9. ԽԱՐԴԱԽՈՒԹՅՈՒՆ ԵՎ ՋԵՂԾԱՐԱՐՈՒԹՅՈՒՆ

Ողջույն, ֆինանսական կրթության դասընթացի շրջանակներում այսօր խոսելու ենք ֆինանսական խարդախությունների և զեղծարարությունների մասին: Սկզբում հասկանանք՝ արդյո՞ք տարբեր են այս երկու հասկացությունները:

Ֆինանսական զեղծարարությունների նպատակն է հափշտակել գումար՝ անձնական տվյալներ կորզելու միջոցով, այս գործողություններն ուղղված են հանրության դեմ, դե իսկ **ֆինանսական խարդախությունները** կոնկրետ անձին ուղղված գործողություններ են՝ նրան ֆինանսապես վնասելու, գումար կորզելու նպատակով:

Եկե'ք ծանոթանանաք առավել հաճախ հանդիպող զեղծարարությունների և խարդախությունների որոշ տեսակներին, որպեսզի, ինչպես ասում են, լինենք տեղեկացված և զինված:

Սկսենք **վնասակար համակարգչային ծրագրերից:**

Վերջիններս կարող են գողանալ տեղեկատվություն, վնասել տվյալներ, յուրացնել վեբ-կայքի այցելությունների վերաբերյալ տեղեկատվություն և լրտեսել ձեզ և ձեր բիզնեսի գործունեությունը թվային տիրույթում:

Վնասակար ծրագիրը սովորաբար ներբեռնվում է էլեկտրոնային նամակների միջոցով կամ կեղծ հղումներով, այնպես որ անհրաժեշտ է չափազանց ուշադիր լինել էլեկտրոնային նամակներ ստանալիս, ինչպես նաև ոչ վստահելի հղումներով անցնելիս:

Զեղծարարության հայտնի և տարածված տեսակ է **սփուֆինգը**: Սա գործողությունների մի շարք է, որն ուղղված է այս կամ այն վավեր տեղեկատվությունը կեղծ տեղեկություններով փոխարինելուն: Սփուֆինգը հաճախ օգտագործվում է խաբեբաների կողմից՝ քողարկելու էլեկտրոնային փոստի հասցեն, ցուցադրվող անունը, հեռախոսահամարը, տեքստային հաղորդագրությունը կամ կայքի URL-ը՝ զոհին համոզելու համար, որ վերջինս առնչվում է հայտնի և վստահելի աղբյուրի հետ: Սովորաբար, այս դեպքում փոփոխությունները ազդում են մեկ տառի, թվի կամ նշանի վրա, այնպես որ առաջին հայացքից աղբյուրը հուսալի է թվում:

Այսպես, օրինակ, եթե դուք հաճախ գնումներ եք կատարում արտասահմանյան գործընկերներից, ապա զեղծարարները կարող են կեղծել ձեր գործընկեր

մատակարարների իրական էլ. փոստի հասցեն՝ կեղծ տվյալներով հաշիվ-ապրանքագիր ներկայացնելով ձեզ։

Օրինակ՝ կարող ենք նամակ ստանալ @CompanyACB.com հասցեից @CompanyABC.com-ի փոխարեն, տարբերությունն ընդամենը մեկ տառ է, որը, ցավոք, կարող է շատ թանկ արժենալ։

Այլ դեպքերում հանցագործները կեղծում են հեռախոսահամարը կամ զանգահարողի անունն այնպես, որ մենք համոզված լինեք, որ զանգը, օրինակ, բանկից է։

Օրինակ՝ 010 70 70 70 համարի փոխարեն զանգ ենք ստանում 0010 70 70 70 հեռախոսահամարից։ Արդյունքում, հավատալով, որ զանգն իրական հասցեատիրոջից է, մենք կարող ենք հետևել «հոգատար» աշխատակցի հրահանգներին, կատարել ֆինանսական միջոցների տեղաշարժ տարբեր հաշիվների միջև կամ փոխանցել խիստ գաղտնի տեղեկատվություն։

