Phishing

1. Ի՞նչ է ֆիշինգը:

Ֆիշինգը կիբեռհանցագործության տեսակ է, որի նպատակն է ստանալ որևէ սոցիալական կայքի օգտատիրոջ գաղտնի տվյալները, ծածկագիրը և ծածկանունը: Սա կատարվում է զանգվածային էլեկտրոնային սպամ նամակների միջոցով, որոնք հասցեատիրոջը հասնում են հայտնի բրենդների անունից, ինչպես նաև տարբեր ծառայությունների վերաբերյալ անձնական նամակներ, օրինակ բանկի կամ սոցիալական ցանցերի կողմից: Նամակը հաճախ պարունակում է ուղղակի կայքի հղումը, որը արտաքնապես չի տարբերվում իրական նույն կայքից: Այն բանից հետո, երբ հաղորդագրության օգտատերը ստանում է կեղծ էջը, խաբեբաները (հաքերները) տարբեր հոգեբանական հնարքներով փորձում են դրդել օգտատիրոջը մուտք գործել կեղծ էջ՝ իրենց իրական մուտքանունը և գաղտնաբառը լրացնելով, որը հաքերներին թույլ է տալիս մուտք գործել դեպի օգտատիրոջ բանկային հաշիվ կամ ակաունտ:

2. Ի՞նչ եղանակներով են իրականացնում ֆիշինգը:

- **Email phishing**:

Հարձակվողները նամակներ են ուղարկում, որոնք կարծես վստահելի աղբյուրից են, օրինակ՝ բանկից կամ հեղինակավոր ընկերությունից: Այս նամակները հաճախ հրատապության զգացում են պարունակում՝ խրախուսելով ստացողներին սեղմել վնասակար հղումների վրա կամ տրամադրել անձնական տեղեկատվություն:

- **Spear phishing**:

Սա նպատակաուղղված ֆիշինգային հարձակում է, որն օգտագործում է էլ. նամակներ՝ որոշակի անհատի կամ կազմակերպությանը խաբելու համար, որպեսզի հավատան, որ դրանք օրինական են: Այն հաճախ օգտագործում է թիրախի մասին անձնական տեղեկատվություն հաջողության շանսերը մեծացնելու համար: Այս հարձակումները

հաճախ ուղղված են ղեկավարներին կամ ֆինանսական գերատեսչություններին, որոնց հասանելի են զգայուն ֆինանսական տվյալներ և ծառայություններ:

- **SMS phishing**:

Ֆիշինգի այս տեսակն օգտագործում է բջջային հեռախոսից կամ սմարթֆոնից ստացված տեքստային հաղորդագրությունները՝ խայծ հաղորդագրություն փոխանցելու համար: Թիրախին սովորաբար խնդրում են սեղմել հղման վրա, զանգահարել հեռախոսահամարով կամ կապվել հարձակվողի կողմից տրամադրված էլ.փոստի հասցեի հետ: Այնուհետև նրանց կարող է պահանջվել տրամադրել անձնական տեղեկատվություն, օրինակ՝ այլ կայքերի մուտքի հավատարմագրերը:

- **Voice phishing**:

Այս տեսակի միջոցով հարձակվողները ավտոմատացված հեռախոսազանգեր են կատարում մեծ թվով մարդկանց, հաճախ օգտագործելով ավտոմատ պատասխանիչներ՝ պնդելով իրենց հաշիվների վրա խարդախության գործողությունների իրականացման վերաբերյալ փաստարկներ: Հարձակվողները կատարում են զանգը իբրև որևէ օրինական բանկի կամ հաստատության անունից: Այնուհետև զոհին հուշում են մուտքագրել տեղեկատվություն կամ կապվել կենդանի անձի հետ, ով օգտագործում է սոցիալական ինժեներական մարտավարություն տեղեկատվություն ստանալու համար:

3. Ի՞նչ միջոցներ են կիրառում վեբ ֆիշինգ իրականացնելու համար:

1. Խաբուսիկ տիրույթի անուններ.

Ֆիշերները հաճախ գրանցում են տիրույթի անուններ, որոնք շատ նման են օրինականներին: Այս խաբուսիկ տիրույթները կարող են օգտագործել տառասխալներ, գծիկներ կամ այլ տարբերակներ՝ օգտատերերին համոզելու համար, որ այցելում են վստահելի կայք:

2. URL մանիպուլյացիա.

Ֆիշերները կարող են շահարկել URL-ը՝ ավելացնելով պարամետրեր կամ փոխելով վեբ հասցեի մասերը՝ խաբուսիկ հղում ստեղծելու համար: Սա կարող է հղումը դարձնել օրինական՝ օգտատերերին ֆիշինգի կայք վերաուղղորդելիս:

