Securitatea Cibernetica

Proiect elaborat de: Cheibas Elena & Cioban Bogdan
Profesor: Gutu Maria
Data realizarii: 16 octombrie 2018

Obiectivele Proiectului

Dupa studierea acestei prezentari, veti fi capabili:
• Sa recunoasteti un calculator virusat
• Sa instalati protectia antivirus
• Sa recunoasteti tipurile de programe maltioase
• Sa va protejati de fenomenul cyber-bullying
• Sa determinati modul de securizare a informatiilor si aplicatiilor software

1. Beneficiile si riscurile navigarii pe internet (Elena)

Beneficii. Internetul oferă:
• Informatii din toate domeniile (politica, administrație, sport, agricultură, vreme, informații juridice etc) prezentate sub tot felul de forme: știri, articole, imagini, videoclipuri etc.
• Comunicare rapidă cu oameni de oriunde de pe glob prin: mail, site-uri de socializare, messenger, skype etc;
• Acces la cursuri online, și alte informații/documente utile în pregătirea profesională și carieră
• Căutarea şi găsirea unui serviciu
• Posibilitatea de a lucra de acasă
• Comerț electronic – posibilitatea de a găsi și cumpăra sau comercializa produse
• Posibilitatea de a da anunturi referitoare la orice: cumpărări-vânzări, matrimoniale, evenimente, proteste etc
• Economie de timp

Riscurile navigării pe internet:
• Calitatea si veridicitatea informațiilor de pe internet este nesigura. Pentru că oricine are acces la internet, oricine poate posta informații pe internet, oricine poate spune neadevăruri, poate dezinforma, sau poate minți pe internet.
• Informatiile personale nu sunt in siguranța când folosim internetul. Această securitate a datelor personale pe care o promovează site-urile ce oferă de exemplu căsuță de mail, este falsă.
• Toate informațiile de pe mail sau din orice alte conturi online, toate parolele noastre, toate “mișcările” noastre pe internet sunt stocate si accesibile celor care oferă serviciile respective.
• Identitatea virtuală ce nu coincide cu cea reala. Atunci când vorbești cu cineva pe internet, indiferent în ce domeniu, habar nu ai cine este de fapt, ce fel de om este, cât de corect, cât adevăr spune sau cât minte.

2. 10 reguli pentru o navigare sigura pe internet (Bogdan)

1.Stabileste împreuna cu parintii tai regulile de folosire a calculatorului si a Internetului.
2.Nu da nici unei persoane întalnite pe Internet informatii personale despre tine sau familia ta.
3.Parolele sunt secrete si îti apartin.
4.Daca vrei sa te întalnesti fata în fata cu persoanele cunoscute pe Internet sau de la care ai primit mesaje pe telefonul mobil, anunta-ti parintii pentru a te însoti, preferabil într-un loc public.
5.Posteaza cu mare grija fotografii cu tine sau cu familia ta!
6.Nu tot ceea ce citesti sau vezi pe Internet este adevarat.
7.Nu raspunde la mesajele care te supara sau care contin cuvinte sau imagini nepotrivite!
8.Da dovada de respect, chiar daca nu-i cunosti pe cei cu care comunici.
9.Cumpararea produselor pe Internet este permisa doar parintilor.
10.Poti oricand sa te opresti din navigarea pe Internet sau sa refuzi sa continui discutiile pe chat, daca s-a întamplat ceva care nu ti-a placut, te-a speriat sau, pur si simplu, nu ai înteles.

3. Cum recunoaștem un calculator virusat (Elena)

Cele mai raspandite semne de infectare :

1 "Calculatorul vorbeste cu mine“ - apar pe ecran tot felul de ferestre “pop-up” si mesaje publicitare, precizand ca PC-ul este infectat si ca are nevoie de protectie.

2. “Calculatorul meu functioneaza extrem de incet“ - acesta poate fi un simptom al infectarii cu un virus, vierme sau troian, care poate consuma resursele calculatorului, facandu-l sa functioneze mai greu decat de obicei.

3. “Am aplicatii care nu pornesc” – simptom care va spune ca ceva nu este in regula.

4. “Nu ma pot conecta la Internet“ – daca ati fost infectat, virusul se poate conecta la o anumita adresa de Internet sau poate deschide anumite conexiuni separate, limitand astfel viteza de accesare a Internetului sau chiar facand imposibila folosirea acestuia.

