I. REGULI PRIVIND UTILIZAREA SERVICIULUI DE MESAGERIE ELECTRONICĂ AL UNIVERSITĂȚII DIN PITEȘTI

Serviciul de mesagerie electronică al Universității din Pitești este destinat pentru efectuarea comunicărilor în interes de serviciu, atât în interiorul instituției cât și în exteriorul acesteia.

Având în vedere importanța serviciului de e-mail pentru buna desfășurare a misiunilor și activităților specifice ale Universității, este necesar ca toți utilizatorii să cunoască și să respecte un set de reguli și proceduri de operare, menite să asigure funcționarea corespunzătoare a acestui serviciu. Spațiul cibernetic contemporan se caracterizează printr-o creștere și diversificare a aplicațiilor malware și a atacurilor informatice care au ca efect îngreunarea sau chiar imposibilitatea utilizării serviciului de e-mail. Dintre acestea, cele mai des întâlnite sunt spam-urile (mesajele nesolicitate) și atacurile de tip phishing (înșelăciune electronică).

Phishing-ul este o formă de activitate infracțională prin care se încearcă obținerea de informații confidențiale (ex. nume de utilizator, parole, detalii despre carduri bancare etc.) folosind tehnici de manipulare a datelor identității unei persoane sau a unei instituții. Prin astfel de mesaje victima este sfătuită să-și dea datele personale pentru a câștiga anumite premii, sau este informat că acestea sunt necesare datorită unor erori tehnice care au dus la pierderea datelor originale.

Phishing-ul este de obicei efectuat prin e-mail spoofing (falsificarea adresei de email a expeditorului) sau mesaje instant, şi de multe ori direcţionează utilizatorii să introducă detalii confidențiale pe un site fals al cărui aspect este aproape identice cu cel legitim. Mai nou a apărut conceptul de spearphishing. Acesta este similar cu phishing-ul, diferența majoră constând în faptul că atacul vizează ținte clar identificate.

Având în vedere aspectele menționate, a fost creat următorul set de reguli privind utilizarea serviciului de mesagerie electronică:

1. Activităţi interzise

- ✓ Transmiterea/re-transmiterea de e-mailuri în lanț.
- ✓ Transmiterea de mesaje cu caracter de intimidare sau hărţuire.
- ✓ Folosirea e-mailului de serviciu în scopuri personale.
- ✓ Folosirea e-mailului de serviciu în scopuri politice.
- ✓ Distribuirea neautorizată a documentelor protejate de drepturile de autor;
- ✓ Folosirea altei identităţi decât cea reală pentru transmiterea de masaje;
- ✓ Transmiterea de mesaje nesolicitate către grupuri de persoane, cu excepția situațiilor în care acestea deservesc instituția;
- ✓ Transmiterea de atașamente de dimensiuni foarte mari;
- ✓ Transmiterea de atașamente sau link-uri susceptibile de conținut malițios.
- ✓ Ignorarea solicitărilor administratorului de eliberare a spațiului ocupat, la atingerea limitei maxime alocate casuței de e-mail.

2. Alte menţiuni

- ✓ În exercitarea atribuțiilor de serviciu, tot personalul instituției va folosi adresele configurate pe serverul de e-mail al Universității din Pitești (domeniul upit.ro)
- ✓ Toate informaţiile şi datele cu cracter confidenţial, transmise către alte reţele externe, trebuie să fie protejate.
- ✓ Utilizatorii nu trebuie să transmită sau să primească informaţii confidenţiale ce privesc Universitatea din Pitești, folosind conturi de utilizator configurate pe servere care nu sunt proprietate a Universității (ex. Yahoo mail, Gmail, Hotmail, AOL mail etc.).
- ✓ Utilizatorii nu trebuie să transmită, primească sau să stocheze informaţii confidenţiale ce privesc Universitatea din Pitești folosind dispozitive care nu sunt autorizate (ex. laptop-uri/notebook-uri

personale, telefoane mobile, asistenţi digitali personali (PDA), pagere ce permit trimiterea/primirea de informaţii).

II GHID DE BUNE PRACTICI PRIVIND UTILIZAREA SERVICIULUI DE EMAIL

Pentru evitatea incidentelor care pot crea disfuncționalități ale serviciului de e-mail, ducând uneori chiar la imposibilitatea utilizării serviciului, se impune respectarea unui set minim de recomandări, după cum urmează:

- Nu accesați link-urile primite prin e-mailuri care solicită actualizarea informațiilor personale. Entitățile legitime nu îți vor cere niciodată să furnizezi sau să verifici informații sensibile printr-un mijloc nesigur, precum e-mailul.
- Prima regulă a navigatului pe Internet este să rămâi cât mai anonim posibil. Aceasta înseamnă să nu faci publice informațiile personale (numele complet, adresa, numărul de telefon, CNP-ul, parole, nume ale membrilor de familie, numere de cărți de credit). Majoritatea oamenilor și companiilor credibile nu îți vor cere să le comunici astfel de date pe Internet.
- Nu deschide atașamentele aferente unor e-mailuri venite din partea unor expeditori necunoscuți. Cea mai frecventă metodă de răspândire a aplicaţiilor maliţioase este prin email. Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text sau printr-un titlu interesant al ataşamentului, însă ataşamentul lansează în fapt un virus sau o altă aplicaţie maliţioasă. Ca atare, este indicat să nu deschideţi ataşamentele despre care nu sunteţi convinşi că sunt documente utile.
- Link-urile nu sunt întotdeauna ceea ce par a fi: verificaţi-le înainte de a le deschide. Pentru a vedea adevărata resursă URL ce se ascunde în spatele unui link, ține pointerul mouse-ului deasupra link-ului și vei observa, de obicei în partea stângă-jos a ferestrei, link-ul real.
- Nu rula programe a căror origine nu poate fi verificată.
- Fii întotdeauna sceptic când primești o ofertă ce sună foarte tentant. Multe tehnici de phishing încearcă să te păcălească în a oferi date personale.
- Dacă primești un e-mail de la cineva cunoscut dar care are un subiect nefamiliar, șterge mesajul fară să-l deschizi. La o noua apariție, raportează-l ca spam.
- Dacă primești un e-mail care te informează că ai câștigat ceva, sterge-l fără să mai stai pe gânduri.
- Dacă primești un e-mail care pare de la o adresă cunoscută dar care are conținutul scris neglijent gramatical (ca si cum s-ar fi folosit Google Translate), șterge-l fără să mai stai pe gânduri. Există tehnici care permit trimiterea de mesaje de la adrese de email cunoscute. Se poate întâmpla să primesti astfel de e-mailuri chiar de la tine.
- Dacă primești un e-mail de la o adresă cunoscută, cu conținut corect gramatical, dar care îți solicită să accesezi un link necunoscut, nu face asta. Șterge imediat e-mailul.
- Nu răspundeţi mesajelor spam. Dacă o faceţi, veţi confirma adresa dvs. de e-mail celor care v-au trimis spam-ul. Nu aveți garanția că toate link-urile care promit să vă elimine din lista lor de distribuţie sunt veridice. Răspunsurile automate de genul “absent din birou” de asemenea creează o problemă, deoarece aceste mesaje răspund atât persoanelor autorizate, cât și spamerilor.
- Evitaţi să expediaţi adresa dvs. de e-mail unui număr mare de persoane. Reţineţi că dacă plasaţi e-mailul dvs. pe o pagină web, roboţii (web crawlers) o pot include în lista de distribuţie a spam-ului.