CYBER HYGIENE CAPACITY BUILDING SKILLS THROUGH THE PRISM OF THE UNIVERSITY ECOSYSTEM

FORMAREA DEPRINDERILOR DE IGIENĂ CIBERNETICĂ PRIN PRISMA ECOSISTEMULUI UNIVERSITAR

Tutunaru Sergiu
Doctor în științe economice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: tutunaru@ase.md

Covalenco Ion
Inginer principal, Direcția Tehnologii Informaționale
Academia de Studii Economice a Moldovei
e-mail: covalenco@ase.md

Abstract
In this article, the authors address the importance of information security knowledge literacy for all categories of citizens, especially young people. The risks caused by non-compliance with cyber hygiene and the ways to overcome them are described. The main threats in the information space and the main methods to combat these threats are provided. The relevance of non-formal education and the possibility of implementing such non-formal education in the Republic of Moldova based on created in the Academy of Economic Studies of Moldova (AESM) educational ecosystem in the ICT fields and the materials provided free of charge by the American project CRDF is invoked. It is proposed to launch a pilot project at the AESM which aims to include as many universities and colleges as possible in the Republic of Moldova, with the task for promote non-formal education through an online course developed by CRDF.

Keywords: *education, ecosystem, cybersecurity, cyberhygiene.*

JEL Classification: *I25, I26, O39, Y80*

INTRODUCERE

Luna europeană a securității cibernetice, care a avut loc pe parcursul lunii octombrie a acestui an sub deviza „Securitatea cibernetică este fundamentul lumii digitale", s-a axat pe sensibilizarea publicului cu privire la amenințările cibernetice și promovarea importanței securității cibernetice în rândul cetățenilor și organizațiilor prin educație și schimbul de bune practici. Campania din acest an este rezultatul unei recomandări a Comisiei Europene de a se concentra asupra atacurilor online și își propune să contribuie la promovarea mesajului că igiena cibernetică ar trebui să facă parte din viața de zi cu zi a fiecărui cetățean.

Vicepreședintele Comisiei Europene Andrus Ansip, responsabil pentru piața unică digitală, a declarat: „Securitatea cibernetică este fundamentul lumii digitale; este responsabilitatea noastră comună, a tuturor, în fiecare zi." [1]

Problemele legate de dezvoltarea capacităților digitale pentru toate segmentele populației au fost reflectate pe larg și în cadrul a două reuniuni ministeriale ale Parteneriatului estic privind economia digitală (11 iunie 2015, Luxemburg și 5 octombrie 2017, Estonia), unde au fost identificate caracteristicile și direcțiile dezvoltării eficiente a economiei digitale.

REZULTATELE CERCETĂRII

Criminalitatea informatică este un domeniu aflat într-o permanentă inovare şi cunoaşte o rată foarte rapidă de dezvoltare şi diversificare. Astfel, expansiunea tipurilor de dispozitive care fac posibilă accesarea mobilă a internetului a dus la creşterea exponenţială a numărului de utilizatori şi, implicit, a riscurilor de victimizare.

În contextul în care, pe fundalul creșterii numărului de utilizatori, se poate constata o scădere a gradului de cunoaștere a riscurilor și amenințărilor care apar în mediul online, precum și a metodelor de eliminare a acestora, apreciem că este foarte importantă dezvoltarea parteneriatului cu toate organizațiile care pot contribui la creşterea gradului de conștientizare a fenomenului în rândul cetățenilor și, implicit la o mai bună siguranță".

În prezent se depun eforturi pentru prevenirea și combaterea criminalității cibernetice, care se manifestă prin infectarea cu malware, hacking, social engineering, phishing, diverse fraude online sau vulnerabilități ale hotspot-urilor Wi-Fi abordări tehnice sau legale, precum și de creștere a gradului de conștientizare în rândurile utilizatorilor de tehnologie.