5. “Cand ma conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate” - multe fisiere virale sunt concepute special pentru redirectarea traficului de Internet catre anumite website-uri, fara consimtamantul utilizatorului, sau chiar sa imite anumite website-uri, creand impresia unui site legitim.

6. “Unde au disparut fisierele mele?“ - anumite atacuri sunt concepute special pentru criptarea sau stergerea anumitor fisiere si chiar mutarea documentelor dintr-un loc in altul.

7. “Antivirusul meu a disparut, firewall-ul este dezactivat” – o actiune tipica a amenintarilor este dezactivarea sistemelor de securitate instalate pe calculator.

8. “Calculatorul meu vorbeste in alta limba” - daca limba anumitor aplicatii se schimba, ecranul apare inversat, “insecte” ciudate incep sa “manance” ecranul, este posibil sa aveti un sistem infectat.

9. “Calculatorul meu, practic, a innebunit” – daca calculatorul incepe sa actioneze singur sau sa trimita email-uri fara sa stiti, iar aplicatii sau ferestre de Internet se deschid singure, atunci sistemul ar putea fi compromis.

4. Protectie antivirus (Bogdan)

Exista multe solutii antivirus pe piata. Important in cazul unei astfel de solutii este nivelul de protectie pe care il ofera. Sunt mai multe metode de a identifica virusi, astfel in alegerea solutiei antivirus este important sa tinem cont de acest lucru. Un alt aspect important este frecventa cu care solutia antivirus isi face actualizarile privind semnaturile virusilor. Practic, exista o baza de date pentru fiecare produs antivirus care contine semnaturile virusilor informatici cunoscuti, iar aceasta se actualizeaza constant.
Un alt aspect important este pe ce echipamente folosim solutii antivirus. Este bine ca protectia antivirus sa fie pe mai multe nivele. Daca avem un echipament de retea prin care este filtrata antivirus toata informatia care vine din internet dar statiile de lucru nu au o solutie proprie antivirus este posibil ca un utilizator sa foloseasca un stick usb si sa infecteze toata reteaua. Pentru echipamentele de retea care filtreaza traficul internet in si dinspre internet sunt solutiile oferite de Fortinet si Juniper. Pentru statiile de lucru si servere exista solutiile antivirus oferite de Bitdefender, Kaspersky, Microsoft Forefront.

5. Cum sa te feresti de virusi, viermi, troieni (Elena)

* Virușii: programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componentele sistemului de operare sau alte programe informatice.
* Viermi: programe care se pot auto-replica. Acestia folosesc rețeaua de calculatoare pentru a-și trimite propriile copii în alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, în timp ce virușii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.
* Troieni: programe ce se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat.

În ceea ce privește securitatea calculatorului dumneavoastră, aveți în vedere următorii pași:
1. Verificați-vă calculatorul de infecții.
2. Instalați pachetele de servicii disponibile și actualizările de securitate pentru sistemul dumneavoastră. Activați actualizările automate.
3. Verificați regulat browser-ul de internet și plugin-urile încorporate (ex: Java, Flash, Shockwave, Quicktime).
4. Instalați un program antivirus și actualizați-l în mod regulat.
5. Folosiți un firewall, de exemplu Windows Firewall sau un router.

6. Ce sunt Cookie-urile (Elena)

Ce sunt cookie-urile de pe internet?

*Cookie-urile sunt fișiere care stochează informații despre tine, browser-ul tău web și comportamentul tău pe internet. Ele sunt fișiere foarte mici păstrate pe dispozitivul tău, ce pot fi folosite de site-urile sau de aplicațiile web pentru a ajusta experiența ta online.

Ce fac cookie-urile?
Un cookie este creat și interpretat de către expeditor, în timp ce destinatarul doar îl păstrează și îl trimite înapoi dacă expeditorul cere asta.
Atunci când navighezi pe internet, expeditorul este serverul care găzduiește un site web și destinatarul este browser-ul web care vizitează acel site. Scopul lor este de a identifica utilizatorul, de a verifica activitatea lui din trecut pe acel site și de a oferi conținut specific bazându-se pe aceste date.

Cookie-urile conțin doar date, nu și instrucțiuni executabile: ele nu pot să șteargă sau să citească nimic de pe PC-ul utilizatorului. Totuși, ele permit detectarea paginilor vizitate de un utilizator pe unul sau mai multe site-uri.