3. Հոմոգրաֆ

Հոմոգրաֆը ներառում է նիշերի օգտագործում, որոնք նման են, բայց ունեն տարբեր Յունիկոդ ներկայացումներ: Օրինակ՝ օգտագործելով տարբեր սկրիպտների նիշերը, որոնք տեսողականորեն նման են անգլերեն տառերին, կարող են ստեղծել URL-ներ, որոնք օրինական տեսք ունեն, բայց հանգեցնում են ֆիշինգի կայքերի:

4. Man-in-the-Middle (MITM) հարձակումներ.

MITM հարձակման ժամանակ հարձակվողը ընդհատում է օգտատիրոջ և օրինական կայքի միջև հաղորդակցությունը: Հարձակվողը կարող է փոխել վեբ էջի բովանդակությունը, օգտվողներին վերահղել դեպի ֆիշինգ կայք կամ գրավել զգայուն տեղեկատվություն:

5. Թռուցիկ պատուհաններ

Ֆիշերը կարող է ստեղծել թռուցիկ պատուհաններ, որոնք ընդօրինակում են մուտքի օրինական ձևերը կամ մուտքագրման այլ դաշտերը: Օգտատերերը, ովքեր տեղեկատվություն են մուտքագրում այս կեղծ թռուցիկների մեջ, անգիտակցաբար տրամադրում են իրենց հավատարմագրերը ֆիշինգի կայքին:

6. JavaScript վերահղում.

JavaScript-ը կարող է օգտագործվել օգտատերերին օրինական կայքից ֆիշինգ կայք վերահղելու համար: Սա կարող է առաջանալ մեկ այլ կոդի միջոցով, որը միացվել է վտանգված կայքերին կամ տարածվել էլփոստի հավելվածների կամ հղումների միջոցով:

7. Վնասակար բրաուզերների ընդարձակումներ.

Ֆիշերները կարող են ստեղծել բրաուզերի վնասակար ընդլայնումներ, որոնք տեղադրվելուց հետո փոփոխում են վեբ էջերը, գրավում օգտատերերի մուտքերը կամ օգտատերերին վերահղում դեպի ֆիշինգ կայքեր: Այս ընդլայնումները հաճախ քողարկվում են որպես օգտակար գործիքներ:

8. Որոնիչի միջոցով

Ֆիշերները շահարկում են որոնման արդյունքները՝ ֆիշինգ կայքերը խթանելու համար: Օպտիմիզացնելով վնասակար էջերը հանրաճանաչ որոնման տերմինների համար՝ հարձակվողները մեծացնում են օգտվողների՝ իրենց խաբուսիկ հղումների վրա սեղմելու հավանականությունը:

9. Կայքային սկրիպտավորում (XSS):

Կայքերում XSS խոցելիությունները կարող են շահագործվել հարձակվողների կողմից՝ այլ օգտվողների կողմից դիտված վեբ էջերում վնասակար սկրիպտներ ներարկելու համար: Այս սկրիպտները կարող են այնուհետև վերահղել օգտվողներին դեպի ֆիշինգ կայքեր կամ գողանալ զգայուն տեղեկատվություն:

10. Բովանդակության կեղծում.

Ֆիշերը կարող է ստեղծել կեղծ կայքեր, որոնք նմանակում են օրինական կայքերի բովանդակությունն ու տեսքը: Բովանդակության կեղծումը ներառում է դասավորության, լոգոների և դիզայնի այլ տարրերի պատճենում՝ օգտատերերին խաբելու համար, որպեսզի կարծեն, թե վստահելի կայքում են:

11. Tabnabbing.

Tabnabbing-ը տեղի է ունենում, երբ բրաուզերի բաց ներդիրը փոխարինվում է ֆիշինգի էջով, մինչդեռ օգտատերը կենտրոնացած է մեկ այլ ներդիրի վրա: Այս տեխնիկան օգտվում է օգտվողներից, ովքեր կարող են չնկատել ներդիրի փոփոխությունը:

4. Ի՞նչպես պաշտպանվել ֆիշինգից:

Ֆիշինգից պաշտպանվելը պահանջում է տեղեկացվածության, առցանց զգուշավոր վարքագծի և տեխնիկական նախազգուշական միջոցների համադրություն: Ահա մի քանի խորհուրդներ, որոնք կօգնեն ձեզ խուսափել ֆիշինգի հարձակումների զոհ դառնալուց.

1. Եղեք թերահավատ նամակների և հաղորդագրությունների նկատմամբ.

Հղումների վրա սեղմելուց կամ հավելվածները բացելուց առաջ ստուգեք ուղարկողի էլփոստի հասցեն: Զգույշ եղեք անսպասելի նամակներից, հատկապես այն նամակներից, որոնք ձեզ կոչ են անում անհապաղ միջոցներ ձեռնարկել կամ տրամադրել զգայուն տեղեկատվություն:

2. Ստուգեք տառասխալների և կասկածելի URL-ների համար.