Educația în domeniul securității cibernetice trebuie începută de la vârste fragede, întrucât copiii de astăzi au acces la echipamente conectate la internet și pot expune în mediul online, în mod periculos, date importante. Această educație trebuie susținută că efort atât de școală cât și de familie, iar cei responsabili trebuie să fie implicați în acest proces de educație, conștienți fiind de riscurile pe care le implica greșelile și nerespectarea unor reguli de comportament în mediul online, precum și de nevoia continuă de a cunoaște informații privind amenințările la care se expun. [2]

Probleme comune de igienă cibernetică. Întreprinderile au adesea mai multe elemente care au nevoie de igienă cibernetică. Toate componentele hardware (calculatoare, telefoane, dispozitive conectate), programele software și aplicațiile online utilizate ar trebui incluse într-un program de întreținere obișnuit și continuu. Fiecare dintre aceste sisteme prezintă vulnerabilități specifice care pot duce la diferite probleme. Unele dintre aceste probleme includ:

– Pierderea datelor: hard disk-urile și spațiul de stocare online cloud care nu sunt copiate sau întreținute sunt vulnerabile la hacking, corupție și alte probleme care ar putea duce la pierderea informațiilor.

– Date înlocuite: o igienă cibernetică deficitară ar putea însemna pierderea datelor în alte moduri. Este posibil ca informațiile să nu fie corupte sau dispărute definitiv, dar cu atâtea locuri de stocare a datelor, plasarea greșită a fișierelor devine din ce în ce mai obișnuită în întreprinderea modernă.

– Încălcarea securității: există amenințări constante și imediate pentru toate datele întreprinderii. Phishingul, hackerii, programele malware, spam-ul, virușii și o varietate de alte amenințări există în peisajul modern al amenințărilor, care este în permanență într-o stare de flux.

– Software învechit: aplicațiile software ar trebui să fie actualizate periodic, asigurându-se că cele mai recente patch-uri de securitate și cele mai multe versiuni actuale sunt utilizate în întreaga întreprindere - pentru toate aplicațiile. Software-ul învechit este mai vulnerabil la atacuri și malware.

– Software de securitate mai vechi: software-ul antivirus și alte software-uri de securitate trebuie să fie actualizate continuu pentru a ține pasul cu amenințările în continuă schimbare. Software-ul de securitate învechit - chiar și software care a trecut câteva luni fără o actualizare - nu poate proteja întreprinderea împotriva ultimelor amenințări

Activitatea online, folosind conferințe video, chat-uri de grup, platforme de schimb de date a permis să se atingă un nou nivel de eficiență și confort. Dar tranziția către munca și studiile la distanță a dus la o creștere semnificativă a atacurilor cibernetice și a scurgerilor de informații. Furtul de identitate și siguranța informațiilor cu caracter confidențial au devenit în prezent o problemă globală,

Pentru a diminua consecințele acestor fenomene este necesar să se respecte principiile de bază ale igienei cibernetice. Igiena cibernetică se referă la acțiunile și metodele pe care utilizatorii de computere și alte dispozitive trebuie să le urmeze pentru protejarea datelor personale și corporative, care ar putea fi preluate sau deteriorate. [3]

În cele ce urmează vom examina principalele pericole care ne urmăresc atunci când folosim rețelele de Internet. [4]

Vulnerabilitatea conexiunilor Wi-Fi. Wi-Fi-ul este un mijloc comod pentru verificarea rapidă a poștei electronice, schimbul de documente și conectarea la rețelele de socializare. Dar utilizarea rețelelor Wi-Fi în locuri publice: parcuri, restaurante, hoteluri, aeroporturi etc. amenință siguranța protecției datelor personale și confidențialitatea informației.

Una din măsurile de protecție ar fi eliminarea rețelelor publice Wi-Fi din lista rețelelor de încredere (acasă, la birou etc.). Astfel se va exclude posibilitatea conectării automate la rețelele publice fără consimțământul utilizatorului. O altă măsură ar fi asigurarea securității maxime a contului personal pentru a contracara încercările hackerilor de a obține acces la dispozitivul utilizatorului și a pirata sau a distruge informațiile.

Poșta electronică și riscurile pe care le comportă. Regula de bază în folosirea poștei electronice în scopuri de serviciu este de a utiliza doar poșta corporativă. Trebuie evitată trimiterea și primirea de informații și fișiere confidențiale prin serviciile de poștă publică (Yandex, Google etc.).

