerii reprezintă unele dintre grupurile cele mai vulnerabile online. În ciuda mult răspânditei iluzii cum că tinerii sunt nativi digitali și în consecință folosesc tehnologia digitală sigur și eficient, studii variate arată că nu aceasta este realitatea³. Spre exemplu, cercetarea Net Children Go Mobile demonstrează că aproximativ jumătate dintre copiii cu vârste între 11 și 16 ani au fost supuși unor riscuri mai mari pe Internet și că proporția copiilor care au raportat că au fost deranjați sau supărați online a crescut în ultimii ani⁴.

Un studiu realizat cu studenții unei universități din Italia a relevat că majoritatea dintre ei au competențe digitale de nivel foarte scăzut. De exemplu, 42% dintre studenți nu sunt în măsură să conștientizeze riscurile folosirii rețelilor Wi-Fi gratuite, 40% dintre ei nu își protejează accesul la propriile telefoane mobile, 50% nu au controlat vreodată sau doar rareori permisiunile pe care aplicațiile le solicita înainte de instalare⁵. Tinerii au de asemenea tendința de a distribui online o serie largă de informații private, de cele mai multe ori regretând mai târziu⁶. Cele mai multe dintre aceste amenințări online ar fi putut fi prevenite dacă tinerii ar fi învățat înainte despre elementele de bază de securitate IT.



Subliniind pericolele pe care le pot prezenta cunoștințele slabe de securitate pe Internet, Panorama¹, un program de televiziune Belgian, a invitat un recruiter de la o agenție de recrutare, Randstad, să arate cum un angajator ar putea să găsească informații despre studenții aplicanți. Aceasta a căutat fotografii ale unuia dintre studenți pe Facebook, și primul rezultat a fost fotografia unei fete într-o cadă de baie, ce fusese postată de către mama acesteia. Fata a fost șocată să vadă fotografia apărută în rezultatele publice. Ea încercase să aibă grijă cu setările de distribuie online, dar, pentru că mama ei a putut să eticheteze fotografia, nu avusese control asupra tipului de fotografii pe care potențialii angajatori l-ar putea vedea atunci când aplică pentru un job. Prin simpla activare a unei setări, care i-ar da posibilitatea să aprobe etichetarea de către alți utilizatori, ar fi putut să evite surpriza și eventuala jenă cauzate de postările online ale fotografiilor personale.

1 VRT, Panorama, <http://deredactie.be/cm/vrtnieuws/videozone/programmas/panorama/2.27142>

3 More information about digital skills of young people can be found in ECDL Foundation position paper "The Fallacy of the 'Digital Native': Why Young People Need to Develop their Digital Skills", 2015, <http://www.ecdl.org/media/TheFallacyofthe'DigitalNative'PositionPaper1.pdf>

4 Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile, 2014, <http://eprints.lse.ac.uk/60513/>

5 Tech and Law Center, "Security of the Digital Natives", 2014, Italy.

6 <http://ikeepsafe.org/be-a-pro/reputation/hey-teens-chances-are-youll-regret-oversharing-personal-information-online/>

3. Pentru a preveni pierderile, afacerile trebuie să se adapteze

Atacurile cibernetice asupra afacerilor au devenit mai frecvente în ultimii ani. Spre exemplu, în 2015, nouă din zece mari organizații din Marea Britanie au raportat experimentarea unei încălcări de securitate a informațiilor⁷. Prejudiciile potențiale pentru companii includ pierderea de proprietate intelectuală, informații comerciale confidențiale și date private ale clienților, o scădere a încrederii consumatorilor și un prejudiciu de reputație. Se estimează că pentru companii cu peste 500 de angajați, costul mediu pentru cele mai severe încălcări de securitate online se încadrează între 2.03 milioane € și 4.38 milioane €⁸.

