CURSUL DE FORMARE „PROFESOR REAL ÎNTR-O ȘCOALĂ VIRTUALĂ”

ORA DE NET

Salvați Copiii
Save the Children România

Securitatea online

Autor: Teodora Carmen Stoica

Internetul și noile dispozitive devin din ce în ce mai prezente în felul în care relaționăm și comunicăm. Acum, mai mult ca niciodată, cadrele didactice, elevii și părinții folosesc internetul pentru a se conecta, pentru a partaja informații și chiar pentru a învăța. Există numeroase discuții în spațiul public pe această temă, însă două întrebări sunt oarecum absente din conversație: 1. „Cum afectează învățarea la distanță confidențialitatea?" și 2. „Care sunt pașii pe care părinții, elevii și profesorii îi pot face pentru a construi un mediu online sigur?"

Deși gestionarea securității rețelei și dispozitivelor școlii revine managementului instituțiilor de învățământ, cu toții știm că în practică sunt multe situații în care nu există un administrator IT desemnat sau în care multe dintre dispozitivele folosite sunt personale, fie ale cadrelor didactice, fie ale elevilor.

Indiferent de apartenența dispozitivelor, ele cu siguranță conțin date confidențiale despre elevi, părinți și chiar despre alte cadre didactice, motiv pentru care este foarte important ca acestea să fie securizate. Deși nu toți suntem specialiști în domeniul IT, există o serie de riscuri pe care este important să le cunoaștem, precum și o serie de măsuri pe care le putem lua pentru a fi în siguranță în mediul online.

Vulnerabilități în ceea ce privește securitatea cibernetică

În rândurile ce urmează, vă invit să explorăm împreună cele mai întâlnite vulnerabilități din mediul online în ceea ce privește securitatea cibernetică. Cunoașterea acestor fenomene vă va ajuta mult în asigurarea unui grad sporit de securitate și protecție, atât a datelor dvs. personale, cât și ale elevilor.

Phishing

Phishing-ul este de departe cea mai comună și poate cea mai periculoasă înșelătorie. În situația unei tentative de phishing, utilizatorul va primi un email (poate fi și SMS) prin care este rugat să se conecteze la un cont sau să-și verifice datele personale. Emailul primit va crea impresia că vine din partea unei instituții reale, precum o bancă, o organizație guvernamentală sau o rețea socială. Emailul va îndemna persoana să acceseze un site fals, care are însă un aspect autentic, și să-și introducă date personale, parole sau date bancare.

Ce este important de reținut!

- În general, companiile nu vă contactează pentru a vă cere numele de utilizator sau parola. Mai mult, instituțiile bancare nu vă vor actualiza niciodată datele online, pe o pagină accesibil public, ci doar în cadrul sucursalei.
- Dacă primiți un astfel de mesaj, nu faceți click pe nimic dintr-un e-mail sau mesaj text nesolicitat. Căutați singur numărul de telefon al companiei și sunați compania pentru a întreba dacă solicitarea este legitimă.
- Examinați cu atenție adresa de e-mail, adresa URL și ortografia utilizată în mesajul primit. Dacă observați inadvertențe sau greșeli, posibilitatea ca pagina să fie falsă este mare.

Software antivirus fals

Uneori, pentru a obține acces la dispozitivul dvs., infractorii cibernetici își vor masca atacul sub forma unui mesaj de instalare a unui program antivirus. Mesajul va apărea ca o încercare legitimă de protecție a computerului, însă în spatele acestuia s-ar putea ascunde un software malițios.

Ce este important de reținut!

- Este vital ca fiecare dispozitiv folosit de către dvs. să aibă un program antivirus instalat. Programele antivirus se pot instala prin accesarea paginii oficiale a producătorului.
- Examinați cu atenție adresa URL și ortografia paginii înainte de a descărca sau instala orice tip de software antivirus.
- Aplicați întotdeauna actualizările pentru produsele dvs. software existente.
- Odată ce aveți un antivirus instalat, priviți cu mare atenție și cu scepticism orice mesaj care vine de la un alt furnizor – acesta este, cel mai probabil, fals.