Nu se recomandă accesarea linkurilor indicate în scrisori și deschiderea fișierelor atașate fără a avea certitudinea că ele nu comportă riscuri de acces neautorizat. De obicei, astfel de scrisori conțin cereri de acțiune imediată (urmați linkul, deschideți urgent un atașament, instalați o aplicație etc.), acțiuni care pot afecta securitatea informației.

Un alt pericol îl prezintă mesajele de tip phishing, având adresa expeditorului similară cu adresa unor resurse oficiale, dar care diferă în unul sau două caractere (decan@asem.md, info@gogle.com etc.).

Phishingul este un tip de fraudă pe Internet, al cărui scop este de a obține acces la datele confidențiale ale utilizatorilor - autentificări și parole. Mesajele de tip phishing conțin fișiere care arată ca documente obișnuite (invitatie.doc, de exemplu), dar sunt de fapt programe care, de îndată ce sunt deschise, rulează în numele utilizatorului. Ca urmare, ele încep să își îndeplinească funcțiile, obținând, de obicei, acces la calculator sau telefon. Din acest moment, atacatorul va avea aceleași drepturi de acces ca și utilizatorul.

Mesageria electronică și pericolul scurgerii informației. Pentru a evita scurgerea de informații confidențiale trebuie evitat, pe cât e posibil, transferul prin aplicații de mesagerie (WhatsApp, Facebook, Messenger, WeChat, Telegram, Viber, Snapchat ș.a.). Dacă trebuie să transmitem urgent informații cu caracter confidențial sau care conțin secrete comerciale, și alte posibilități de transmitere nu există, informația respectivă trebuie ștearsă imediat după ce a fost transmisă. Același lucru trebuie să-l facă și destinatarul.

Atacuri Ransomware. (https://politia.md/ro/content/cunosti-ce-este-ransomware-cum-sa-previi-atacurile)

Ransomware este un tip specific de malware (programe dăunătoare) care cere fraudulos o răscumpărare financiară de la victime, amenințând cu publicarea, ștergerea sau blocarea informației.

Cel mai frecvent, atacurile Ransomware implică criptarea datelor personale sau ale companiei, astfel încât să nu poată fi utilizate sau accesate, și apoi obligă victima să plătească o răscumpărare pentru a debloca datele. Dacă vă aflați în situația în care vi se cere să plătiți răscumpărarea, nu vă lăsați pradă șantajului; aceste acțiuni se consideră drept fraude și se pedepsesc aproape în toate țările.

Pentru a nu fi jertfa unor asemenea atacuri trebuie respectate anumite reguli, cum ar fi neglijarea link-urilor sau atașamentelor suspecte din mesajele email, crearea regulată a cópiilor de rezervă pentru datele importante pe suporturi auxiliare, actualizarea permanentă a sistemului de antivirus etc.

Utilizarea parolelor ”slabe”. Se recomandă de a stabili parole diferite pentru conturi diferite, astfel încât cunoașterea parolei pentru o aplicație să nu permită accesul răufăcătorului la alte aplicații.

Parolele trebuie să fie complexe, suficient de lungi (12-15 caractere mixte) și să nu conțină date personale ușor de ghicit (Ana-1997) sau parole legate de compania la care lucrați (asem-2020).

Experiența ASEM. În scopul de a reduce decalajul dintre formarea academică și nevoile pieței resurselor umane în domeniul TIC a fost format un parteneriat între incubatorul inovator IT4BA cu 8 companii rezidente și Departamentul de informatică aplicată în afaceri, de curând creat,

Una dintre direcțiile ecosistemului creat este pregătirea informală la nivel național a tinerilor și a altor reprezentanți pentru particularitățile economiei digitale, inclusiv problemele de securitate cibernetică, prin seminare, training-uri, mese rotunde și cursuri de specialitate. [5]

În toamna anului 2020, Academia Economică a Moldovei a semnat un memorandum cu organizația CRDF Global, biroul din Kiev, pentru promovarea și desfășurarea unui curs online gratuit pentru învățarea studenților noțiunile de bază ale igienei cibernetice. În acest scop, materiale promoționale au fost postate pe site-ul oficial al ASEM, precum și în diferite rețele sociale. Au fost organizate ateliere de lucru cu studenți de la diferite specialități pentru a explica importanța respectării regulilor de igienă cibernetică în scopul asigurării securității personale și a rețelei.