7. Hărțuirea online (Elena)

“Cyber bullying-ul implică utilizarea tehnologiilor informaționale și comunicaționale pentru a sprijini un comportament deliberat, repetat și ostil desfășurat de către un individ sau grup, care este destinat să aducă prejudicii altor persoane”.

bârfa: emiterea în mediul online a unor declarații speculative referitoare la o anumită persoană;

hărțuirea: luarea în batjocură constant și deliberat o persoană, prin postarea de mesaje publice, poze ce pot afecta integritatea psihică a individului;

urmărirea online: hărțuirea intimidantă cu scopul de a aduce conflictul și în viața reală (ex: de a solicita întrevederi în viața reală prin amenințare cu violență fizică);

trolling: provocarea unor persoane să acționeze agresiv, prin insultarea implicită;

comentarii: postarea de răspunsuri negative, denigrante la adresa unor persoane, la adresa unor fotografii, clipuri video sau mesaje lansate de o anumită persoană;

profiluri false: crearea unor profiluri false de catre agresorii pe internet, ce împrumută identitatea altor persoane pentru a facilita comunicarea cu victimele lor;

sexting: distribuirea de materiale pornografice minorilor, utilizând mijloacele electronice de comunicație.

Ce putem face pentru a opri un asemenea comportament?

1. Dacă hărțuirea se realizează pe o rețea de socializare (facebook, odnoklassniki, instagram, twitter etc.), trebuie să cunoașteți că :

- platformele au opțiuni de a raporta comentariile abuzive, hărțuirea sau spamul, ce pot duce la închiderea contului de pe care sunteți hărțuit.

- vă puteți seta contul în așa fel încât să fie mai puțin accesibil persoanelor cu care nu sunteți “prieteni”.

2. Dacă hărțuirea se realizează prin comentarii defăimătoare pe anumite site-uri sau bloguri, trebuie:

- să notificați proprietarul site-ului prin a solicita ștergerea informației care vă defăimează.

- să apelați la organele competente: poliție, procuratură, instanța de judecată.

- să apelați la un avocat sau un consultant juridic care să vă ajute să identificați și să elaborați o strategie de apărare, reieșind din circumstanțele particulare ale cazului dvs.

8. Reputatia in mediul online (Bogdan)

Cum îți construiești reputatia online

Pasul 1: Analizează-ți reputația actuală
În articolul anterior am discutat despre modul în care analizăm evolutia unui brand, fie în urma unei comunicări intense, fie pe parcursul acesteia. Pentru a realiza aceste evaluări, cel mai indicat este să folosim un instrument de media intelligence pentru a obține rapoarte de analiză cantitativă și calitativă a prezenței unui brand în presa online și în rețelele de socializare.
După cum am menționat în articolul anterior, pentru a evita timpul petrecut prin folosirea motoarelor de căutare și a rețelelor de socializare pentru a realiza manual rapoarte privind apariția brand-ului, este recomandată folosirea instrumentul de monitorizare media oferit de MediaIQ.
Pasul 2: Identifică punctele slabe
Analizează rapoartele obținute și găsește contextele negative în care brand-ul tău a fost menționat. Transformă toate aceste puncte slabe în priorități și găsește soluțiile necesare pentru a le transforma în puncte tari sau a le ascunde.
Dacă există un context negativ predominant, organizează o activitate publică sau distribuie un comunicat de presă prin care să descrii acea situație într-un mod favorabil pentru tine. Dacă există contexte negative de mică anvergură, precum un comentariu nepotrivit din partea unui fan pe Facebook, atunci răspunde în mod public persoanei respective. Nu este recomandat să îi ștergi comentariul –asta îl va înfuria și mai tare.
Pasul 3: Identifică punctele tari
Tot din analiza rapoartelor obținute la pasul 1, găsește-ți atuurile din comunicarea online. Acestea pot consta în:
Postări pe rețelele sociale care au generat interacțiunea mare și aprecieri;
Rețeaua socială care ți-a oferit cele mai multe link-uri;
Traficul și comentariile pozitive de pe blog;
Numărul de căutări pe Google ale brand-ului tău;
Comunicatele tale de presă care au generat reacții pozitive.
Este esențial să găsești mijloacele de comunicare online unde ai cele mai multe avantaje și să le folosești pe acelea pentru a-ți consolida reputația.
Pasul 4: Construiește-ți strategia de comunicare online
Având la dispoziție informațiile de mai sus, acum este momentul să îți adaptezi strategia de comunicare online (sau să începi să o construiești în caz că până acum nu a existat).