Întreaga activitate a unei companii de închirieri autovehicule, MNH Platinum, a fost amenințată în 2015, când unul dintre angajați a deschis un link suspect primit pe e-mail. Rețeaua companiei a fost atacată de un virus care a criptat peste 12 000 de fișiere ce erau vitale pentru activitatea firmei. Atacatorii au cerut o răscumpărare de mai mult de 4 000 € în schimbul decriptării fișierelor companiei. Pentru a primi înapoi datele esențiale, compania nu a avut de ales și a plătit banii ceruți de infractori. “Am fost complet nepregătiți pentru un atac cibernetic, chiar prin simpla lipsă a conștientizării magnitudinii pe care un astfel de atac l-ar avea prin click-ul din greșeală a unui link dintr-un email,” a declarat directorul Mark Hindle. “Sunt recunoscător că am scăpat cu noroc, ce mi-a permis să recuperez documentele care sunt vitale pentru derularea afacerii, chiar dacă a presupus un preț.”¹

MNH Platinum nu ar fi înfruntat niciodată un asemenea pericol pentru afacerea proprie, dacă angajatul care a accesat link-ul ar fi avut o înțelegere mai bună a amenințărilor securității cibernetice.

1 Mark Smith, “Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business”, 2016, <https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses>



Întreprinderile mici și mijlocii (IMM-urile) sunt deosebit de sensibile la încălcări ale securității IT. IMM-urile adesea presupun cu naivitate că nu vor fi amenințate online. De fapt, IMM-urile au o probabilitate mai mare de a fi atacate din cauză că tind să dețină o apărare mai slabă, ca urmare la lipsei de resurse umane și financiare⁹.

7 2015 Information Security Breaches Survey, <http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html>

8 Originally – between £1.46 million and £3.14 million. Currency converted from British pounds to Euros for the approximate date of publication of the study – June 2015. 2015 Information Security Breaches Survey, <http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html>.

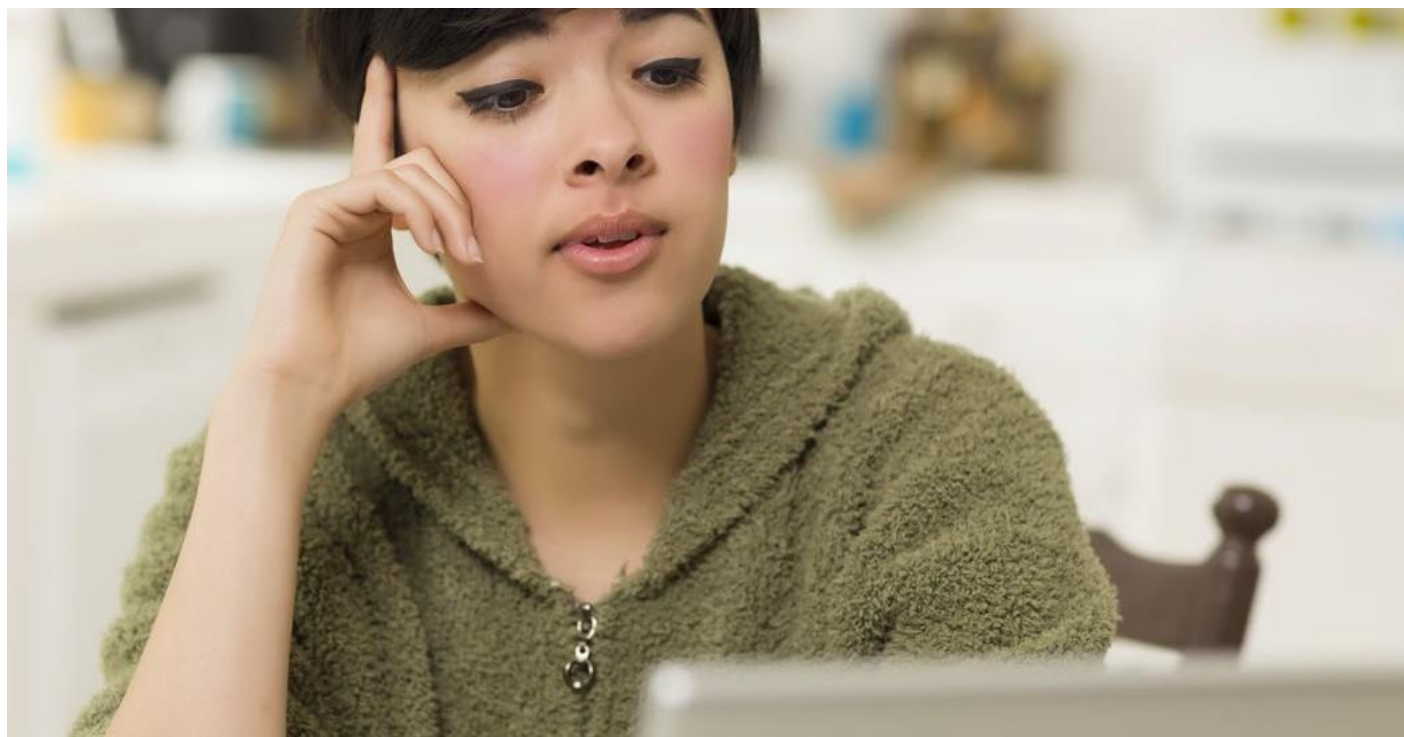
9 Mark Smith, “Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business”, 2016, <https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses>