Զգուշորեն ստուգեք URL-ները տառասխալների, լրացուցիչ նիշերի կամ անսովոր տիրույթների համար: Սավառնեք հղումների վրա՝ առանց սեղմելու՝ իրական URL-ը նախադիտելու համար: Օրինական կազմակերպությունները հիմնականում օգտագործում են անվտանգ և ճանաչելի տիրույթներ:

3. Օգտագործեք երկփուլ նույնականացում (2FA):

Հնարավորության դեպքում միացրեք երկփուլ նույնականացումը: Նույնիսկ եթե ձեր հավատարմագրերը վտանգված են, նույնականացման լրացուցիչ շերտ ունենալը կարող է զգալիորեն բարձրացնել անվտանգությունը:

4. Թարմացված պահեք ծրագրային ապահովման և անվտանգության գործիքները

Պարբերաբար թարմացրեք ձեր օպերացիոն համակարգը, հակավիրուսային ծրագրակազմը և վեբ բրաուզերները: Անվտանգության թարմացումները հաճախ ներառում են խոցելիության համար նախատեսված պատչեր, որոնք կարող են շահագործվել ֆիշինգային հարձակումների միջոցով:

5. Օգտագործեք հեղինակավոր հակավիրուսային և հակաֆիշինգային ծրագիր.

Տեղադրեք հեղինակավոր հակավիրուսային ծրագիր, որը ներառում է հակաֆիշինգի գործառույթներ: Այս գործիքները կարող են օգնել հայտնաբերել և արգելափակել ֆիշինգի փորձերը:

6. Կրթեք ինքներդ ձեզ.

Եղեք տեղեկացված ֆիշինգի ընդհանուր մարտավարության մասին և տեղյակ եղեք վերջին խարդախությունների մասին: Ծանոթացեք, թե ինչպես են ֆիշինգի նամակներն ու հաղորդագրությունները սովորաբար երևում պոտենցիալ սպառնալիքները ճանաչելու համար:

7. Ստուգեք զգայուն տեղեկատվության հարցումները.

Օրինական կազմակերպությունները էլեկտրոնային փոստով չեն պահանջի զգայուն տեղեկատվություն (օրինակ՝ գաղտնաբառեր, կրեդիտ քարտերի համարներ կամ Սոցիալական ապահովության համարներ): Եթե կասկածներ ունեք, ուղղակիորեն կապվեք կազմակերպության հետ՝ օգտագործելով հաստատված կոնտակտային տվյալները:

8. Ապահովե՛ք Ձեր անձնական սարքերը.

Օգտագործեք ուժեղ, եզակի գաղտնաբառեր ձեր հաշիվների համար և մտածեք գաղտնաբառերի հեղինակավոր կառավարչի օգտագործման մասին: Ձեր սարքերը ապահով պահեք գաղտնաբառերով, PIN-ներով կամ կենսաչափական նույնականացմամբ:

9. Խուսափեք չստուգված հղումների վրա սեղմելուց.

Խուսափեք անհայտ կամ կասկածելի աղբյուրներից էլփոստի, հաղորդագրությունների կամ թռուցիկ պատուհանների վրա սեղմելուց: Փոխարենը, մուտքագրեք URL-ը անմիջապես ձեր դիտարկիչում կամ օգտագործեք էջանիշեր հայտնի կայքերի համար:

10. Զգույշ եղեք սոցիալական ցանցերում.

Ուշադիր եղեք այն տեղեկատվությանը, որը դուք կիսում եք սոցիալական լրատվամիջոցների հարթակներում: Ֆիշերը կարող է օգտագործել սոցիալական ճարտարագիտությունը՝ անձնական տվյալներ հավաքելու և նպատակային հարձակումներ անելու համար:

11. Ստուգեք կայքի անվտանգությունը (HTTPS):

Փնտրեք «https://» URL-ում և կողպեքի պատկերակը հասցեագոտում, երբ մուտքագրում եք զգայուն տեղեկատվություն: Անվտանգ կայքերը գաղտնագրում են տվյալները փոխանցման ընթացքում, ինչը հարձակվողների համար դժվարացնում է գաղտնալսումը:

12. Ստուգել անսպասելի հավելվածները.

Եթե դուք ստանում եք անսպասելի հավելվածներ, հատկապես անհայտ աղբյուրներից, խուսափեք դրանք բացելուց: Վնասակար հավելվածները կարող են պարունակել չարամիտ ծրագրեր կամ անվտանգության այլ սպառնալիքներ:

13. Մնացեք տեղեկացված անվտանգության լավագույն փորձի մասին.

Եղեք տեղեկացված անվտանգության վերջին լավագույն փորձի մասին և պարբերաբար վերանայեք անվտանգության ուղեցույցները, որոնք տրամադրվում են հեղինակավոր աղբյուրների կողմից:

5. Ի՞նչպիսի տեղեկատվության կարող է հասանելիություն ստանալ հակառակորդը ֆիշինգի միջոցով:

Ֆիշինգի հարձակումները նախատեսված են խաբել անհատներին՝ բացահայտելու տեղեկատվություն կամ ձեռնարկել այնպիսի գործողություններ, որոնք կարող են

վտանգել նրանց անվտանգությունը: Այն տեղեկատվությունը, որին հակառակորդները կարող են մուտք ունենալ ֆիշինգի միջոցով, ներառում է.