Află care sunt mijloacele de comunicare cele mai folosite de către publicul tău țintă și concentrează-te doar pe acelea. În funcție de analiza reacțiilor negative care îți pot afecta reputația, găsește un scop al comunicării online de acum înainte:
Să îți crești vizibilitatea (dacă nu există reacții la adresa ta în mediul online aproape deloc);
Să îți îmbunătățești reputația (dacă există mai multe reacții negative decât pozitive);
Să îți menții reputația (dacă există mai multe reacții pozitive decât negative – cazul ideal).
Adaptează-ți conținutul pentru fiecare mijloc de comunicare online folosit:
Articole de blog;
Comunicate de presă;
Postări pe rețelele de socializare.
Pasul 5: Construiește-ți reputatia online!
Ultimul pas este punerea în aplicare a planului realizat la pasul anterior, prin crearea de conținut și folosirea mijloacelor de comunicare corespunzătoare pentru construirea unei reputații online.
În timp ce îți desfășori activitățile de comunicare este esențial să folosești un instrument de monitorizare media, precum cel oferit de MediaIQ, pentru a depista orice reacție negativă față de brand-ul tău și a răspunde din timp la acestea.
Menține o comunicare constantă și un mesaj unitar prin intermediul tuturor mijloacelor folosite. Cu o strategie bine pusă la punct, un mesaj solid și un instrument de monitorizare media, nimic nu îți va sta în calea construirii unei reputații online de lungă durată!

9. SPAM-urile (Elena)

*Spam-urile - mesajele nesolicitate trimise unui utilizator de servicii de mesagerie electronică (poşta electronică) sau de telefonie mobilă – în acest caz : spam prin SMS.
*Spam-ul este acel mesaj al cărui expeditor nu se regăseşte în lista de contacte (sau de cunoştinţe) a destinatarului, prin care are loc utilizarea abuzivă a serviciilor de poştă electronică în scopuri publicitare sau de inducere în eroare (înşelare) a destinatarului.
Mesajele spam, deși nu sunt un program malițios în sine, pot include atașamente care conțin astfel de programe, sau trimit utilizatorii către pagini de internet periculoase pentru siguranța sistemului.

Care sunt principalele canale de raspândire amesajelor de tip spam?
Spamurile se gasesc:

- pe e-mail, pentru ca majoritatea oamenilor detin o adresa de e-mail, folosita fie in scop professional, fie personal
- sub forma de comentarii la diverse bloguri (cu cat au o mai mare vizibilitate cu atat vor fi si mai mult targetate)
- sub forma de mesaje pe forumuri
- pe retelele sociale
- prin SMS - este dificil de detectat, pentru ca este foarte variat si localizat.

Care sunt pericolele la care sunt expusi utilizatorii când deschid astfel de mesaje? Cele mi importante pericole

- Mesajele de tip phishing - pot fi extrem de daunatoare, pentru ca ele pretind a veni din partea unei institutii(uneori bancare, uneori nu) si de vreme ce mesajele de acest tip

inca exista (si chiar creste numarul lor) inseamna ca sunt suficient de multe victime pentru ca afacerea sa aiba succes.

- Infectarea calculatorului prin deschiderea unui link periculos dintr-un spam, prin download-ul si rularea unui executabil, prin deschiderea unui eventual atasament infectat etc. Dupa infectarea calculatorului, pericolele pot sa capete forme variate in functie de tipul de malware cu care s-a infectat

Cum se pot feri utilizatorii de mesajele spam?
Utilizatorii trebuie sa aiba un produs de Securitate complet, care sa contina si modulul Antispam. In lipsa lui, utilizatorul nu va fi niciodata protejat 100%.