Sondajul Information Security Breaches din 2015 a arătat că aproape trei sferturi dintre IMM-uri au suferit o încălcare de securitate în ultimul an și că, prețul mediu pentru cele mai grave încălcări s-a încadrat între 104 500 € și 433 160 €¹⁰.

4. Oamenii sunt mai vulnerabili decât sistemele IT

Furnizorii produselor de securitate IT – anti-virus, anti-spyware, etc. – pot sugera uneori că produsele lor vor ataca toate amenințările interne și externe de securitate, într-un mod complet automatizat. Cu toate acestea, tehnologiile menite să asigure securitatea, în cele din urmă, depind de punerea lor în aplicare efectivă de către persoane.

O greșeală uzuală pe care o fac organizațiile este de a minimiza riscurile de securitate, prin aplicarea unor măsuri de securitate IT foarte stringente pentru rețelele interne și, prin punerea în aplicare a unor politici de securitate aparent exhaustive pentru angajați. Aceste măsuri de politică, chiar dacă sunt eficiente, nu pot singure eradică pe deplin amenințările de securitate IT. În timp ce se întâmplă extrem de rar ca angajații să stabilească intenționat să saboteze sau să pună în pericol rețelele și operațiunile angajatorilor, măsurile de securitate IT menționate mai sus nu asigură întotdeauna că angajați bine-intenționați nu compromit accidental securitatea organizației lor, prin acțiuni aparent inofensive.



Literatura de specialitate admite că oamenii sunt legătura cea mai slabă la nivelul oricărui lanț de securitate¹¹. Un număr substanțial de încălcări ale securității online apar din cauză unui simplu click al angajaților unei companii pe un link suspect, descărcării de software neautorizat sau accesarea unor site-uri web care pot compromite rețelele. Majoritatea acestor situații ar putea fi prevenite, dacă angajații companiei ar avea competențele și cunoștințele potrivite pentru a recunoaște amenințările cibernetice și pentru a le evita. Guvernul Marii Britanii estimează că șapte din zece atacuri cibernetice ar putea fi prevenite¹², dacă organizațiile ar urma măsuri de securitate corecte.

10 Originally - from £75,000 to £310,800. Currency converted from British pounds to Euros for the approximate date of publication of the study – June 2015. 2015 Information Security Breaches Survey, <http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html>.

11 Mark Smith, "Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business", 2016, <https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses>

12 "Cyber attacks: Two-thirds of Big UK Businesses targeted", 2016, <http://www.bbc.com/news/uk-36239805>

5. Abilitățile de securitate IT sunt esențiale pentru a fi în siguranță online

Investiția în produse de securitate IT nu va asigura niciodată o protecție completă, dacă nu va fi însoțită de competențele IT potrivite și de o bună conștientizare a amenințărilor cibernetice. Doar prin înțelegerea și abilitatea de a identifica principalele elemente care accentuează utilizarea în siguranță a IT&C în viața cotidiană și prin deținerea abilităților necesare și a cunoștințelor cerute pentru a menține o conexiune de rețea și o utilizare a Internetului sigure, va putea fi capabil utilizatorul să protejeze de a fi compromise datele proprii și cele ale companiei.