1. Մուտքի հավատարմագրերը.

Ֆիշինգի հարձակումները հաճախ նպատակ ունեն գողանալ տարբեր առցանց հաշիվների օգտանուններ և գաղտնաբառեր, ներառյալ էլփոստը, սոցիալական լրատվամիջոցները, բանկային և բիզնես հավելվածները:

2. Անձնական տվյալներ.

Հակառակորդները կարող են թիրախավորել անհատներին անձնական տվյալներ կորզելու համար, ինչպիսիք են լրիվ անունները, հասցեները, հեռախոսահամարները, Սոցիալական ապահովության համարները, ծննդյան տարեթվերը և նույնականացման այլ տեղեկություններ:

3. Ֆինանսական տեղեկատվություն.

Ֆիշինգի հարձակումները կարող են նպատակ ունենալ ֆինանսական տվյալներ ձեռք բերել, ներառյալ վարկային քարտերի համարները, բանկային հաշվի մանրամասները և վճարման այլ տեղեկություններ:

4. Կորպորատիվ հավատարմագրերը.

Spear phishing -ի դեպքում հակառակորդները կարող են թիրախավորել կոնկրետ կազմակերպության աշխատակիցներին՝ հասանելիություն ստանալու կորպորատիվ մուտքի հավատարմագրերին, ներքին համակարգերին կամ ընկերության զգայուն տեղեկատվությանը:

5. Անվտանգության ստուգման կոդերը:

Ֆիշինգի որոշ փորձեր ներառում են խաբել անհատներին՝ SMS-ի միջոցով ուղարկված կամ նույնականացնող հավելվածների կողմից ստեղծված անվտանգության կոդերը տրամադրելու համար, որոնք օգտագործվում են երկգործոն նույնականացման համար:

6. Գործարար տեղեկատվություն.

Հակառակորդները կարող են թիրախավորել ձեռնարկություններին, որպեսզի կորզեն այնպիսի զգայուն տեղեկատվություն, ինչպիսիք են հաճախորդների տվյալների շտեմարանները, գույքային տեղեկությունները, մտավոր սեփականությունը կամ առևտրային գաղտնիքները:

7. Բժշկական գրառումներ.

Թիրախային հարձակումների ժամանակ հակառակորդները կարող են նպատակ ունենալ ձեռք բերել բժշկական տեղեկատվություն, առողջական գրառումներ կամ ապահովագրական տվյալներ ինքնության գողության կամ այլ վնասակար նպատակներով:

8. Սոցիալական լրատվամիջոցների հաշիվներ.

Ֆիշերը կարող է փորձել վերահսկողություն ձեռք բերել սոցիալական մեդիայի հաշիվների վրա՝ թույլ տալով նրանց անձնավորել անհատներին, ապատեղեկատվություն տարածել կամ հետագա հարձակումներ իրականացնել:

9. Հաշվի առգրավում

Երբ հակառակորդները մուտք գործեն մուտքի հավատարմագրերը, նրանք կարող են տիրանալ հաշիվներին, անձնավորել օրինական օգտատիրոջը և պոտենցիալ ներգրավվել խարդախության մեջ:

10. Անձնական նամակներ.

Ֆիշինգի հարձակումները կարող են ներառել էլ. փոստի հաշիվների հասանելիություն, ինչը թույլ է տալիս հակառակորդներին վերահսկել և գաղտնալսել անձնական էլփոստի հաղորդակցությունները:

11. Անձնական փաստաթղթեր

Ֆիշերը կարող է խաբել անհատներին՝ բացելու վնասակար կցորդներ կամ սեղմելով հղումները, որոնք ներբեռնում են չարամիտ ծրագրեր՝ ապահովելով սարքում պահվող զգայուն փաստաթղթերի հասանելիություն:

12. Հեղինակության վնաս.

Հակառակորդները կարող են օգտագործել վտանգված հաշիվները՝ վնասելու անհատի կամ կազմակերպության հեղինակությունը՝ կեղծ տեղեկություններ տարածելով կամ չարամիտ գործողություններ իրականացնելով:

6. Ի՞նչ է ngrok-ը:

Ngrok-ը բազմահարթակ թունելային, հակադարձ պրոքսի ծրագրաշար է, որը անվտանգ թունելներ է ստեղծում հանրային վերջնակետից, ինչպիսին է ինտերնետը, մինչև տեղական գործող ցանցային ծառայություն: Այն ծրագրավորողներին թույլ է տալիս լոկալ սերվերը ներկայացնել ինտերնետին՝ փորձարկման, մշակման կամ այլ նպատակների համար՝ առանց հանրային IP հասցեի կամ բարդ ցանցի կազմաձևման:

Նգրոկի հիմնական հատկանիշները ներառում են.

