ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ
ԳՈՐԾԱԿԱԼՈՒԹՅՈՒՆ

ՈՒՂԵՑՈՒՅՑ

Ինչպես պաշտպանել անձնական տվյալները համացանցում և չդառնալ ֆիշինգի զոհ

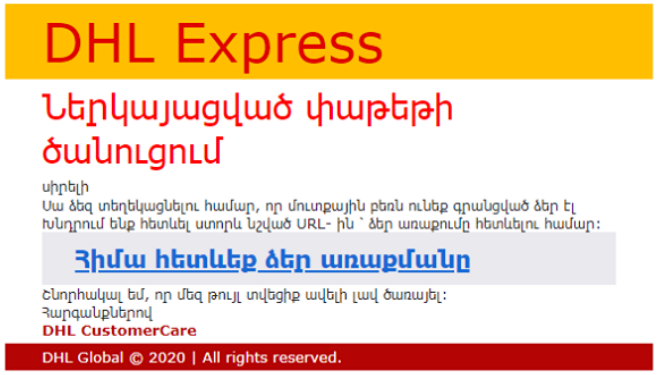
Ֆիշինգը կեղծ էլեկտրոնային նամակներ ու կայքեր օգտագործելու միջոցով այլոց անձնական, էլեկտրոնային տվյալները հափշտակելու միջոց է:

Այս ուղեցույցում կներկայացնենք, թե ինչպես են այն օգտագործում մարդկանց դեմ ու ինչպես պաշտպանվել ֆիշինգից:

Ֆիշինգի նպատակն է կեղծ էլեկտրոնային նամակով ստացողներին համոզել, որ դա հենց այն նամակն է, որին իրենք սպասում են: Օրինակ՝ հարցում բանկի անունից, կեղծված հաղորդագրություն որևէ հայտնի ընկերությունից կամ ծանոթներից:

Ֆիշինգային հարձակման ժամանակ չարագործները քողարկվում են որևէ վստահելի ընկերության կամ անձի անվան տակ, որոնց հետ հավանական է, որ զոհը առնչություն ունեցած լինի ու նրանց հատուկ ձևով կեղծ հաղորդագրություն են ուղարկում: Հաղորդագրությանը կցվում է վնասաբեր ֆայլ կամ հղում է տեղադրվում, որտեղ պահանջում են լրացնել էլեկտրոնային փոստի մուտքանունն ու գաղտնաբառը, իսկ իրականում դրանք փոխանցվում է ֆիշինգային հարձակում կազմակերպողին:

Ֆիշինգի օրինակ: Հարձակվողը քողարկվել է առաքումներ կազմակերպող հայտնի DHL կազմակերպության անվան տակ ու հղում կցել հաղորդագրությանը: Հղումով անցնելու դեպքում պահանջում են մուտք անել էլ. փոստի հասցեն ու գաղտնաբառը և այդպիսով տիրանում են էլ. փոստին:


DHL Express

Ներկայացված փաթեթի ծանուցում

սիրելի

Սա ձեզ տեղեկացնելու համար, որ մուտքային բեռն ունեք գրանցված ձեր էլ

Խնդրում ենք հետևել ստորև նշված URL- ին ՝ ձեր առաքումը հետևելու համար:

Հիմա հետևեք ձեր առաքմանը

Շնորհակալ եմ, որ մեզ թույլ տվեցիք ավելի լավ ծառայել:

Հարգանքներով

DHL CustomerCare

DHL Global © 2020 | All rights reserved.

Ֆիշինգը կիբերհարձակումների ամենահին տեսակներից է: 1990-ականներից մինչ հիմա այն լայնորեն կիրառվում է: Ֆիշինգը անգլերեն «Fish» - ձուկ բառից է, որը ենթադրում է, որ հարձակվողը կարթ է գցում՝ հուսալով, որ զոհը խայծը կուլ կտա: Տերմինը 1990-ականներին ծագել է հաքերների շրջանակներում:

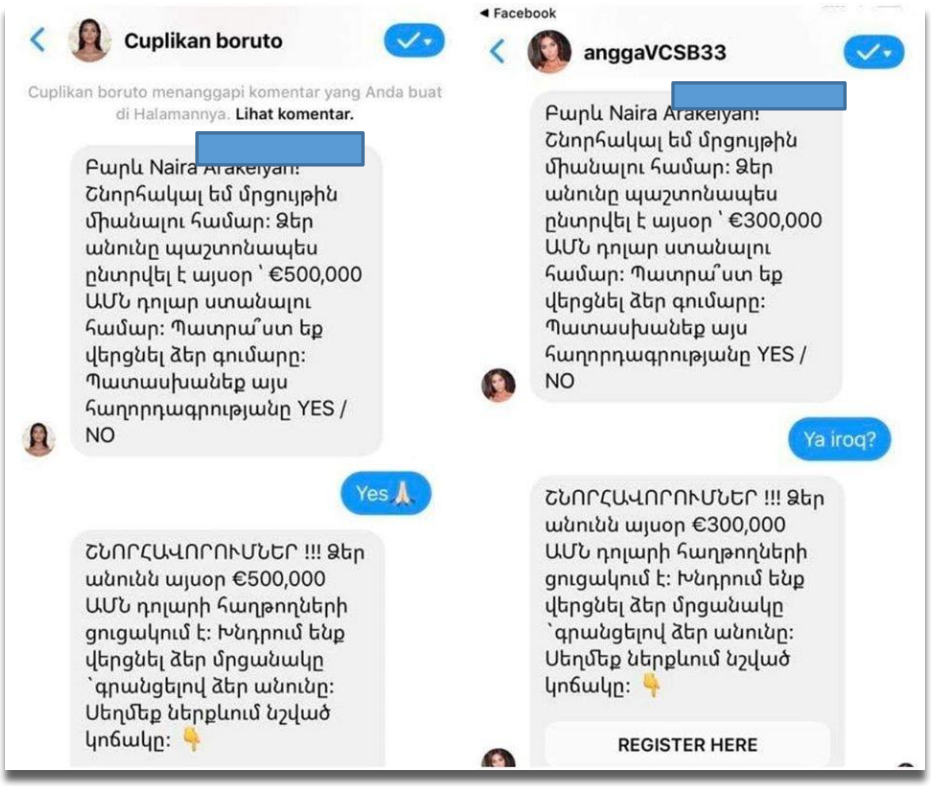
Ֆիշինգային հարձակում կազմակերպողները հաճախ խոստանում են մեծ գումարներ, պարգևատրում, տարատեսակ շահումներ, օրինակ՝ սմարթֆոններ: Նման հաղորդագրությունները հաճախ տարածվում են հայտնի մարդկանց անունով կեղծ էջերից՝ էլեկտրոնային փոստով կամ սոցիալական ցանցերով:
Հարկ է նշել, որ ֆիշինգի դեպքում գաղտնաբառի բարդությունը նույնիսկ չի ապահովում զոհ չդառնալ, քանի որ նամակ ստացողը ինքն է ինքնակամ լրացնում գաղտնաբառը:

Հաճախ հարձակվողները հաղորդագրություններ են ուղարկում այնպիսի բովանդակությամբ, թե նամակ ստացողը ինչ-որ երկրում միլիարդատեր բարեկամ ունի, ով նրան մեծ ժառանգություն է թողել:

Նման «խոստումնալից» նամակներ ստանալիս պետք է վերաբերվել դրանց կասկածամտությամբ: Իսկ իրական կյանքում կհավատայի՞ք, երբ անծանոթ մեկը մոտենար ու ձեզ ասեր, որ միլիոններ են ժառանգել ու պետք է մի քանի հազար դոլար տաք, որ ժառանգությունը փոխանցի ձեզ: Կհավատայի՞ք ու նրան միանգամից կտայի՞ք պահանջված գումարը:
Նման հաղորդագրությունները հաճախ ուղարկում են օտարերկացիներ ու թարգմանում են տեքստը հայերեն էլեկտրոնային թարգմանիչներով, ինչը ենթադրում է, որ տեքստը պարունակում է բազմաթիվ սխալներ:

Այս փաստը նույնպես պետք է կասկած առաջացնի նամակի իսկության վերաբերյալ:

Նկարում ցուցադրված է օրինակ, որում հարձակում է կազմակերպվել Ֆեյսբուք սոցիալական ցանցի հայկական տիրույթի օգտատերերի վրա: Քիմ Քարդաշյանի անունով կեղծ էջից նամակ են ուղարկել ու պահանջել բանկային տվյալներ: Բանկային տվյալները ստանալուց հետո գողացել են քաղաքացիների գումարները:



Ինչպես պաշտպանվել ֆիշինգային հարձակումներից

- **Մտածել քլիք անելուց առաջ**

Էլեկտրոնային հաղորդագրությամբ, սոցիալական ցանցերով ստացած նամակներին պետք է ուշադիր լինել: Եթե պատահական, անծանոթ հասցեից ստանում եք նամակ, որում հղում կամ ֆայլ է առկա, մի շտապեք սեղմել: Պետք է հասկանալ, թե իրականում ինչ են ուղարկել ձեզ, և ով է ուղարկողը:

Եթե ստանում եք նամակ ընկերոջից ու կարծում, որ նա դժվար ձեզ նման բովանդակությամբ նամակ ուղարկեր, պետք է կապի այլ միջոցով հարցնել, թե արդյո՞ք նա է ուղարկել, քանի որ հավանական է՝ կոտրել են ձեր ընկերոջ էջը ու նրա միջոցով ուզում են ձերը կոտրել:
Եթե ինչ-որ հայտնի ընկերության անունից ստանում եք կասկածելի նամակ, ապա կապի ուղիղ միջոցով նրանցից ճշտեք, թե արդյո՞ք իրենք են նամակի հեղինակը:

- **Համոզվել, որ կայքն անվտանգ է**

Ընդհանրապես, ձեր մասին զգայուն տեղեկություններ համացանցում գրանցելիս պետք է զգույշ լինել: Սակայն, եթե օրինակ բանկի անունից նամակ եք ստանում, որտեղ պահանջում են լրացնել ձեր մասին տվյալներ, պետք ստուգել արդյո՞ք կայքի այն հասցեն, որ ուղարկել են ձեզ նույնն է բանկի իրական հասցեի հետ, թե՞ կան տառի կամ սիմվոլի տարբերություններ: Նույնը այլ ընկերությունների մասին կարելի է ասել: Նման դեպքերում, երբ նամակով ստացած կայքի հասցեն տարբերվում է ընկերության իրական կայքի հասցեից, ակնհայտ է դառնում, որ կեղծիք է առկա ու պետք է ճշտել, թե՞ արդյոք իրական է նամակը:
Երբ որևէ կայքում զգայուն ինֆորմացիա եք լրացնում ձեր մասին, ստուգեք, որ կայքի հասցեն սկսվի «https»-ով: Եթե բրաուզերը ձեզ ծանուցում է, որ հնարավոր է կայքը վնասաբեր ծրագրեր է պարունակում, մի բացեք այդ կայքը:

- **Պարբերաբար ստուգել օնլայն օգտահաշիվները**

Եթե որևէ տեղ ունեք հաշիվ, բայց հազվադեպ եք մտնում, ինչ-որ մեկը կարող է օգտվել այդ առիթից: Սովորություն դարձրեք պարբերաբար մտնել ձեր հաշիվներ ու փոխել գաղտնաբառերը: Եթե կասկածում եք, որ ձեր բանկային հաշիվներից գումար է անհետանում, որի մասին տեղյակ չեք, կարող եք բանկից քաղվածք պահանջել

- **Թարմացնել բրաուզերը**

Բրաուզերը պետք է միշտ թարմացնել: Դրանցում պարբերաբար հայտնաբերվում են խոցելի տեղեր, որոնք շտկվում են թարմացումներով ու հաքերները չեն կարողանում օգտագործել խոցելիությունը: Հավանական հարձակման դեպքում բրաուզերը կհայտնի ձեզ վտանգի մասին, եթե միշտ թարմացնեք:

Ֆիշինգի օրինակ

- **Զգուշացեք բրաուզերում բացվող կողմնակի պատուհաններից (Pop-up պատուհաններ)**

Բրաուզերում բացվող փոքրիկ պատուհանները թվում է, թե կայքի բաղկացուցիչ մասն են, բայց հաճախ դրանք հղումներ են դեպի վնասաբեր կայքեր: Հայտնի բրաուզերների մեծ մասը հնարավորություն են տալիս արգելափակել բացվող pop-up պատուհանները: Դուք կարող եք թույլատրել դրանք մասնավոր դեպքերում, եթե ուզում եք այդ կայքում լինեն նման պատուհաններ: Այդպիսի պատուհանները փակելու համար պետք չէ սեղմել «Չեղարկել» (Cancel, Отмена, Закрыть) կոճակը: Փակելու համար տեղադրում են թաքնված X նշանը, պետք է այն սեղմել:

- **Երբեք մի հայտնեք անձնական զգայուն տեղեկություններ**

Որպես ընդհանուր կանոն՝ անձնական զգայուն տվյալներ, բանկային տվյալներ ու կարևոր այլ տեղեկություններ (օրինակ՝ տեղեկայման վայր, անձնագրի նկար, բանկային քարտի նկար և այլն) համացանցի միջոցով պետք չէ փոխանցել կամ պահել համացանցում:

Այսպիսի կարևոր տվյալներ երբեք ու երբեք պետք չէ փոխանցել այն կայքին, որի հղումը ստացել եք էլեկտրոնային հաղորդագրության միջոցով: Հիշեք, որ դուք ունեք բանկից կամ այլ կազմակերպությունից ճշտելու հնարվորություն, թե արդյո՞ք նրանք են ուղարկել ձեզ այդ նամակը: Երբեք ոչ-ոքի մի ուղարկեք էլեկտրոնային հաղորդագրություն, որը ձեր մասին զգայուն տվյալներ է պարունակում:

- **Զգայուն անձնական տվյալներ, կարևոր տեղեկություններ կամ այլ փաստաթղթեր անվտանգ փոխանցելը**

Կարևոր փաստաթղթեր կամ այլ տեղեկություններ փոխանցելիս ցանկալի է դա անել անձամբ: Եթե անհրաժեշտություն կա փոխանցել առցանց տարբերակով պետք է ընտրել առկա հնարավորություններից առավել անվտանգը, օրինակ՝ Էլ. փոստի դեպքում Gmail համակարգը, որը դեպքերի մեծամասնությունում հասկանում է նամակի կեղծ լինելն ու զգուշացնում է այդ մասին կամ միանգամից նամակը հայտնվում է Spam բաժնում: Կամ երբ կազմակերպությունն ինքն է աշխատակիցներին տրամադրում բավարար պաշտպանության մակարդակ ունեցող համակարգ փաստաթղթաշրջանառության համար, ապա տվյալներ փոխանցելիս պետք է օգտվել հենց այդ հարթակից: Էլեկտրոնային տարբերակով կարևոր ինֆորմացիա փոխանցելուց հետո նախընտրելի է այն ջնջել էլ. հասցեից, այդ դեպքում նույնիսկ եթե հաքերային հարձակման ենթարկվեք, Էլ. փոստի հետ միասին չեք կորցնի նաև այդ կարևոր տեղեկությունները:

- **Ֆիզիկական կրիչների անվտանգություն**

Սարքերը երբեք մի թողեք առանց հսկողության: Եթե կարիք կա ինչ-որ ժամանակով հեռանալու սմարթֆոնի, պլանշետի կամ համակարգչի մոտից, անկախ նրանից, թե որքան ժամանակով եք հեռանում, անպայման կոդավորում դրեք, որ ոչ ոք չկարողանա այն օգտագործել: Եթե կոնֆիդենցիալ տեղեկություններ եք պահում USB կրիչի կամ հիշողության արտաքին սարքի վրա, անպայման կոդավորեք դրանք:

Եթե այնուամենայնիվ ստանում եք կասկածելի հաղորդագրություն ու չեք կողմնորոշվում, թե ինչ անել, կարող եք խորհրդի համար դիմել Անձնական տվյալների պաշտպանության գործակալությանը:

Կարճ կանոններ միշտ հիշելու համար

- **Երբեք մի ուղարկեք անձնական տվյալներ էլ. հաղորդագրությամբ, եթե միանշանակ վստահ չեք, թե ում եք ուղարկում:**

- **Մի սեղմեք անծանոթ, պատահական հասցեներից եկած նամակներում առկա հղումներին ու ֆայլերին:**

- **Ձեր էլ. փոստում, սոցիալական ցանցի էջերում ու այլ հաշիվներում, որտեղ կա հնարավորություն, միացրեք երկփուլանի վավերացում ֆունկցիան՝ որպես պաշտպանության հավելյալ միջոց:**
  Երկփուլանի վավերացումը միացրած լինելու դեպքում մուտքանունն ու գաղտնաբառը մուտք անելուց հետո պետք է հավաքել նաև այն կոդը, որը համակարգը ուղարկում է ձեր սարքին:

- **Ֆիշինգային հարձակման ժամանակ հաքերները կիրառելու են իրական կայքին շատ նման կայք, պետք է ուշադրությամբ զննել ու համոզվել, որ տառային ու սիմվոլային տարբերություններ չկան կայքի հասցեում:**

- **Անվտանգ կայքի հասցեն սկսվում է «https»-ով:**