O modalitate de a stabili practici bune de securitate IT pentru un individ și, prin extensie pentru o organizație, este prin a implementa programe de instruire și certificare recunoscute, care stabilesc nivelurile de referință pentru competențele și cunoștințele utilizatorului, pe baza unui standard recunoscut internațional.

6. Dezvoltarea competențelor de securitate IT – Perspectiva ECDL Foundation

Modulul IT Security 1.0

În 2010, ECDL Foundation a dezvoltat un modul specific referitor la securitatea IT¹³. Principalul factor care a dus la acest demers a fost cererea operatorilor naționali ECDL pentru o certificare orientată spre consumator, față de cele orientate spre specialiști. Alături de această solicitare a venit și conștientizarea securității IT în creștere, atât în rândul companiilor, cât și la nivelul factorilor de decizie politică. ECDL Foundation a decis că o soluție de certificare separată ar permite o interacțiune mai complexă și mai largă, cu aspecte de securitate IT care ar putea fi împinse dincolo de faza de conștientizare și, s-ar putea concentra pe cunoștințe conceptuale și aptitudini practice.

Versiunea 1.0 a Modulului IT Security a fost lansată în 2010. Modulul a stabilit conceptele și competențele esențiale referitoare la abilitatea de a înțelege principalele elemente care subliniază utilizarea în siguranță a IT&C în viața de zi cu zi și abilitatea de a utiliza tehnici și aplicații relevante pentru a menține o conexiune de rețea securizată, pentru a folosi Internetul în siguranță și cu condiții de securitate și pentru a gestiona date și informații în mod corespunzător.



¹³ ECDL Foundation folosește următoarele procese de dezvoltare a modulelor: mai întâi, se bazează pe expertiza rețelei de operatori naționali, care include asociațiile și societățile informatice din Europa. Aceasta expertiză este crucială pentru a identifica cunoștințele și competențele esențiale ce ar trebui incluse în obiectivele de învățare ale modulelor ECDL de certificare. În plus, acești operatori naționali coordonează rețele de centre de testare acreditate ECDL. Aceste centre de testare nu numai că sunt decisive în implementarea programului de certificare – ele sunt de asemenea foarte valoroase în a identifica abilitățile și cunoștințele corecte pentru un anumit domeniu, cum ar fi securitatea IT.

Modulul IT Security 2.0

În 2014, ECDL Foundation a decis să actualizeze modulul IT Security pentru a se asigura că, conținutul reflectă unele dintre tendințele emergente și cele mai importante pe acest subiect de cercetare. În mod particular, se acordă atenție aspectelor legate de apariția domeniului cloud ca o locație pentru date și servicii, utilizarea în siguranță a rețelelor sociale, precum și utilizarea ubicuă a dispozitivelor mobile.

Modulul¹⁴ este destinat oricui are nevoie să înțeleagă concepte referitoare la utilizarea sigură a IT&C în viața cotidiană și să aplice abilități în scopul de a menține o conexiune de rețea securizată, să utilizeze Internetul în siguranță și condiții de securitate și să gestioneze date și informații în mod corespunzător. Persoanele care doresc să protejeze propriile date și identitatea digitală, precum și angajații care au nevoie să protejeze datele organizației lor, pot beneficia de acest modul.

Preluarea Modulului

Până astăzi, adoptarea modulului IT Security a fost pozitivă. Spre exemplu, în 2015, aproximativ 93 000 de teste ECDL pentru modulul IT Security au fost susținute de candidați la nivel global, demonstrând relevanța acestui modul pentru toți cei își dezvoltă competențele digitale prin intermediul programului de certificare ECDL mai larg.

'Click safely! You can with ECDL – Protect yourself with IT Security'¹⁵ este un proiect ce a început în Italia în anul 2015. Acesta își propune să ofere tuturor elevilor de liceu competențele necesare pentru a naviga și a folosi mediul web într-un mod sigur și conștient. Construit pe o relație între AICA, operatorul național ECDL în Italia și Ministerul Educației, acest proiect dezvoltă conștientizarea utilizării în siguranță a noilor tehnologii și dispozitive mobile pentru elevi, părinți și profesori. Proiectul include aproape 3 milioane de elevi de liceu italieni, care pot accesa un program de învățare e-learning și apoi, dacă doresc, să înceapă procesul formal de certificare ECDL.