1. Թունելավորում:

Ngrok-ը ստեղծում է անվտանգ թունելներ՝ NAT-ների և firewalls-ի հետևում գտնվող տեղական սերվերները հանրային ինտերնետին բացահայտելու համար:

2. Ապահով կապեր.

Այն ծածկագրում է թունելի վրայով երթևեկությունը՝ ապահովելով անվտանգ կապ տեղական սերվերի և Ngrok վերջնակետի միջև:

3. HTTP և TCP թունելավորում:

Ngrok-ն աջակցում է ինչպես HTTP, այնպես էլ TCP թունելավորմանը՝ թույլ տալով ծրագրավորողներին բացահայտել վեբ սերվերները, ինչպես նաև այլ տեսակի ծառայություններ:

4. Ենթադոմեյններ:

Ngrok-ը տրամադրում է ենթադոմեյններ ngrok.io-ում, ինչը հեշտացնում է տեղական սերվերի հասանելիությունը հանրությանը հասանելի URL-ով:

5. Երթևեկության ստուգում.

Մշակողները կարող են ստուգել թունելով անցնող HTTP տրաֆիկը, օգտագործելով Ngrok վեբ ինտերֆեյսը, որը մանրամասներ է տալիս հարցումների և պատասխանների մասին:

6. Նույնականացում և հատուկ տիրույթներ.

Ngrok-ն առաջարկում է այնպիսի գործառույթներ, ինչպիսիք են գաղտնաբառի պաշտպանությունը թունելների համար և վճարովի պլանների համար հատուկ տիրույթների աջակցություն:

Ngrok-ի օգտագործման տիրույթները ներառում են.

Վեբ մշակում:

Մշակողները կարող են բացահայտել տեղական վեբ սերվերները՝ կիսելու իրենց աշխատանքը հաճախորդների կամ գործընկերների հետ՝ փորձարկման և հետադարձ կապի համար:

API-ի փորձարկում:

Այն օգտակար է տեղական API-ների փորձարկման համար՝ դրանք հանրությանը հասանելի դարձնելով արտաքին փորձարկման կամ ինտեգրման նպատակներով:

Գովազդ կամ ցուցադրման հնարավորություն

- Ngrok-ը ծրագրավորողներին թույլ է տալիս ցուցադրել իրենց նախագծերը կամ հավելվածները՝ առանց դրանք արտադրական սերվերում տեղակայելու:

IoT և բջջային հավելվածների թեստավորում.

Ngrok-ը հեշտացնում է IoT սարքերի և բջջային հավելվածների փորձարկումը, որոնք մշակման ընթացքում պետք է շփվեն սերվերների հետ:

Ngrok-ն օգտագործելու համար դուք սովորաբար ներբեռնում և գործարկում եք Ngrok երկուական տարբերակը, նշում եք ձեր տեղական սերվերի կոորդինատները, և Ngrok-ը ստեղծում է հանրային URL, որը թունելներ է ստեղծում դեպի ձեր տեղական միջավայրը: Հիշեք, որ թեև Ngrok-ը հարմար է մշակման և փորձարկման համար, անվտանգության նկատառումները շատ կարևոր են, հատկապես, երբ այն օգտագործվում է արտադրության նման միջավայրերում:

7. Ի՞նչ է XAMPP-ը:

XAMPP-ն անվճար և բաց կոդով վեբ սերվերի լուծումների փաթեթ է, որը մշակվել է Apache Friends-ի կողմից: Այն բաղկացած է Apache HTTP սերվերից, MariaDB տվյալների բազայից և PHP-ով և Perl-ով գրված սկրիպտների թարգմանիչներից: XAMPP-ը նախագծված է որպես հեշտ տեղադրվող և օգտագործման համար պատրաստ մշակման միջավայր վեբ ծրագրավորողների համար: Այն ապահովում է տեղական սերվերի միջավայր ստեղծելու հարմար միջոց փորձարկման և զարգացման նպատակներով:

8. Ֆիշինգի իրականացման փուլերը:

Ֆիշինգի իրականացումը սովորաբար ներառում է մի քանի փուլ.

