**Ce este Phsihing?**

Phishing este o formă de criminalitate cibernetică în care un adversar imită o persoană sau o instituție și se prezintă ca agent sau entitate, in cele mai multe cazuri prin trimiterea unui e-mail. Prin acest tip de cyberattack, un atacator trimite link-uri rău intenționate sau atașamente care pot efectua diverse funcții, printre care si colectarea informatiilor personale sau de cont ale victimei. Aceste mesaje dăunează victimelor în ceea ce privește pierderea de bani sau furtul de identitate.

Phishing este definită ca fiind colectarea frauduloasă a datelor confidențiale și folosirea necorespunzătoare a acestora. În general, sunt necesare informații personale, cum ar fi numărul cardului de credit sau parola contului. Atunci când utilizatorii vizitează acest site, aceștia sunt rugați să furnizeze informații personale care sunt trimise ulterior atacatorului.

Phishingul este o formă larg răspândită de cyberattack, de care toată lumea ar trebui să învețe să se protejeze. Există diferite moduri prin care atacatorii dobândesc informațiile necesare pentru acest acl fraudulos. În unele cazuri, malware-ul este descărcat direct pe computerul victimei, iar escrocii beneficiază de faptul ca detin informatii personale sau ale cardului de credit.

In multe cazuri, o organizatie este tinta unui asemenea atac si nu o persoana.

În situații ca aceasta, e-mailurile sunt trimise angajaților pentru a obține acreditări sau alte informații confidențiale necesare pentru un atac avansat. Cyberatack-urile, cum ar fi Advanced Persistent Threats (APT) și ransomware, încep de multe ori cu phishing.

Pentru ca atacul să aibă succes, e-mailul expediat trebuie să pară demn de încredere și important pentru victimă. Prin urmare, atacatorii folosesc adesea rețelele de socializare pentru a afla cât mai multe informații despre interesele victimei, cercurile sociale, istoria personală și de lucru etc. După colectarea acestor informații, aceștia sunt capabili să creeze un e-mail perfect personalizat, care ar putea înșela o persoană.

Cum detectam un asemenea atac?

În afară de faptul că trebuie să fim mereu vigilenți și să punem la îndoială orice e-mail neașteptat, mai ales atunci când suntem rugați să descărcăm un program / software / fișier sau să actualizăm datele de logare in anumite conturi, de asemenea se pot identifica și e-mailuri rău intenționate observand greșeli de ortografie în cadrul conținutului sau chiar la link-ul URL.

Masuri de precautie

Primul pas pe care îl puteți lua pentru a vă proteja împotriva acestor atacuri este de a devini informati despre ceea ce implică și de modul de identificare a unui astfel de atac. Există, desigur, metode, cum ar fii utilizarea unui filtru de poștă electronică care poate capta și reduce numărul de e-mailuri de phishing.