14 ECDL Foundation "IT Security", http://www.ecdl.org/programmes/media/ECDLITSecurity_Syllabus2.01.pdf

15 AICA, <http://www.aicanet.it/iocliccosicuro>

CONCLUZII

În cele din urmă, acțiunile utilizatorului uman sunt cele care cresc nivelul de expunere la încălcări ale securității IT. Instalarea celor mai performante măsuri automate de securitate și politicilor de prevenire reprezintă o soluție parțială. Majoritatea încălcărilor de securitate cibernetică ar putea fi prevenite și s-ar putea evita costurile aferente ridicate, dacă oamenii ar urma principii simple de securitate IT precum utilizarea unor parole sigure, instalarea programelor anti-virus și anti-malware, să nu dezvăluie informații confidențiale și de identitate personală pe paginile web de rețele sociale și să nu acceseze link-uri suspecte.

Copiii și tinerii sunt extrem de vulnerabili online. Încă de la vârste fragede, aceștia ar trebui să fie capabili să se protejeze astfel încât să se poată bucura de beneficiile vieții digitale. Ideal, toți elevii de gimnaziu și liceu ar trebui să fie instruiți cu privire la riscurile și utilizarea în siguranță a Internetului.

Costurile provocate de încălcări de securitate cibernetică ar putea fi semnificative pentru afaceri. Pentru a se evita pierderi potențiale, companiile ar trebui să se asigure că angajații sunt corect instruiți și sunt conștienți de riscurile on-line.

Pentru a îmbunătăți și a menține securitatea IT, atât la nivel individual, cât și la nivel organizațional, gradele de conștientizare și de comportament ale utilizatorilor trebuie să fie influențate pozitiv. Programele de dezvoltare a competențelor și cunoștințelor, care se concentrează pe cele mai importante și actuale amenințări de securitate IT, sunt cele mai bune instrumente de a atinge acest scop.

DESPRE ECDL FOUNDATION

ECDL Foundation este o organizație internațională dedicată dezvoltării standardelor de competențe digitale la nivelul forței de muncă, în educație și la nivelul societății în general. Programele noastre de certificare, oferite prin intermediul unei rețele active prezente în mai mult de 100 de țări, permit indivizilor și organizațiilor să evalueze, să dezvolte și să certifice propriile competențe de utilizare a computerelor și a instrumentelor digitale, pe baza standardului recunoscut global, ECDL.

Fiind o întreprindere socială non-profit, ECDL Foundation beneficiază de suportul unic al experților din cadrul societăților naționale de tehnologie și a partenerilor din întreaga lume, pentru a dezvolta standarde vendor-independente ce definesc aptitudinile și cunoștințele necesare, pentru a utiliza tehnologia digitală în mod eficient. Pentru a livra programele noastre, lucrăm cu parteneri educaționali și formatori, autorități locale și regionale, guverne naționale, organizații internaționale de dezvoltare, precum și cu angajatori din sectorul privat și public, din toate domeniile.

Calitatea și reputația ECDL sunt construite pe aproape 20 de ani de experiență în a asigura programele noastre de certificare pentru peste 14 milioane de oameni, în peste 40 de limbi vorbite în întreaga lume, cu mai mult de 2.5 milioane de teste ECDL susținute anual. Succesul nostru se bazează pe inovarea continuă în dezvoltarea de programe de certificare, pe angajamentul nostru pentru metodologii riguroase de testare și aderarea consecventă la standardele noastre de asigurare a calității.

ECDL Foundation susține inițiativele Operatorilor Naționali ai programului în Europa și Statele Arabe prin biroul nostru central din Dublin, Irlanda și biroul nostru European din Bruxelles, Belgia. Am înființat de asemenea trei operatori regionali – ICDL Africa (în Rwanda), ICDL Asia (în Singapore) și ICDL Americas (în Panama). Toți operatorii ECDL Foundation lucrează îndeaproape cu partenerii regionali, naționali și locali, pentru a dezvolta rețeaua globală de Centre de Testare Acreditate ECDL.