10. Securitatea informatiilor (Bogdan)

11. Securitatea aplicatiilor (software) (Bogdan)

Echipa noastră globală care se ocupă de securitatea software-ului depune mari eforturi pentru a proteja activele informaționale, serviciile și produsele Sony Mobile, precum și confidențialitatea informațiilor clienților. Dar suntem întotdeauna dornici de mai mult ajutor. Recunoaștem rolul important pe care comunitatea de cercetare îl joacă în consolidarea poziției noastre privind securitatea și salutăm oportunitatea de a colabora cu comunitatea respectivă. Programul Sony Mobile privind securitatea software-ului acceptă raportarea de erori care-i asigură unui potențial atacator capacitatea să compromită integritatea, disponibilitatea sau confidențialitatea produselor, a serviciilor sau a infrastructurii IT a Sony Mobile și care respectă **instrucțiunile noastre de remitere..** În cazul în care considerați că ați descoperit o vulnerabilitate validă privind securitatea într-un produs sau site Web Sony Mobile, dorim să ne aduceți la cunoștință acest lucru.
Dacă doriți să remiteți o vulnerabilitate, vizitați adresa **https://hackerone.com/sony.** Veți fi redirecționat la un site terț unde veți găsi mai multe informații privind instrucțiunile de remitere și veți putea remite un raport. Ne vom strădui să investigăm cu promptitudine informațiile primite.
Alte tipuri de asistență
Dacă întâmpinați dificultăți care nu au legătură cu securitatea software-ului, de exemplu, la descărcarea și instalarea de actualizări, sau dacă aveți nevoie de asistență suplimentară pentru telefon, contactați **asistența Sony Mobile.**
Soluțiile software de securitate a sistemelor sunt instrumente cu rol în detectarea și eliminarea virușilor, lucrând activ la îmbunătățirea principiilor de apărare a computerelor. Cele mai importante module ale sistemelor de securitate sunt cele de scanare, diagnosticare și protejare împotriva programelor de tip spion, viruși, cai troieni sau multe altele.

12. Spyware si Keyloggers (Elena)

* Spyware: o categorie de software maliţios, ataşate de obicei la programe gratuite (jocuri, programe de schimbat fişiere, programe de video chat etc.), care captează pe ascuns date de marketing (prin analiza site-urilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ş.a.m.d.) şi le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

În general, chiar după ștergerea programelor gratuite care au instalat programul spion, acesta rămâne în continuare activ. Există și numeroase programe anti-spion, dar atenție: unele dintre ele sunt false antispyware - inducând utilizatorul în eroare deoarece ele însele conțin programe spion mascate.

Pentru înlăturarea programelor spion sunt folosite programele antispyware

*Keyloggers: troieni care ruleaza in background si inregistreaza tot ceea ce se introduce de la tastatura, permitand unui utilizator extern sa aiba acces la continutul introdus. In majoritatea cazurilor este vorba despre conturi de e-mail si parole, conturi de instant messenger, carduri de credit, parole de la domeniul personal s.a.m.d.

Cum se detecteaza?

Cea mai simplă modalitate de a detecta orice software nedorit este să te uiți în Managerul de activități pentru a verifica procesele care rulează.

Cum ne putem proteja de aceste programe „rau facatoare”?

Antrivirusi cu licenta sau versiuni open source actualizate la timp, un firewall cu licenta sau open source la fel cu update-urile la zi. Acest lucru va scadea rata dumneavoastra de infectare cu pana la 90% .

13. Securitatea in reţelele Wi-Fi (Bogdan)

Majoritea utilizatorilor de internet folosesc conexiunea Wi-Fi , cu ajutorul unui laptop, telefon, etc. şi în multe cazuri dacă aceste reţele nu sunt securizate oricine se poate conecta fără probleme (nesecurizat – fără parolă de acces). Ţinând cont că majoritatea hotspot-urilor nu folosesc criptare, ar trebui să fiţi conştienţi că traficul de internet poate fi văzut de oricine. Anumite echipamente Wi-Fi oferă posibilitatea administrării via wireless şi cel mai bine ar fi să blocaţi acest feature pentru o securitate mai ridicată. Majoritatea echipamentelor noi au posibilitatea alegerii unei criptări : WPA + WPA2 , avantaj fiind compatibilitatea cu adaptoarele WPA. Obs: Să alegeţi o criptare WPA, WPA2 sau WPA + WPA2, o parolă de minim 10 caractere (cât mai complex şi schimbarea ei la o perioadă de 3-6 luni) pentru o securitate mai ridicată. Echipamentele Wi-Fi, de obicei au by default SSID-ul (un identificator unic) pentru a evita interferenţele dintr-o reţea wireless. Accesul la Wi-Fi se poate securiza şi mai mult cu ajutorul setărilor din echipamentul avut. Obs: Limitarea DHCP pentru controlul numărului de ip-uri care doriţi să le permiteţi accesul la reţeaua wireless. Un alt sfat pentru o securitate mai bună a echipamentului Wi-Fi, ar fi poziţionarea acestuia în casă cât mai central, cât mai departe de fereastră ca să nu poată fi accesat din exterior (semnalul să fie cât mai slab, sau inexistent).