Առավել հաճախ է հանդիպում նաև **ֆիշինգը**։ Սա կիբեռհանցագործության տեսակ է, որի նպատակն է ստանալ որևէ սոցիալական կայքի օգտատիրոջ գաղտնի տվյալները, ծածկագիրը և ծածկանունը։
Ֆիշինգն արվում է զանգվածային էլեկտրոնային սպամ նամակների միջոցով, որոնք մեզ կարող են ուղարկվել հայտնի բրենդների, գործընկեր բանկերի կամ սոցիալական ցանցերի անունից։ Օրինակ՝ կարող եք նամակ ստանալ կարծես թե ֆեյսբուքյան ադմինիստրացիայից, որը նշում է, որ ձեր ֆեյսբուքյան հաշվի հետ խնդիր կա և դուք անհապաղ պետք է թարմացնեք կամ վերահաստատեք ձեր տվյալները։ Արդյունքում ամբողջ տեղեկատվությունը հայտնվում է խաբեբաների տիրապետության տակ։

Նման նամակները հաճախ պարունակում են ինչ-որ կայքի հղում, որը արտաքնապես չի տարբերվում իրական կայքից։ Անցնելով հղումով մուտք ենք գործում կեղծ էջ՝ մեր իրական մուտքանունը և գաղտնաբառը լրացնելով, որը հաքերներին թույլ է տալիս մուտք գործել մեր բանկային հաշիվ, սոց ցանցի հաշիվ և այլն։

Հայտնի նաև նաև **«կանխավճար» կամ «Խարդախություն 419» անունով խարդախությունը:**
Այս խարդախության դեպքում Դուք կարող եք անծանոթ անձանցից ստանալ նամակներ և էլ. հաղորդագրություններ, որտեղ Ձեզ կառաջարկեն խոշոր դրամական

պարգև: Սակայն, որպես կանոն, ձեզ կխնդրեն վճարել որոշակի վճար՝ գործարքն ավարտին հասցնելու համար: Արդյունքում, ոչ միայն չեք ստանում ձեզ խոստացված գումարը, այլև կորցնում եք ձեր կողմից փոխանցված դրամական միջոցները:

Օրինակ՝ որևէ կայք այցելելիս կայքը «ուրախությամբ տեղեկացնում է», որ դուք հարյուր հազարերորդ այցելուն եք, և ունեք մեծ նվեր. միայն պետք է գրանցվել և տրամադրել ձեր բանկային քարտի տվյալները: Նվերն այդպես էլ չի ստացվում, իսկ քարտային հաշվից անհասկանալի գումարներ են գանձվում անհայտ անձանց կողմից:

Հանցագործությունների տեսակների շարքը կարելի է երկար թվարկել: Դրանք կարող են ներառել փաստաթղթերի կեղծումից, այդ թվում՝ հաշիվ-ապրանքագրերի, մինչև օր-օրի ավելացող կիբերհանցագործությունների նորանոր տեսակները:

Ձեզ և ձեր բիզնեսը պաշտպանելու համար անհրաժեշտ է լինել զգոն և կատարել որոշակի պաշտպանական քայլեր, այդ թվում՝