Partenerul acestui proiect este organizația americană independentă non-profit CRDF Global, înființată în 1995, care promovează cooperarea științifică și tehnică internațională prin granturi, resurse tehnice, instruire și servicii. CRDF se angajează să promoveze aplicarea științei și tehnologiei la creșterea economică prin parteneriate internaționale și învățare care promovează invenția, inovația, antreprenorialul și comercializarea tehnologiei și accelerează cercetarea universitară și educația în știință și tehnologie. [6]

Implementarea acestui proiect va fi realizată de Incubatorul de Inovație IT4BA al ASEM are ca scop promovarea cursurilor online gratuite cu tema „Reguli de securitate de bază în sistemul digital mediu înconjurător". Instruirea online este disponibilă în prezent în engleză și ucraineană, iar versiunile în rusă și română vor fi disponibile în curând.

În termen de două săptămâni de la lansarea proiectului peste 80 de studenți s-au înscris pe site-ul CRDF Global (https://cybereducation.org/), o parte dintre care, după finalizarea cursurilor, au trecut cu succes testul final. În viitor, geografia educației va fi extinsă, atrăgând în proiect studenți și din alte universități din Moldova (Universitatea de Stat, Universitatea Pedagogică, Universitatea din Comrat și altele). Programul online conține următoarele 11 module:

Introducere și evaluare inițială; Principalele greșeli ale utilizatorilor; Utilizarea în siguranță a telefoanelor mobile; Utilizarea în siguranță a computerelor; Utilizarea în

siguranță a e-mailului; Siguranța în rețelele sociale; Utilizarea în siguranță a internetului; Tipuri de software rău intenționat; Știri false; Regula de bază a protecției datelor; Ce să faci dacă ai avut probleme.
Cursul se încheie cu un test online de 41 de întrebări cu răspuns multiplu. Participanții care răspund cu succes la cel puțin 31 de întrebări din 41 vor primi diplome internaționale de la CRDF Global, ceea ce va fi, fără îndoială, un bun suport pentru cariera lor. Pentru a trece testul, fiecare participant are dreptul la 3 încercări. Finalizarea proiectului este programată pentru aprilie 2021.

CONCLUZII

Concluzionând, putem spune că răspândirea virusului COVID-19 a schimbat radical viața oamenilor de pe glob. În aceste circumstanțe, instituțiile de stat și companiile private încearcă să se adapteze la condițiile noi, una din soluții fiind activitatea la distanță. Dar organizarea activităților online atrage după sine și o creștere bruscă a criminalității cibernetice. Se urmărește extinderea pe mai departe a proiectului prin atragerea unui număr cât mai mare de universități și colegii din țară.

BIBLIOGRAFIE

1. https://www.caleaeuropeana.ro/luna-europeana-a-securitatii-cibernetice-avira-si-cert-ro-vor-distribui-gratis-licente-antivirus-liceenilor-din-romania/
2. https://start-up.ro/bune-practici-de-igiena-cibernetica-cum-te-aperi-de-amenintarile-din-online/
3. https://DIGITALGUARDIAN.COM/BLOG/WHAT-CYBER-HYGIENE-DEFINITION- CYBER -HYGIENE-BENEFITS-BEST-PRACTICES-AND-MORE
4. https://vc.ru/u/545411-konsaltingovaya-gruppa-obereg/138612-kak-obezopasit-sebya-v-cifrovom-mire
5. Tutunaru, Sergiu; Covalenco, Ion. National Activities IT4BA incubator in the framework of the EU Digital Economy Strategy (DES). Conferința științifică Internațională ”Competitivitatea si inovarea în economia cunoașterii”, 28-29 septembrie 2018, Chișinău 2018, p. 49-52, ISBN 978-9975-75-934-
6. https://ru.qaz.wiki/wiki/CRDF_Global