14. Comunicarea pe rețele de socializare (Elena)

Reguli de securitate în cadrul rețelelor sociale

* Alegeți o parolă pentru contul dumneavoastră care să nu fie ușor de ghicit de către un alt utilizator sau program. Evitați parolele generice, precum ”123456789” sau ”parola” sau o parolă identică cu numele de utilizator;
* Asigurați-vă că știți pe cine urmăriți și pe cine adăugați drept prieten
* Evitați să accesați link-urile împărtășite de către alți utilizatori;
* Evitați să faceți publice informații personale, precum ziua de naștere, adresa de e-mail sau adresa domiciliului;
* Atunci când împărtășiți poze, asigurați-vă că o faceți doar cu persoanele cunoscute
* Nu dezvăluiți niciodată informații referitoare la perioadele în care părăsiți locuința (mesaje precum: ”plec la mare tot weekend-ul; ”sunt singur acasă” trebuie evitate)
* Utilizați o soluție de securitate specializată, care să scaneze mesajele și comentariile, și care să verifice nivelul de securitate al informațiilor confidențiale;

Dezavantajele comunicării pe rețele

- Nu ai siguranta ca cel cu care discuti este cu adevarat cel care se pretinde. Nu poti identifica identitatea acestuia.
- Nu poti verifica cat este de sincer cu tine celalalt atunci cand aveti o comunicare virtuala.
- Avand o comunicare virtuala, nu poti urmari mesajele non-verbale si paraverbale (ex. zambetul, privirea, tonul vocii).
- Poti fi tradat, in cazul in care ai prea multa incredere in prietenul cu care ai o comunicare virtuala.

Avantaje

Procesul de comunicare virtuala este avantajos in cazul persoanelor care se cunosc in lumea reala,intrucat nu ofera vreun risc.

- Poti comnica cu rude si prieteni ce se afla la o mare distanta
- Iti poti crea noi prietenii si relatii care ti-ar oferi noi oportunitati.
- Costurile comunicarii sunt mult reduse, singura plata fiind abonamentul la internet.
- Singur decizi daca vrei o astfel de comunicare virtuala.
- Singur alegi cu cine discuti si cat discuti

15. Ce este phishingul? (Bogdan)

Phisingul constă în trimiterea de e-mailuri care au ca şi expeditor fals diverse instituţii cu care potenţiala victimă are anumite relaţii (de ex: bănci, magazine on-line etc). Aceste e-mailuri de obicei direcţionează userii către anumite site-uri unde sunt rugaţi să-şi actualizeze diverse informaţii sau să introducă date personale. La prima vedere tentativele de phishing pot trece neobservate însă sunt câteva lucruri de care ar trebui să ţinem cont atunci cand primim un e-mail ce pare a fi de la una din insituţiile cu care colaborăm. De regulă toate urmează aceeaşi structură. Introducerea Salutul este generic, de exemplu : “Stimate client”. De obicei companiile cu care colaboraţi, personalizează e-mailurile cu numele dumneavoastră. Majoritatea companiilor nu procedeaza aşa, este puţin probabil ca un colaborator de-al dumneavoastră să vă solicite informaţii confidenţiale prin e-mail. Linkurile pe care ar trebui să daţi click sunt mai lungi în comparaţie cu cele obişnuite şi adesea conţin simbolul @. Cum ne putem proteja? Persoanele din spatele phisingului se bazează pe naivitatea utilizatorilor. Nu există o metodă de protecţie 100% sigură atâta timp cât totul depinde de factorul uman. Practic orice utilizator de

e-mail este o potenţiala victimă. Cunoscând cele câteva reguli esenţiale despre comunicarea prin e-mail şi luându-ne toate măsurile de precauţie, ne putem feri de astfel de răufăcători.