ÇFARË ËSHTË SPOOFING (MASHTRIMI)?

Spoofing (Mashtrimi) ndodh kur një kriminel kibernetik maskohet si një individ, biznes ose ent tjetër për të kryer veprime keqdashëse.

Pavarësisht nga taktikat e përdorura, qëllimi i një mashtruesi kibernetik është të vjedhë nga viktimat dhe të dëmtojë reputacionin e tyre. Kriminelët kibernetikë përdorin teknika të zakonshme të inxhinierisë sociale si, përdorimi i adresave të rreme emaili, faqe interneti ose numra telefoni të rreme, për të mashtruar viktimat për marrjen e informacionin konfidencial, shkarkimin e bashkëngjitjeve ose klikimin në linket që instalojnë malware.

Mashtruesit i shpërqëndrojne viktimat duke përdorur entitete me të cilat shumica e njerëzve janë të njohur, si markat e njohura, institucionet financiare, zyrat qeveritare, etj.

Disa mënyra për të dalluar mashtrimet

Të dhëna për faqet e rreme në internet

- Nëse mungon ikona e drynit në fushën e adresave të një faqe interneti, faqja e internetit nuk është e sigurt dhe mund të jetë e falsifikuar.
- URL-ja fillon me http dhe jo https. Mos u besoni faqeve të internetit që nuk përdorin https.
- Shumë faqe interneti për tu loguar, plotësojnë automatikisht emrin e përdoruesit dhe fjalëkalimin. Duhet përdorur një menaxher fjalëkalimi për të ruajtur të dhënat e logimeve në faqe të ndryshme, për t'u mbrojtur ndaj logimit automatik në një faqe interneti të falsifikuar. Nëse menaxheri i fjalëkalimit nuk e njeh faqen e internetit, ai nuk do të plotësojë automatikisht të dhënat e logimit.
- Gabimet drejtshkrimore, linke që nuk hapin faqe interneti, informacioni i dyshimtë tek kontaktit me ne në faqen e internetit, mungesa e simboleve identifikues të mediave sociale, mund të janë të gjitha tregues që faqja e internetit është e rreme.
- Adresat e faqeve të internetit që përmbajnë emrin e domenit të rremë dhe jo domein zyrtar.

Të dhëna për adresa emaili-i të rremë

- Gabimet drejtshkrimore ose një emër domaini i pasaktë në adresën e emailit të dërguesit tregojnë një email të falsifikuar.
- Gjuha e emailit që nxit të veproni shpejt, të transferoni para ose të jepni informacion konfidencial.
- Përmban URL që nuk i njihni. Lëvizni mousin mbi URL ose theksoni URL-në përpara se të klikoni për të kontrolluar legjitimitetin e tyre.
- Gabimet drejtshkrimore, gramatikore dhe gjuha e panjohur tregojnë se emaili nuk vjen nga një burim i vërtetë.
- Bashkëngjitjet dhe mesazhi i emailit që nxit të shkarkohet bashkëngjitja. Verifikoni nëse bashkëngjitja nuk ka një prapashtese EXE në emrin e saj.

Të dhënat e rreme të ID së telefonuesit, mesazhit tekst ose të SMS-ve

- Nëse numri i telefonit shfaqet pa kllapa () ose viza -. Për shembull, 355682062865.

- ID-ja e telefonuesit është numri juaj i telefonit ose duket shumë i ngjashëm (p.sh.,ndryshon një shifër).
- Numri i telefonit ose emri i telefonuesit janë të fshehura.

Si të parandalohet mashtrimi?

1. Zbatoni kontrollet dhe procedurat teknike për t'u mbrojtur nga spoofing (mashtrimet) e postës elektronike, uebsajtit, etj.

2. Vendosni në fokus edukimin e ekipit tuaj rreth inxhinierisë sociale. Edukoni ekipin se si ndodh inxhinieria sociale duke përdorur trajnime dhe skenarë të botës reale për të treguar se sa e lehtë është të mashtrohesh nga inxhinieria sociale.

3. Kujtojuni punonjësve për rreziqet që vijnë me anë të adresës së emailit. Përdorni simulimet, buletinet dhe fushatat e komunikimit për ti mbajtur koherent punonjesit në lidhje me spoofing (mashtrimin) dhe sigurinë kibernetike.

4. Sigurohuni që të gjitha aplikacionet, sistemet operative, shfletuesit, mjetet e rrjetit dhe softueri i brendshëm të jenë të përditësuar dhe të sigurt. Instaloni softuerë për mbrojtjen e malware dhe anti-spam.

5. Kryeni fushata trajnimi të rregullta rreth ndërgjegjësimit për sigurinë që u kujtojnë personave rreziqet e publikimit në internet të informacionit konfidencial, fjalëkalimeve, të dhënave të organizatës dhe detajeve të kartës së kreditit.

6. Edukoni ekipin rreth spoofing (mashtrimit). Përdorni softuer simulues dhe trajnime që përfshin shembuj të jetës reale të sulmeve të spoofing (mashtrimit).

7. Monitoroni rregullisht nivelet e ndërgjegjësimit të punonjësve me simulime, për spoofing (mashtrimet), inxhinierinë sociale dhe kërcënimet e tjera kibernetike.

Si ndihmojnë simulimet e phishing në mbrojtjen nga spoofing (mashtrimi)

Ndërsa spoofing (mashtrimi) dhe phishing janë lloje të ndryshme të sulmeve kibernetike, phishing për të pasur sukses mbështetet në spoofing (mashtrim).

Simulimet e phishing janë ideale për të matur ndërgjegjësimin e punonjësve për inxhinierinë sociale dhe rreziqet që vijnë nga posta elektronike.

Punonjësit mësojnë te dallojnë se si përdoret gjuha e zgjuar në email për të vjedhur informacione konfidenciale dhe të dhëna të korporatës.

Simulimet e phishing i aftësojnë punonjësit që të mbrohen nga sulmet e spoofing (mashtrimit), në këto mënyra kryesore:

1. Redukton nivelin e rrezikut të kërcënimit kibernetik.

2.Rrit ndërgjegjësimin dhe vigjilencën për rrezikun e inxhinierisë sociale dhe spoofing (mashtrimit).

3. Mat shkallët e cënueshmërisë së korporatave dhe punonjësve.

4. Nxit një kulturë rreth ndërgjegjësimit për sigurinë dhe zhvillon heronj të brendshëm kibernetikë.

5. Përforcon mesazhet për nevoja për trajnime rreth ndërgjegjësimit për sigurinë.

6. I mban punonjësit vigjilentë ndaj spoofing (mashtrimeve), phishing dhe sulmeve të inxhinierisë sociale.

7. Vlerëson performancën e trajnimeve rreth ndërgjegjësimit për sigurinë kibernetike.