Ransomware

Ransomware-ul este un tip de software malițios care împiedică accesarea fișierelor, sistemelor sau rețelelor computerului și solicită să plătiți o răscumpărare pentru returnarea acestora. Atacurile de acest tip pot provoca pierderea informațiilor și datelor importante. De cele mai multe ori, un fișier de ransomware pătrunde în computer prin deschiderea unui atașament de e-mail, făcând click pe un anunț sau link străin sau prin vizitarea unui website nesigur.

Ce este important de reținut!

- Păstrarea soluțiilor antivirus și sistemelor de operare actualizate va oferi protecție suplimentară împotriva unui ransomware.
- Păstrați o copie de rezervă a datelor dvs.
- Evitați accesarea de linkuri necunoscute sau deschiderea unor fișiere primite din partea străinilor.

Vulnerabilitatea smartphone-urilor

Infractorii cibernetici pot exploata cu ușurință vulnerabilitățile telefonului dvs. mobil pentru a obține date private. Aceste vulnerabilități provin uneori din aplicațiile pe care le utilizați sau din propriul smartphone.

Ce este important de reținut!

- Dispozitivele mobile precum smartphone-urile și tabletele sunt vulnerabile atacurilor, motiv pentru care este important ca ele să aibă un program antivirus instalat.
- Evitați conectarea la rețele Wi-Fi nesecurizate – orice tip de informații transmise prin intermediul unei astfel de rețele, pot fi interceptate.
- Verificați cu atenție orice aplicație înainte de a o instala și asigurați-vă că eliminați în mod periodic aplicațiile pe care nu le folosiți.

Ingineria socială

Întrucât multe dintre atacurile de pe Internet se bazează mai degrabă pe inginerie socială, decât pe premise pur tehnice, considerăm important să abordăm succint acest subiect.

Ingineria socială este o tehnică de manipulare care exploatează erorile umane și folosește emoțiile pentru a obține informații private sau acces la date sensibile. Escrocheriile bazate pe ingineria socială sunt construite în jurul modului în care oamenii gândesc și acționează. Ca atare, atacurile de inginerie socială sunt utile în special pentru manipularea comportamentului unui utilizator. Odată ce un atacator înțelege ce motivează acțiunile unui utilizator, acesta îl poate înșela și manipula în mod eficient.

De pildă, un hacker va trimite mesaje alarmante de genul: „Contul tău va fi închis imediat" sau „Tocmai ai accesat conținut ilegal. Plătește amenda aici!" pentru a păcăli un utilizator neavizat să-și dea datele. Mai mult, infractorii pot folosi informații publicate online sau pe rețelele sociale (numele animalelor de companie, școala pe care ați urmat-o, numele membrilor familiei sau ziua de naștere) pentru a vă ghici parola sau pentru a răspunde la întrebările dvs. de securitate.

Am ales să abordăm și acest tip de vulnerabilitate pentru că ea este adesea exploatată atunci când vine vorba despre dispute între elevi sau atacuri asupra cadrelor didactice. O protecție bună a datelor și aspectelor de natură personală, parole puternice, precum și tratarea cu scepticism a mesajelor întâlnite online, pot contribui la un grad sporit de protecție, atât a elevilor, cât și a cadrelor didactice.

Recomandări

Vă încurajăm să aplicați aceste recomandări atât în utilizarea de către dvs. a tehnologiei, cât și să le promovați mai departe elevilor dvs.

Instalați un antivirus și mențineți-l actualizat.

Pentru a avea computerul sau dispozitivul mobil protejat este foarte important să folosiți un program antivirus. Indiferent de programul ales (poate fi chiar și o variantă gratuită), este esențial ca acesta să fie actualizat constant. Dacă un antivirus nu își actualizează zilnic baza de date, el nu va putea să vă protejeze de noi atacuri apărute și nu va fi util. În același timp, este bine de reținut că și dvs. aveți un rol activ în a vă proteja computerul și dispozitivul – nu dați click pe linkuri necunoscute, nu instalați programe decât de pe site-urile lor oficiale și scanați materialele descărcate înainte de a le deschide.