1. Պլանավորում. Այս փուլում հարձակվողները պլանավորում են իրենց թիրախային լսարանը և նպատակները: Նրանք որոշում են ֆիշինգի հարձակման տեսակը, որը պետք է օգտագործվի (օրինակ՝ էլ. փոստ, կայք կամ սոցիալական ճարտարագիտություն):

2. Կարգավորում. Հարձակվողները ստեղծում են հարձակման համար անհրաժեշտ ենթակառուցվածքը: Սա կարող է ներառել կեղծ կայքերի ստեղծում, ֆիշինգ նամակների ստեղծում կամ վնասակար ծրագրերի պատրաստում:

3. Առաքում. Ֆիշինգի նամակները, հաղորդագրությունները կամ այլ հաղորդակցությունները ուղարկվում են թիրախավորված անձանց: Այս հաղորդագրությունները հաճախ օրինական են թվում և փորձում են խաբել օգտատերերին՝ որոշակի գործողություն կատարելու, օրինակ՝ սեղմելով հղումը կամ տրամադրելով զգայուն տեղեկատվություն:

4. Շահագործում. Երբ օգտատերը փոխազդում է ֆիշինգի փորձի հետ (օրինակ՝ սեղմելով հղումը), հարձակվողն օգտագործում է իրավիճակը՝ հասնելու իր նպատակին: Սա կարող է ներառել մուտքի հավատարմագրերի գողություն, չարամիտ ծրագրերի տեղադրում կամ օգտագործողին ֆինանսական գործարք կատարելու խաբեություն:

5. Էքսֆիլտրացիա. Հարձակվողը հավաքում է տեղեկատվությունը կամ մուտք է ստանում համակարգեր՝ որպես իրենց սկզբնական նպատակի մաս: Սա կարող է ներառել մուտքի հավատարմագրերի, ֆինանսական տեղեկատվության կամ այլ զգայուն տվյալների գողություն:

6. Ծածկող հետքեր. Բարդ հարձակվողները կարող են փորձել ծածկել իրենց հետքերը՝ հայտնաբերումից խուսափելու համար: Սա կարող է ներառել նրանց գործունեության հետքերը ջնջելու կամ անվտանգության մասնագետների համար ավելի դժվարացնել հարձակումը հետագծելու աղբյուրը:

Այս փուլերի ընթացքում հարձակվողները հաճախ օգտագործում են տարբեր մեթոդներ՝ իրենց ֆիշինգի փորձերն ավելի համոզիչ դարձնելու համար, օրինակ՝ ստեղծելով իրատեսական տեսք ունեցող կայքեր, օգտագործելով պաշտոնական լոգոները և կիրառելով սոցիալական ինժեներական մարտավարություն՝ օգտագործելու մարդու հոգեբանությունը:

9. Ինչպե՞ս են գեներացնում ժամանակավոր email եւ ինչ նպատակով է այն կիրառվում:

Ժամանակավոր էլ. փոստը, որը նաև հայտնի է որպես միանգամյա օգտագործման կամ նետվող էլ.

1. Սպամից խուսափելը. Օգտագործողները կարող են օգտագործել ժամանակավոր նամակներ՝ գրանցվելու ծառայության կամ կայքէջի համար, որը կարող է գովազդային նամակներ ուղարկել: Նպատակին հասնելուց հետո ժամանակավոր էլփոստը կարող է չեղարկվել՝ նվազագույնի հասցնելով առաջնային էլփոստի մուտքի արկղում սպամի վտանգը:

2. Ստուգում. Որոշ առցանց ծառայություններ կամ կայքեր հաշիվ ստեղծելու համար պահանջում են էլ.փոստի հաստատում: Օգտատերերը կարող են օգտագործել ժամանակավոր էլփոստ՝ հաստատման հղումը ստանալու համար՝ առանց իրենց հիմնական էլ.

3. Թեստավորում. Մշակողները և փորձարկողները կարող են օգտագործել ժամանակավոր էլ. նամակներ՝ փորձարկման նպատակով հաշիվներ ստեղծելու համար՝ առանց իրենց իսկական էլ. հասցեների օգտագործման: Սա հատկապես օգտակար է այն հավելվածների վրա աշխատելիս, որոնք ներառում են էլփոստի ծանուցումներ:

4. Գաղտնիություն. Գաղտնիության մասին մտահոգված անձինք կարող են օգտագործել ժամանակավոր էլ. նամակներ՝ գրանցվելու առցանց ֆորումների, տեղեկագրերի կամ այլ ծառայությունների համար՝ առանց իրենց իրական էլ. հասցեն բացահայտելու:

5. Անցանկալի շփումներից խուսափելը. Մրցույթներ մտնելիս, անվճար ֆայլեր ներբեռնելիս կամ առցանց որոշակի բովանդակություն մուտք գործելիս օգտատերերը կարող են օգտագործել ժամանակավոր էլ.