- Կիրառե՛ք ուժեղ արձագանքման, վերականգնման և պահուստային կրկնօրինակման գործընթացներ, փորձեք տեղեկատվության կրկնօրինակները պահել օգտագործվող համակարգիչներից տարբեր այլ կրիչների վրա:
- Պարբերաբար, պլանավորված հիմունքներով գործարկե՛ք արդի հակավիրուսային ծրագրեր կազմակերպության բոլոր սարքերի վրա:
- Խուսափե՛ք կասկածելի կայքերից, և մի՛ ներբեռնեք կասկածելի և անծանոթ անվճար ծրագրեր/ հավելվածներ, մի օգտագործեք USB քարտեր չստուգված աղբյուրներից:
- Կիրառե՛ք հավելվածների whitelisting-ը՝ սպիտակ ցուցակագրումը, ինչը թույլ է տալիս արգելափակել ցանկացած համակարգչային ծրագիր, որը նախապես լիազորված չէ:
- Եթե կասկածելի նամակներ կամ զանգեր եք ստանում, օրինակ, ձեզ սպասարկող բանկի անունից, ապա մի՛ տրամադրեք ոչ մի տվյալ, մի՛ անցեք հղումներով: Եթե կասկածներ ունեք, մի՛ վախեցեք դադարեցնել հեռախոսազանգը կամ նամակագրությունը՝ հրաժարվելով տրամադրել որևէ տեղեկատվություն: Պարզապես հնարավորինս արագ կապ հաստատեք բանկի հետ, ներկայացրեք իրավիճակը:
- Ուշադի՛ր եղեք անծանոթ զանգերին, հատկապես, երբ ձեզնից պահանջվում է տրամադրել գաղտնի տեղեկատվություն ընկերության մասին:

- Գնումներ կատարե՛ք անվտանգության համակարգ ունեցող կայքերից՝ համոզված լինելով, որ անվտագության բանալին երևում է վեբ-կայքի պատուհանում՝ անձնական տեղեկատվություն մուտքագրելիս։
- Պահպանե՛ք Ձեր պատվերի հաստատման պատճենը։ Կրեդիտ քարտով օնլայն գնումներ կատարելիս, միշտ մուտք գործեք Mastercard Securecode կամ Verified by Visa համակարգերով։ Վերջիններս ապահովում են անձնական տվյալների պաշտպանություն։
- Պաշտպանե՛ք Ձեր գաղտնաբառերը։ Օգտագործե՛ք տարբեր գաղտնաբառեր տարբեր համակարգեր մուտք գործելու համար, փորձե՛ք դրանք դարձնել դժվար կռահելի, օրինակ մի՝ օգտագործեք երեխաների անունները կամ ծննդյան ամսաթվերը, և, ընդհակառակը, օգտագործե՛ք մեծատառեր/փոքրատառեր, թվեր և նշաններ մեկ գաղտնաբառի մեջ։
- Բանկային հաշիվների քաղվածքներն ամբողջական վիճակով մի՛ նետեք աղբը, պատառոտե՛ք դրանք մանր կտորների։ Նույն կերպ վարվե՛ք Ձեր բանկային հաշվի տվյալներ պարունակող փաստաթղթերի հետ՝ անդորրագրեր, ծանուցումներ, հաշվի վավերապայմաններով թերթիկներ և այլն։
- Եվ, վերջապես, ձեր բանկային տվյալները մի՝ բարձրաձայնեք հանրային տարածքներում, մի՝ ուղարկեք դրանք նամակագրությամբ։ Եթե անհրաժեշտություն է առաջանում պահպանելու քարտի տվյալները ինչ-որ տեղ, ապա առանձին գրանցեք և պահեք քարտի վրայի թվերը, գաղտնաբառը, CVV կոդը։

Հիշեք, որ ոչ մի բանկ ձեզ երբեք չի խնդրի տրամադրել հետևյալ տեղեկատվությունը՝

- Ձեր 4 նիշանի PIN կոդը,
- Կրեդիտ կամ դեբետ քարտի ամբողջական տեղեկատվությունը,
- Օնլայն բանկային ծառայության կոդը կամ գաղտնաբառը,
- Ինչպես նաև չի խնդրի իրականացնել միջոցների տեղափոխում մեկ հաշվից մեկ այլ հաշիվ՝ հիմնավորելով գործարքի իրականացման անհրաժեշտությունը որպես միջոցների ապահովության երաշխիք։

Եվ, վերջապես, վստահ եղեք, որ ձեր կազմակերպության բոլոր աշխատակիցները նույնպես տեղեկացված են անվտանգության պահպանման բոլոր կանոնների և ընթացակարգերի մասին և անպայմանորեն հետևում ու պահպանում են դրանք։