Folosiți parole puternice, diferite pentru fiecare cont.

Multe persoane se tem că un hacker ar putea să le spargă conturile, însă principalul mod prin care aceștia ajung să aibă acces la conturi nu necesită vreo tehnologie avansată. Este chiar foarte simplu atunci când intrusul ghicește parola. Folosiți parole puternice și setați parole diferite pentru fiecare cont în parte. Dacă găsiți dificil să puneți în practică această recomandare, puteți folosi un manager de parole, un program special ce vă va ajuta să faceți acest lucru cu succes.

Limitați cantitatea de date personale pe care le împărtășiți.

Odată ce o imagine sau o informație este postată pe internet, ea scapă din controlul nostru – poate fi preluată, copiată și partajată altora. De aceea, este important să ne securizăm conturile și să alegem cu grijă ceea ce alegem să postăm.

Feriți-vă de atacurile de tip phishing.

Înainte de a introduce date personale într-un formular, verificați întotdeauna adresa URL pentru a vă asigura că este un site sau o aplicație legitimă. Mai mult, evitați să dați click pe linkuri primite prin email dacă mesajul sună suspect, vă cere să introduceți date personale sau vă promite premii ori câștiguri. Aplicați această regulă și pe rețelele sociale – nu dați click pe ceva ce sună parcă prea bine pentru a fi adevărat.

Păstrați o copie de rezervă (back-up) a datelor dvs.

Fie că vorbim de documente importante sau de imagini pe care le păstrați ca amintiri, faceți o copie a acestor date pentru a vă asigura că nu se vor pierde.

Îndrumați părinții să folosească programe de control parental.

O recomandare foarte importantă pe care toate instituțiile de învățământ și părinții ar trebui să o pună în practică este instalarea pe dispozitivele copiilor a unui program de control parental. Acesta este un tip de software special ce vă poate ajuta să protejați copiii de conținuturi nepotrivite sau mesaje comerciale și să limitați timpul pe care aceștia îl petrec online.

Rețineți însă! Soluțiile de control parental sunt menite să vină în completarea unei relații de încredere cu copilul, a educării acestuia cu privire la riscurile și beneficiile mediului online și a comunicării deschise.

Dacă după parcurgerea acestor informații, constatați că nu sunteți familiarizați cu unii dintre termenii sau conceptele din acest material sau că aveți nevoie de ajutor pentru punerea în practică a recomandărilor făcute, vă încurajăm să discutați cu consilierii liniei ctrl_AJUTOR, care pot oferi clarificări și îndrumare.

Bibliografie selectivă

https://www.fbi.gov/scams-and-safety

https://www.kaspersky.com/resource-center/threats/top-7-cyberthreats

Salvaţi Copiii România este o organizaţie de utilitate publică, a cărei misiune este aceea de a garanta egalitatea de şanse pentru toţi copiii, indiferent de mediul din care aceştia provin, prin utilizarea propriei expertize, precum şi prin activităţi de lobby şi advocacy asupra factorilor de decizie şi mobilizarea liderilor din societatea civilă.

Salvaţi Copiii promovează de 30 ani drepturile copilului, în acord cu prevederile Convenţiei Naţiunilor Unite cu privire la Drepturile Copilului. Peste 2.220.000 de copii au fost incluşi în programe educative, de protecţie şi asistenţă medico-socială, de stimulare a participării lor în acţiuni de promovare şi recunoaştere a drepturilor lor.

Salvaţi Copiii este membru al Save the Children International, cea mai mare organizaţie independentă din lume de promovare a drepturilor copiilor, care cuprinde 28 de membri şi desfăşoară programe în peste 120 de ţări.

Salvaţi Copiii
Save the Children România

HUAWEI

Secretariatul General

Intr. Ştefan Furtună nr. 3, sector 1,
010899, Bucureşti, România

telefon: +40 21 316 61 76

e-mail: secretariat@salvaticopiii.ro
web: www.salvaticopiii.ro

Cofinanţat de Mecanismul pentru Interconectarea Europei al Uniunii Europene