Ժամանակավոր էլփոստի ծառայությունները ստեղծում են կարճաժամկետ էլփոստի հասցեներ, որոնց ժամկետը լրանում է որոշակի ժամանակահատվածից կամ որոշակի քանակի օգտագործումից հետո: Օգտատերերը կարող են մուտք գործել նամակներ սահմանափակ ժամանակով, և հասցեները սովորաբար անտեսվում են, երբ նախատեսված նպատակն իրականացվի: Կարևոր է նշել, որ թեև ժամանակավոր էլ. նամակներն առաջարկում են հարմարավետություն, դրանք չեն կարող ապահովել նույն

անվտանգության և գաղտնիության մակարդակը, ինչ հատուկ և ապահով էլփոստի ծառայությունից օգտվելը:

10.Ինչպե՞ս են գեներացնում ժամանակավոր հեռախոսահամարը եւ ինչ դեպքերում է այն կիրառվում:

Ժամանակավոր հեռախոսահամարը սովորաբար ստեղծվում է առցանց ծառայությունների միջոցով, որոնք տրամադրում են միանգամյա օգտագործման կամ վիրտուալ հեռախոսահամարներ: Այս թվերն օգտագործվում են տարբեր նպատակներով և օգտատերերին առաջարկում են գաղտնիության և անանունության մակարդակ: Ահա մի քանի դեպքեր, երբ սովորաբար օգտագործվում են ժամանակավոր հեռախոսահամարներ.

1. Օնլայն ստուգում. Շատ առցանց հարթակներ, հավելվածներ և ծառայություններ օգտվողներից պահանջում են հաստատել իրենց ինքնությունը՝ տրամադրելով հեռախոսահամար: Այդ նպատակով օգտվողները կարող են օգտագործել ժամանակավոր հեռախոսահամար, հատկապես, եթե նրանք մտահոգված են գաղտնիությամբ կամ չեն ցանկանում կիսվել իրենց հիմնական հեռախոսահամարով:

2. Ժամանակավոր հաղորդակցություն. Օգտատերերը կարող են օգտագործել ժամանակավոր հեռախոսահամարներ կարճաժամկետ հաղորդակցության կարիքների համար, օրինակ՝ առցանց ֆորումների, ծանոթությունների հավելվածների կամ այլ հարթակներում մասնակցելու ժամանակ, որտեղ նրանք ցանկանում են խուսափել իրենց իրական հեռախոսահամարով կիսվելուց:

3. Անձնական համարի պաշտպանություն. Իրեր առցանց վաճառելիս, նոր մարդկանց հանդիպելիս կամ գործարքների մեջ ներգրավվելիս, որոնք ներառում են կոնտակտային տեղեկությունների փոխանակում, անհատները կարող են օգտագործել ժամանակավոր հեռախոսահամար՝ իրենց անձնական համարը հնարավոր չարաշահումից պաշտպանելու համար:

4. Աշխարհագրական սահմանափակումների շրջանցում. Ժամանակավոր հեռախոսահամարները կարող են օգտագործվել աշխարհագրական

սահմանափակումները շրջանցելու համար: Օրինակ, որոշ ծառայություններ կարող են հասանելի լինել միայն որոշակի երկրների օգտատերերին, և մուտքի համար կարող է օգտագործվել տվյալ երկրի ժամանակավոր հեռախոսահամարը:

5. Թեստավորում և մշակում. Մշակողները և փորձարկողները կարող են օգտագործել ժամանակավոր հեռախոսահամարներ, երբ աշխատում են ծրագրերի կամ համակարգերի վրա, որոնք ներառում են SMS կամ հեռախոսազանգերի ստուգում: Այն թույլ է տալիս նրանց ստուգել ստուգման գործընթացը՝ առանց իրական հեռախոսահամարների օգտագործման:

6. Սպամից և հեռամարքեթինգային զանգերից խուսափելը. Օգտագործողները կարող են օգտագործել ժամանակավոր հեռախոսահամարներ՝ գրանցվելու ծառայությունների կամ առաջխաղացումների համար՝ չբացահայտելով իրենց իրական հեռախոսահամարը՝ նվազեցնելով սպամ զանգեր կամ հաղորդագրություններ ստանալու ռիսկը:

Ժամանակավոր հեռախոսահամարների ծառայությունները հաճախ տրամադրում են համարներ, որոնք վավեր են կարճ տևողության կամ սահմանափակ թվով օգտագործման համար: Կարևոր է զգույշ լինել նման ծառայությունների օգտագործման անվտանգության և գաղտնիության հետևանքների վերաբերյալ, քանի որ դրանք կարող են չառաջարկել պաշտպանության նույն մակարդակը, ինչ հատուկ և ապահով հաղորդակցման հարթակ օգտագործելը:

11.Ինչո՞վ է տարբերվում սովորական կայքը ֆիշինգ կայքից:

Սովորական վեբկայքը և ֆիշինգի կայքը տարբերվում են իրենց բովանդակությամբ և նպատակային գործողություններով: Ահա հիմնական տարբերությունները.

- **Նպատակաուղղվածություն**

Սովորական կայք - ստեղծվում է օրինական նպատակներով, ինչպիսիք են տեղեկատվություն տրամադրելը, ապրանքներ կամ ծառայություններ առաջարկելը, ժամանցը, կրթությունը կամ համայնքի հետ փոխգործակցությունը: Նպատակն է օգտատերերին ծառայել օրինական և էթիկական ձևով:

Ֆիշինգի կայք - նախագծված է օգտատերերին խաբելու վնասակար մտադրությամբ: Այն նպատակ ունի խաբել այցելուներին՝ բացահայտելու անձնական տեղեկությունները, ինչպիսիք են մուտքի հավատարմագրերը, անձնական տվյալները կամ ֆինանսական տվյալները:

- **Բովանդակություն**

Սովորական կայք - սովորաբար ունեն իրական և ճշգրիտ բովանդակություն՝ կապված իրենց նպատակի հետ: Նրանք արժեքավոր տեղեկատվություն, ֆունկցիոնալություն կամ ծառայություններ են տրամադրում օգտվողներին:

Ֆիշինգի կայք - նմանակում են օրինական կայքերի տեսքը: Նրանք հաճախ օգտագործում են իսկական կայքերից պատճենված կամ կեղծ բովանդակություն՝ ծանոթության զգացում ստեղծելու համար: Առաջնային նպատակը օգտատերերին խաբելն է, որպեսզի հարձակվողին օգուտ բերեն գործողություններ:

- **Գործողություններ**

Սովորական կայք - օգտատերերի համար որևէ վտանգ չեն ներկայացնում: Նրանք գործում են օրինական և էթիկական սահմաններում, և օգտատերերը կարող են ապահով շփվել նրանց հետ:

Ֆիշինգի կայք - զգալի սպառնալիքներ են ներկայացնում: Նրանք փորձում են գողանալ տեղեկատվություն՝ հանգեցնելով ինքնության գողության, ֆինանսական կորստի կամ հաշիվների չարտոնված մուտքի: Ընդհանուր մարտավարությունը ներառում է կեղծ մուտքի էջեր, ձևաթղթեր կամ հաղորդագրություններ, որոնք խաբում են օգտատերերին գաղտնի տվյալներ բացահայտելու համար:

- **URL**

Սովորական կայք - ունեն օրինական և ճանաչելի տիրույթի անուններ, որոնք համապատասխանում են իրենց բովանդակությանը կամ ապրանքանիշին: Նրանք օգտագործում են ստանդարտ HTTP կամ HTTPS արձանագրություններ:

Ֆիշինգի կայք - հաճախ օգտագործում են խաբուսիկ տիրույթի անուններ, որոնք շատ նման են օրինական կայքերին: Նրանք կարող են օգտագործել ուղղագրական տատանումներ, լրացուցիչ նիշեր կամ ենթադոմեյններ՝ օգտատերերին խաբելու համար: Ֆիշինգ կայքերը կարող են օգտագործել HTTP, բայց որոշ բարդ կայքեր կարող են օգտագործել HTTPS՝ ավելի օրինական երևալու համար:

- **Օգտատիրոջ իրազեկում**

Սովորական կայք - Օգտագործողները կարող են ընդհանուր առմամբ վստահել սովորական կայքերին, հատկապես նրանց, ովքեր ունեն հայտնի ապրանքանիշեր, հեղինակավոր տիրույթներ և անվտանգ կապեր:

Ֆիշինգի կայք - հիմնված են օգտատերերին խաբելու վրա, ուստի տեղեկացվածությունն ու զգուշությունը շատ կարևոր են: Օգտատերերը պետք է թերահավատորեն վերաբերվեն անսպասելի էլ. նամակներին, հաղորդագրություններին կամ հղումներին և ստուգեն կայքերի իսկությունը՝ նախքան զգայուն տեղեկատվություն տրամադրելը:

12. **Նշել ֆիշինգի տեսակները:** Հարց 2

13.Ինչո՞վ է տարբերվում սովորական email ֆիշինգ-ը email -ից:

Էլեկտրոնային փոստը լայնորեն օգտագործվող հաղորդակցման մեթոդ է, որը թույլ է տալիս անհատներին և կազմակերպություններին ուղարկել և ստանալ թվային հաղորդագրություններ ինտերնետով: Այն ծառայում է որպես տեքստի, ֆայլերի և մուլտիմեդիայի փոխանակման միջոց օգտատերերի միջև՝ ինչպես անձնական, այնպես էլ մասնագիտական:

Էլեկտրոնային փոստով ֆիշինգի նամակները խարդախ հաղորդագրություններ են, որոնք նախատեսված են հասցեատերերին որոշակի գործողություններ կատարելու մեջ խաբելու համար, ինչպիսիք են՝ կտտացնելով վնասակար հղումները, ներբեռնել վարակված հավելվածները կամ տրամադրել զգայուն տեղեկություններ, ինչպիսիք են օգտանունները և գաղտնաբառերը:

Էլեկտրոնային փոստի սովորական ֆիշինգը սովորաբար ներառում է խաբուսիկ նամակների զանգվածային փոխանցում մեծ թվով հասցեատերերի՝ փորձելով լայն ցանց ստեղծել՝ զգայուն տեղեկատվություն հավաքելու համար: