Արժե կանգ առնել և մտածել

Պաշտպանեք Ձեզ ֆինանսական խարդախությունից

2018 թվականի առաջին վեց ամիսների ընթացքում ավելի քան 34,000 մարդ դարձել է զեղծարարության զոհ 145.4 միլիոն ֆունտ ստեռլինգի չափով

HSBC-ն անընդմեջ աշխատում է, որպեսզի իր հաճախորդները լինեն պաշտպանված զեղծարարությունից:

Այնուամենայնիվ, երբ ավելի ու ավելի շատ մարդիկ թիրախավորվում են զեղծարարների կողմից, կարևոր է դառնում հասկանալ ավելին տվյալ հանցագործության և այն հայտնաբերելու եղանակների վերաբերյալ: Պետք է կանգ առնել և մտածել իրավիճակի մասին, ինչը կօգնի Ձեզ ճիշտ որոշում կայացնել այսպիսի որոշիչ պահերին:

Զեղծարարությունը կարող է տեղի ունենալ ցանկացած վայրում և ցանկացած պահի:
Դա կարող էր պատահել, երբ

- Դուք տանն եք և զանգ եք ստանում Ձեր հաշվից շտապ գումար փոխանցելու պահանջով
- Դուք ռեստորանում եք և ստանում եք տեքստային հաղորդագրություն՝ խնդրելով շտապ զանգահարել տվյալ համարին
- Դուք ճանապարհում եք երեխաներին դպրոց և ստանում եք էլ.նամակ՝ խնդրելով Ձեզ փոխանցել անձնական տեղեկատվություն

Զեղծարարները գործողություններով, արտաքին տեսքով, ձայնով նմանվում են Բանկին, Ոստիկանությանը, նույնիսկ Ձեր Ինտերնետ մատակարարին:

HSBC

*Source: www.ukfinance

Զեղծարարությունը կարող է տեղի ունենալ ցանկացած վայրում և ցանկացած պահի:

Ահա և օրինակ.
Դուք տանը դիտում եք հեռուստացույց և զանգ եք ստանում մի անձից, ով ասում է, որ նա Ձեր Բանկի՝ զեղծարարության դեմ պայքարի դեպարտամենտի աշխատակից է:

Բանկը ...
...կտեղեկացնի, որ Ձեր հաշվին նկատվել է ինչ-որ անորոշ շարժ և կստուգի ՝ արդյո՞ք դուք կատարել եք վճարումներ: Եթե ոչ, ապա նրանք կդադարեցնեն վճարումը, կարգելափակեն Ձեր քարտը և կպատվիրեն նոր քարտ:

Զեղծարարը կարող է...
...խնդրել Ձեզ մուտք գործել Ձեր ինտերնետային բանկային հաշիվ և ապահովության նպատակով միջոցներ փոխանցել մեկ այլ հաշվի: Նրանք կարող են հայցել Ձեր PIN-ը կամ առցանց բանկային գաղտնաբառերը և այլ անվտանգության մանրամասներ:

Բանկն արդեն իսկ կարող է փոխանցել դրամական միջոցները Ձեր իսկ խնդրանքով: Բանկը երբեք չի պահանջի տրամադրել Ձեր գաղտնաբառերը կամ **PIN**- ը:

Եթե կասկածում եք, որ Ձեր հաշվին կատարվել է խարդախության փորձ, ապա կապ հաստատեք HSBC-ի՝ Ձեր կորպորատիվ բիզնեսի զարգացման գծով կառավարչի հետ:

Զեղծարարություն հեռախոսակապի միջոցով ՝ Վիշինգ

Հեռախոսային խարդախությունը կամ վիշինգի դեպքում, զեղծարարները զանգահարում են ընկերություն՝ ներկայանալով որպես Բանկ կամ այլ վստահություն ներշնչող կազմակերպություն: Նրանք կարող են միտումնավոր կեղծել իրենց հեռախոսահամարը, այնպես, որ այն Ձեզ համար թվա վստահելի:

Նրանք կարող են շատ համոզիչ թվալ և իմանալ Ձեր անձնական տվյալների մի մասը, օրինակ՝ Ձեր հաշվեհամարը կամ հասցեն: Եթե դուք զգում եք, որ մի բան այն չէ, ապա մի վախեցեք դադարեցնել զանգը: Դուք միշտ կարող եք զանգահարել Բանկ Ձեզ արդեն հայտնի կամ քարտի հետևում նշված հեռախոսահամարով:

Զեղծարարները կարող են բաց պահել գիծը և նույնիսկ վնասել այն, այնպես որ փորձեք օգտագործել այլ հեռախոսակապ կամ սպասել առնվազն 10 վայրկյան Ձեր զանգը կատարելուց առաջ: Կարող եք նախևառաջ զանգահարել Ձեր ընկերոջը կամ հարազատին՝ համոզվելու, որ կեղծարարը չի լսում, երբ զանգ եք կատարում:

Վիշինգի օրինակներ
- Ոստիկանությունը կամ Հանցավորության դեմ Պայքարող Ազգային Գործակալությունը ունեն Ձեր օգնության կարիքը՝ հանցագործությունը բացահայտելու համար և այդ իսկ պատճառով խնդրում են Ձեզ գումարը տեղափոխել «ապահով հաշիվ»:
- Ձեր բանկին անհրաժեշտ է Ձեր օգնությունը՝ խարդախությունը բացահայտելու համար
- Ձեր Ինտերնետ մատակարարը զանգահարում է Ձեզ այնպիսի խնդրի լուծման համար, որի մասին Դուք տեղյակ չեք
- Հարկային Տեսչությունը սպառնում է Ձեզ բանտարկել, եթե անհապաղ չվճարվեք հարկերը

Իսկ դուք գիտեիք, որ Անգլիայում զեղծարարությունը տարեկան արժենում է £190 բիլիոն:

Աղբյուր՝ Experian 'Annual Fraud Indicator' 2017 report

Զեղծարարություն կարճ հաղորդագրության միջոցով՝ Սմիշինգ

Կարճ հաղորդագրության միջոցով զեղծարարությունը կամ Սմիշինգ –ի դեպքում զեղծարարը ուղարկում է Ձեզ այնպիսի տեքստային հաղորդագրություն, որը կարծես թե ուղարկվել է Ձեր բանկից կամ մեկ այլ կազմակերպությունից, որին դուք վստահում եք:

Նրանք կարող են Ձեզ տեղեկացնել, որ Ձեր հաշիվը ենթարկվել է խարդախության և խնդրեն Ձեզ տրամադրել կամ թարմացնել անձնական տվյալները: Տեքստը կարող է առաջարկել վաուչերներ, հարկերի փոխհատուցում կամ խնդրել Ձեզ հաստատել ծանրոցների առաքումը:

Ահա և օրինակը
Դուք ռեստորանում եք և ստանում եք տեքստային հաղորդագրություն Ձեր Բանկ զանգահարելու խնդրանքով: Դուք զանգահարում եք տրված համարին և Ձեզ տեղեկացնում են, որ Ձեր հաշվին կասկածելի շարժ է տեղի ունեցել և հարցնում են՝ արդյոք արդեն կատարել եք վճարում:

Բանկը ...
...կդադարեցնի վճարումը, կապաակտիվացնի Ձեր քարտը և կթողարկի նորը:

Զեղծարարը կարող է...
...խնդրել Ձեր գաղտնաբառը, PIN- ը, հաշվեհամարը կամ տեսակավորող ծածկագիրը վճարումը դադարեցնելու նպատակով:

Սմիշինգ-ի օրինակներ
- Ձեր Բանկը տեղեկացնում է, որ Ձեր ինտերնետ բանկային ծառայության մուտքը սահմանափակված է, և խնդրում է Ձեզ սեղմել հղումը՝ կրկին վերականգնելու համար:
- Ձեր Բանկը խնդրում է Ձեզ գումարը տեղափոխել «ապահով հաշիվ»:

էլ. հաղորդագրության միջոցով զեղծարարություն

Նաև հայտնի է որպես ֆիշինգ, էլեկտրոնային նամակները ուղարկվում են զեղծարարների կողմից ՝ խրախուսելով Ձեզ տրամադրելու անձնական տվյալները կամ բացելու կեղծ հղումները: Մի քանի րոպե տրամադրեք էլ. նամակի իսկությունը ստուգելու համար:

Ահա և օրինակը.
Աշխատավայրում եք և ստանում եք էլեկտրոնային նամակ, որը, կարծես թե ուղարկվել է Ձեր Բանկից:

Բանկը պետք է...
...Էլեկտրոնային նամակով Ձեզ տեղեկացնի իրենց խնայողական հաշիվների, հիփոթեքային վարկերի կամ այլ հաշիվների և ծառայությունների մասին, որոնք կարող են Ձեզ համար օգտակար լինել:

Զեղծարարը կարող է...
...էլեկտրոնային նամակով խնդրել Ձեզ տրամադրելու անձնական տվյալներ կամ տեղեկատվություն Ձեր բանկային հաշիվների վերաբերյալ:

Ֆիշինգ-ի օրինակ
- Հարկային Տեսչությունը Ձեզ էլեկտրոնային նամակով տեղեկացնում է, որ դուք ունեք հարկերի վերադարձ
- Դուք շահել եք վիճակախաղում, որում չեք մասնակցել

Էլ.փոստի միջոցով զեղծարարության՝ ֆիշինգ -ի նշանները

- Ձեզանից պահանջվում է անհապաղ վճարում կատարել:
- Ուղարկողի էլեկտրոնային փոստի հասցեն չի համընկնում կազմակերպության վեբ կայքի հասցեի հետ, որին այն պատկանում է. ուղղեք Ձեր կուրսորը ուղարկողի անվան վրա իրական հասցեն պարզելու նպատակով:
- Այն խնդրում է Ձեզ կիսվել անձնական տեղեկատվությամբ:
- Էլեկտրոնային փոստով հղումները պաշտոնական հասցեներ չեն, այսինքն՝ hsbc: co.uk.: Ուղղեք Ձեր կուրսորը հղման վրա վերջինիս իրական հասցեն բացահայտելու համար:

Ներդրումային զեղծարարություն

Ներդրումային զեղծարարության դեպքում Ձեզ առաջարկվում է բարձր եկամտաբերություն՝ ցածր ռիսկայնությամբ: Խարդախություններին իրական տեսք հաղորդելու նպատակով զեղծարարները հաճախ կիրառում են կեղծ վկայագրեր, կեղծ կայքեր և մարքեթինգային այլ նյութեր: Հավանաբար այն խաբեություն է առաջարկի շատ գրավիչ լինելու դեպքում:

Ներդրումային զեղծարարությունը հայտնաբերելու ուղիներ

- Ձեզ հետ կապվում են հեռախոսով, էլեկտրոնային փոստով, տեքստային հաղորդագրությամբ կամ Ձեր տուն զանգահարում է որևէ մեկը՝ ներդրումային առաջարկով:
- Այն «ընկերությունը», որը կապվել է Ձեզ հետ, Ձեզ թույլ չի տալիս հետ զանգահարել:
- Ձեր վրա ճնշում է գործադրվում արագ որոշում կայացնել, օրինակ, եթե զանգահարողը ասում է, որ առաջարկը «միայն ներկա պահին է հասանելի» կամ «բաց չթողնեք հնարավորությունը»
- Միակ հետադարձ կապի միջոցը, որը Ձեզ տրվել է, բջջային հեռախոսահամարն է կամ փոստարկղի հասցեն
- Թվում է չափազանց լավ իրական լինելու համար՝ բարձր եկամտաբերություն՝ ցածր ռիսկայնությամբ:

Վերջերս նկատվում է, որ զեղծարարները, շահագործելով կորոնավիրուսի բռնկումը, ներկայանում են որպես վստահություն ներշնչող կազմակերպություններ, ինչպիսիք են Բանկերը և նույնիսկ Առողջապահության Համաշխարհային Կազմակերպությունը: Մենք նկատում ենք, որ զեղծարարները հատուկ թիրախավորում են բժշկական սեգմենտը: Ստորև Ձեզ ներկայացնում ենք զեղծարարության որոշ օրինակներ, որոնք կօգնեն Ձեզ պաշտպանվել հարձակումներից: Նմանատիպ զեղծարարությունները կատարվում են հետևյալ եղանակներով՝

Հեռախոսազանգեր

Էլ.հաղորդագրություններ

Տեքստային հաղորդագրություններ (SMS)

Սոցիալական մեդիայի հրապարակումներ

Նրանք կարող են լինել Ձեզ արդեն հայտնի հեռախոսահամարները կամ էլ.փոստի հասցեները: Այսպիսով, խնդրում ենք Ձեզ լինել ուշադիր և պարզել այդ տվյալների իսկությունը: Երբեք մի՛ հաստատեք կապ ուղարկողի հետ՝ օգտագործելով հաղորդագրությունում առկա կոնտակտային տվյալները: Եթե կասկածներ ունեք, ապա զանգահարեք HSBC կայքում նշված հեռախոսահամարներով կամ կապ հաստատեք Ձեր կորպորատիվ բիզնեսի գծով կառավարչի հետ:

Խարդախության օրինակներ

Բժշկական ոլորտի աշխատակիցներ

Հանցագործները թիրախավորում են բժշկական ոլորտի աշխատակիցներին՝ ուղարկելով կեղծ հաղորդագրություններ կառավարության կողմից, որոնք առաջարկում են կորոնավիրուսի տարածման նպատակով կատարել վճարումներ: Կառավարությունը չի զանգահարի և չի ուղարկի Ձեզ նման տեքստային կամ էլ հաղորդագրություն, հետևաբար այն կարող է խաբեություն լինել: Ուշադիր եղեք տառասխալներին, տարօրինակ հասցեներին և ողջույնի ձևին: Երբեք մի բացեք հղումներ տարօրինակ հաղորդագրությունների մեջ:

Կեղծ ապրանքներ

Հանցագործները շահագործում են կորոնավիրուսի բռնկումը՝ առաջարկելով այնպիսի կեղծ ապրանքներ, ինչպիսիք են դիմակները, ձեռքերն ախտահանող գելը և այլն, որոնք արդյունքում չեն առաքվելու: Եթե ստանում եք շատ գրավիչ առաջարկ, ապա դա հավանաբար զեղծարարություն է: Ուշադիր եղեք օնլայն գնումներ կատարելիս: Օգտագործեք անվտանգ վճարման եղանակներ, որոնք խորհուրդ են տրվում վստահելի մանրածախ գնորդների կողմից և ուշադիր եղեք բանկային հաշվին փոխանցումներ կատարելու պահանջներին:

Նմանակություն

Զեղծարարները կարող են ներկայանալ որպես Բանկի կամ պետական մարմինների աշխատակից և խնդրել Ձեզ կորոնավիրուսի պատճառով գումար փոխանցել «ապահով հաշիվներին»: HSBC-ն Ձեզանից երբեք չի պահանջի տրամադրել PIN-ը, գաղտնաբառերը կամ առաջարկի Ձեր գումարները փոխանցել այլ հաշիվների: Եթե Ձեզ մոտ առաջանում է հնարավոր զեղծարարության վերաբերյալ կասկած, ապա մի պատասխանեք հաղորդագրություններին և մի շարունակեք հեռախոսային խոսակցությունը:

Կիբերհանցավորություն

Առցանց զեղծարարությունների թիվը աճում է: Զեղծարարներն օգտագործում են բարդ մարտավարություններ, ինչպիսիք են կեղծ հղումների, մանրածախ վեբ էջերի, կեղծ pop-up պատուհանների ստեղծումը՝ Ձեր ֆինանսական տվյալներն ու գաղտնաբառերն իրենց համար հասանելի դարձնելու համար:

Պաշտպանվեք առցանց զեղծարարությունից

- Միշտ թարմացրեք Ձեր պլանշետի, սմարթֆոնի և համակարգչի վրա գործարկվող համակարգերը՝ դրանք հասանելի դառնալուն պես:
- Տեղադրեք հակավիրուսային ծրագիր հայտնի և վստահելի ընկերությունից:
- Առցանց գնումներ կատարելիս միշտ ստուգեք Ձեր կայքի իսկությունը, և Ձեր անձնական կամ վճարման մանրամասները մուտքագրելիս համոզվեք, որ հասցեների տողում առկա է փական, որը ցույց է տալիս, որ Ձեր կապն ապահով է:
- Եթե ինչ-որ բան եք գնում առցանց և չգիտեք վաճառողին, երբեք մի վճարեք բանկային փոխանցումով: Միշտ օգտագործեք կրեդիտ/դեբետ քարտեր, PayPal - կամ վճարման այլ եղանակ, որն առաջարկում է որոշակի պաշտպանություն կեղծիքներից:

Հաշվի ապօրինի տնօրինում

Այս աճող հանցագործությունը ինքնության գողության մի ձև է, որտեղ զեղծարարը ձեռք է բերում տուժողի բանկային կամ վարկային քարտի հաշիվը, այնուհետև կատարում է չարտոնված վճարումներ:

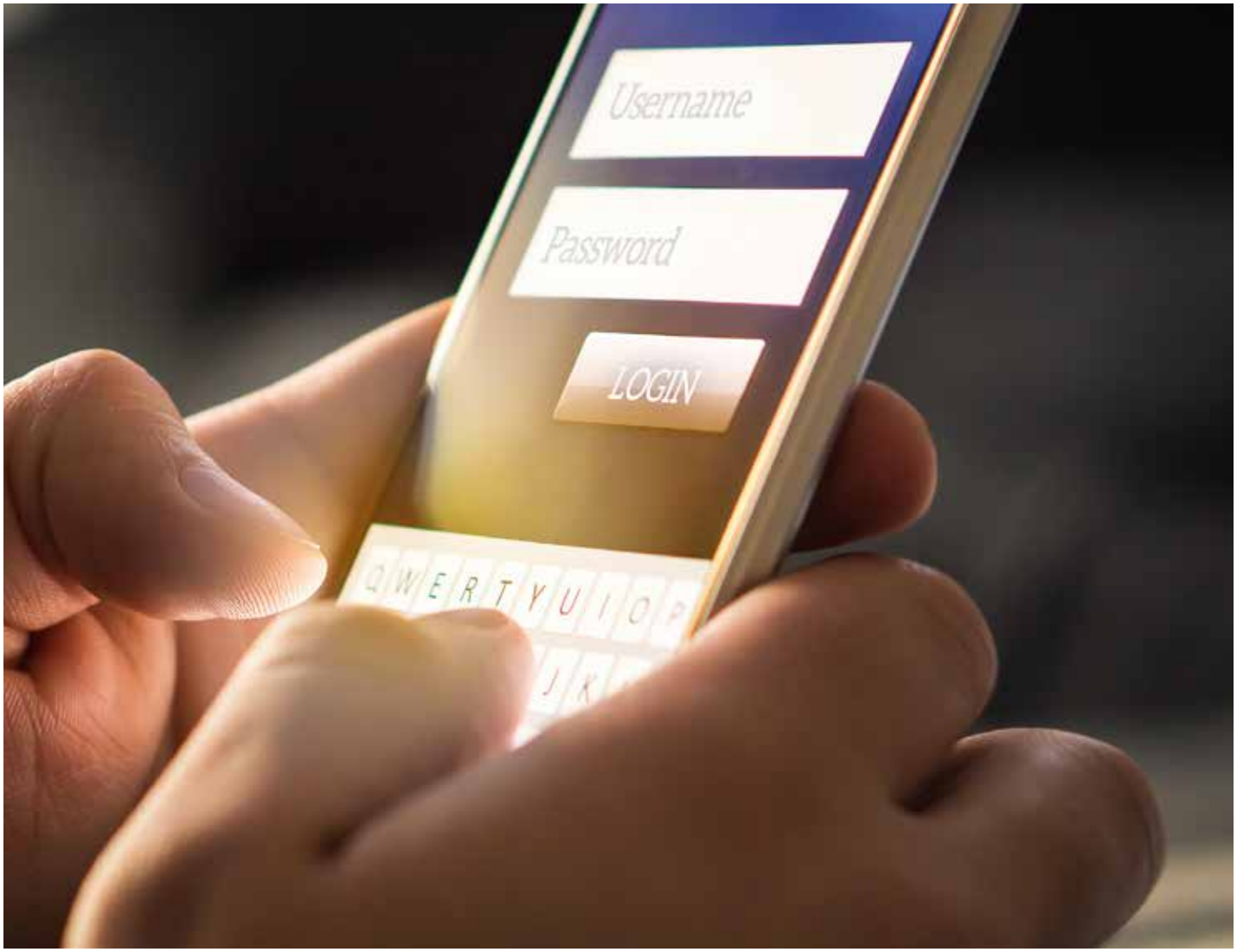
Ինչպե՞ս դա կարող է տեղի ունենալ

Զեղծարարը զանգահարում է՝ ներկայանալով որպես Ձեր ինտերնետ մատակարար: Նրանք Ձեզ տեղեկացնում են, որ դուք ունեք կապի որոշ խնդիրներ: Խնդիրը շտկելու համար նրանք խնդրում են մուտք գործել Ձեր համակարգիչ և ներբեռնել որոշակի ծրագիր:

Տվյալ ծրագիրը թույլ է տալիս զեղծարարին տեսնել Ձեր էկրանը: Դրանից հետո նրանք խնդրում են մուտք գործել Ձեր օնլայն բանկային հաշիվ: Զեղծարարն այժմ հնարավորություն է ունենում գողանալու Ձեր բանկային տվյալները և գումարները:

Հաշվի բռնագրավման զեղծարարության օրինակ

- Զանգահարողը Ձեզ առաջարկում է դրամական փոխհատուցում և «պատահաբար» Ձեզ չափազանց մեծ գումար է փոխանցում և խնդրում է վերադարձնել գերվճարը: Սա Ձեր հաշվին զեղծարարի անվամբ նոր վճար է ստեղծում, և այժմ զեղծարարը կարող է Ձեր հաշվից գումար փոխանցել իր հաշվին



Լավագույն խորհուրդներ, որոնք կօգնեն Ձեզ զերծ մնալ զեղծարարությունից

Միշտ կասկածի տակ դրեք անցանկալի մոտեցումները
Փոխարենը՝ ուղղակիորեն կապվեք ընկերության հետ՝ օգտագործելով էլեկտրոնային փոստ կամ հեռախոսահամար, որը կարող եք ստուգել՝ իրական է, թե ոչ:

Մի՛ կիսվեք անձնական տվյալներով
Երբեք մի բացահայտեք Ձեր գաղտնաբառը կամ մի տվեք Ձեր քարտի տվյալները էլեկտրոնային հասցեով: Ստուգեք Ձեր կողմից օգտագործվող կայքէջի հասցեն: Զգույշ եղեք սոցիալական կայքերում կիսվող մանրամասներից և ստուգեք Ձեր անձնական գաղտնիության կարգավորումները:

Թարմացրեք Ձեր գաղտնաբառերը
Փորձեք փոխել Ձեր գաղտնաբառերն առնվազն տարին երկու անգամ: Մի՛ օգտագործեք գաղտնաբառ, որը կարելի է հեշտությամբ կռահել, և համոզվեք, որ Ձեր օնլայն բանկային ծառայության գաղտնաբառը նույնը չէ, որն օգտագործում եք այլ կայքերում:

Պարբերաբար ստուգեք բանկային հայտարարությունները
Եթե կան գործարքներ, որոնք Ձեզ անծանոթ են, միշտ կապնվեք մեզ հետ.

Ստուգեք Ձեր վարկի մասին հաշվետվությունը
Եթե ինչ-որ մեկը Ձեր անունն օգտագործել է վարկ կամ վարկային քարտ ձևակերպելու համար, այն կարող է չերևալ Ձեր քաղվածքներում: Ստուգեք Ձեր վարկի մասին հաշվետվությունը առնվազն տարին մեկ անգամ տարօրինակ գործողության բացահայտման նպատակով:

Պարբերաբար թարմացումներ
Միշտ թարմացրեք Ձեր համակարգչի, պլանշետի և սմարթֆոնի գործող ծրագրերը՝ դրանք հասանելի դառնալուն պես և տեղադրեք հակավիրուսային ծրագիր:

Ոչնչացրեք կարևոր փաստաթղթերը
Ոչնչացրեք ցանկացած փաստաթուղթ, որը պարունակում է անձնական տեղեկություններ, ինչպիսիք են բանկային հաշվետվությունները, քարտի տվյալները և այլ կարևոր տվյալները:

Եթե կասկածում եք, որ Ձեր հաշվին կատարվել է խարդախության փորձ, ապա կապ հաստատեք HSBC-ի՝ Ձեր կորպորատիվ բիզնեսի զարգացման գծով կառավարչի հետ:

HSBC-ն երբեք չի…

- Զանգահարի և խնդրի տրամադրել Ձեր PIN-ը կամ գաղտնաբառը, նույնիսկ հավաքելով դրանք Ձեր հեռախոսի ստեղնաշարի միջոցով:
- Խնդրի, որ հեռախոսով մեզ տրամադրեք թվեր էլեկտրոնային փոստից, տեքստային հաղորդագրության կամ Ձեր անվտանգության բանալիի միջոցով:
- Խնդրի Ձեզ գումար փոխանցել Ձեր անունով մեկ այլ «ապահով» հաշվի, նույնիսկ զեղծարարության կասկածի առկայության դեպքում
- Խնդրի Ձեզ գումար հանել հաշվից և մեզ հանձնել՝ ապահովության համար:
- Ուղարկի որևէ անձի Ձեր տուն՝ կանխիկ գումար, Ձեր PIN-ը, քարտեր կամ չեկային գրքույկ վերցնելու նպատակով, նույնիսկ եթե դուք զեղծարարության զոհ եք:
- Խնդրի Ձեզ վճարում կատարել ապրանքների համար՝ օգտագործելով Ձեր քարտը, այնուհետև պահպանման նպատակով դրանք հանձնել մեզ: