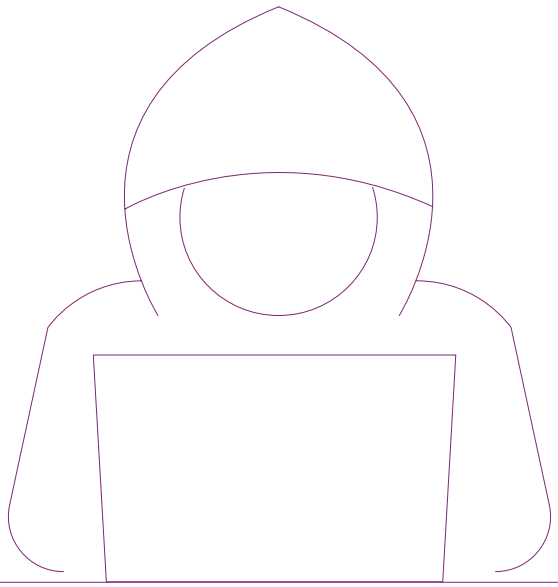
UK Government

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

Կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունների կիբեռանվտանգություն

ՈՒՂԵՑՈՒՅՑ ՀԱՅ ԱԿՏԻՎԻՍՏՆԵՐԻ, ԽԱՂԱՂԱՇԻՆԱՐԱՐՆԵՐԻ ԵՎ ՓԱՍՏԱԲԱՆՆԵՐԻ ՀԱՄԱՐ



Հեղինակ՝ Ջենիֆեր Կանաան
Խմբագիր՝ Դանիելլա Պելեդ
Թարգմանիչ՝ Սիրանուշ Հովհաննիսյան
Դիզայն՝ Համբըլ Բի Դիզայն
Դիզայնը հարմարեցրեց հայերենին՝ Լուսինե Խանդիլյան

Կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունների կիբերանվտանգություն

ՈՒՂԵՑՈՒՅՑ ՀԱՅ ԱԿՏԻՎԻՍՏՆԵՐԻ, ԽԱՂԱՂԱՇԻՆԱՐԱՐՆԵՐԻ և ՓԱՍՏԱԲԱՆՆԵՐԻ ՀԱՄԱՐ

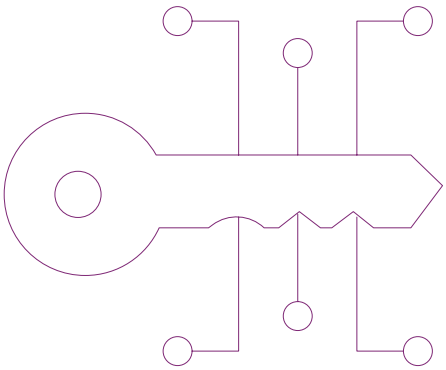
Սույն հրապարակումը պատրաստվել է Միացյալ Թագավորության արտաքին գործերի, համագործակցության և զարգացման նախարարության (FCDO) աջակցությամբ իրականացվող «Ուժեղացնելով արևելյան հարևանության կայունությունը» (BREN) նախագծի շրջանակներում: Սույն փաստաթղթում ներկայացված կարծիքները, արդյունքները և եզրակացությունները հեղինակային են և պարտադիր չէ, որ արտացոլեն Միացյալ Թագավորության կառավարության տեսակետները:

Կին խաղաղաշինարարների համաշխարհային ցանցի (ԿԽՀՑ) հետ համատեղ իրականացվող BREN նախագծի նպատակն է ամրապնդել քաղաքացիական հասարակության կազմակերպությունների կայունությունը և նպաստել մարդու անվտանգությանը, խաղաղությանն ու կայունությանը Հարավային Կովկասում և Մոլդովայում, հատկապես կանանց և այլ մարգինալացված համայնքների համար:

Պատերազմի և խաղաղության լուսաբանման ինստիտուտը (ՊԽԼԻ) տեղական մարմիններին հնարավորություն է տալիս փոփոխություններ անել հակամարտությունների, ճգնաժամերի և անցումային փուլերում գտնվող երկրներում: Այնտեղ, որտեղ տարածվում են ատելության խոսքն ու քարոզչությունը, իսկ լրագրողներն ու քաղաքացիական ակտիվիստները հարձակման են ենթարկվում, ՊԽԼԻ-ն տարածում է հավաստի կարևոր տեղեկատվություն և կազմակերպում հանրային բանավեճեր:

Սույն ուղեցույցում ներկայացված տեղեկատվությունը չի հանդիսանում և նախատեսված չէ որպես կիբերանվտանգության վերաբերյալ խորհրդատվություն տրամադրելու միջոց: Այն կրում է բացառապես տեղեկատվական բնույթ:

Կազմակերպությունների համար չափազանց կարևոր է ներգրավել կիբերանվտանգության խորհրդական, խորհրդատու, կամ, առնվազն, SS ոլորտի փորձագետ՝ կազմակերպության կիբերմիջավայրն ամրացնելու համար: Այս փորձագետները կարող են օգնել, ուղղորդել և արագ արձագանքել հարձակման կամ այլ խնդիրների դեպքում:



INSTITUTE FOR WAR & PEACE REPORTING

IWPR

Ձենիֆեր Կանաանի մասին

Ձենիֆեր Կանաանը Պատերազմի և խաղաղության լուսաբանման ինստիտուտի (ՊԽԼԻ) «Ուժեղացնելով արևելյան հարևանության կայունությունը» (BREN) նախագծի տարածաշրջանային հաղորդակցության համակարգող է: Թվային հաղորդակցության և շահերի պաշտպանության փորձագետ Ձենիֆերը 2016 թվականից աշխատում է ՊԽԼԻ-ում՝ մասնակցելով տարբեր նախագծերի, այդ թվում՝ նորարարական «Սայբըր էրըբս» “Cyber Arabs” նախագիծը, ՊԽԼԻ-ի կիբերանվտանգության ռեսուրսների համապարփակ արաբալեզու կայքը, էթիհադ-ի շահերի պաշտպանության թվային ձեռնարկը, ինչպես նաև Մերձավոր Արևելքի և Հյուսիսային Աֆրիկայի տարածաշրջաններում ԼԳԲՏՔԻ կազմակերպություններին աջակցող նախագիծը:

Դանիելլա Պելեդի մասին

Դանիելլա Պելեդը ՊԽԼԻ-ի գլխավոր խմբագիրն է, որը վերահսկում է խմբագրական ողջ բովանդակությունը և թողարկումը: Արտաքին գործերի լուսաբանման ավելի քան 20 տարվա փորձ ունեցող լրագրողը և խմբագիրը նաև մշակել և իրականացրել է լրագրության դասընթացներ ՊԽԼԻ-ի գործունեության բազմաթիվ շրջաններում, այդ թվում՝ Աֆղանստանում, Իրաքում և Թուրքիայում:

Շնորհակալություն Toro-ին և GNWP-ին:

Կիբերփորձագետներ՝ Սամվել Մարտիրոսյան, Արթուր Պապյան, Դավիթ Ղոնղաձե և Վլադ Մազուրեակ

gnwp Global Network of Women Peacebuilders

Հայաստանի կիբերանվտանգության լանդշաֆտ՝ գենդերային վերլուծություն

Հարավային Կովկասում գտնվող Հայաստանը վերջերս ականատես է եղել զգալի քաղաքական և տնտեսական փոփոխությունների, որոնք նշանավորվել են Լեռնային Ղարաբաղի հակամարտությունների հետևանքներով: Պատերազմի հետևանքները ոչ միայն առաջացրել են քաղաքական և սոցիալ-տնտեսական տեղաշարժեր, այլև հանգեցրել են բնակչության զանգվածային տեղահանումների՝ ստեղծելով նոր մարտահրավերներ ազգի համար: Տարածաշրջանային անկայունության համատեքստում, ներառյալ ուկրաինական պատերազմը, Հայաստանը բախվում է կիբերանվտանգության բարդ լանդշաֆտի և կիբերսպառնալիքների էսկալացիային:

Հայաստանի ոստիկանությունը հայտնել է 2016-2018 թվականներին կիբերհանցագործությունների 20-25 տոկոս աճի միտման մասին՝ ընդգծելով թվային սպառնալիքների զարգացող բնույթը (1):

Հայաստանում քաղաքացիական հասարակության կազմակերպությունները (ՔՀԿ), որոնք կենսական դեր են խաղում ակտիվիզմի և շահերի պաշտպանության գործում, բազմաթիվ կիբերսպառնալիքների թիրախում են:

Կիբերանվտանգության լանդշաֆտ

Ինտերնյուզի 2023 թվականի «Հայաստանի թվային սպառնալիքների լանդշաֆտ. քաղաքացիական հասարակություն և լրատվամիջոցներ» (2) զեկույցում ներկայացված են մի քանի հիմնական ներհայեցումներ:

- **Ֆինանսական տվյալներ և ռեսուրսներ.** կիբերհարձակվողները սովորաբար թիրախավորում են անհատներին իրենց ֆինանսական տվյալների և ռեսուրսների պատճառով՝ օգտագործելով տարբեր մարտավարություններ, ինչպիսիք են անձի կեղծումը և խաբեությունները վաճառքում:
- **Սոցիալական մեդիայի օգտատերեր.** ցանցահենները թիրախավորում են սոցիալական մեդիայի օգտատերերին, օրինակ՝ Telegram և WhatsApp հարթակներում՝ հաճախ դիմելով խարդախությունների:
- **Պետության կողմից հովանավորվող հարձակումներ.** հայերը երբեմն կարող են «ուղեկցող վնաս» հանդիսանալ Հայաստանում Ռուսաստանի քաղաքացիների դեմ ուղղված կիբերհարձակումներում՝ ցույց տալով կիբերսպառնալիքների փոխկապակցված բնույթը:

- **Նամակագրության հավելվածների գրավում.** հաղորդվում է, որ Telegram-ը և WhatsApp-ը թիրախավորված սոցիալական ինժեներիայի միջոցով գրավելու փորձեր են կատարվել, ինչը ցույց է տալիս կիբերհարձակումների լրջությունը:
- **Հարձակումների վերջին ալիքը.** համացանցի հայկական տիրույթում արձանագրված կիբերհարձակումների թվի զգալի աճն ընդգծում է կիբեռանվտանգության հուսալի միջոցներ ձեռնարկելու հրատապությունը (3):
- **Օրենսդրական արձագանք.** Բաց կառավարման գործընկերության (ԲԿԳ) 2022-2024 թվականների գործողությունների փոփոխված ծրագիրն (4) անդրադառնում է կիբերանվտանգության միջադեպերի հայտնաբերման, ծանուցման և կանխարգելման հետ կապված ասպեկտներին՝ նպատակ ունենալով բարելավելու Հայաստանի կիբերանվտանգության ընդհանուր դաշտը:

Քաղաքացիական հասարակություն և կիբերսպառնալիքներ

Հայաստանում ՔՀԿ-ները, որոնք արդեն իսկ պայքարում են քաղաքական փոփոխությունների և տարածաշրջանային պատերազմների պատճառով տեղի ունեցող քաղաքացիական իրավունքների ոտնահարման դեմ, թվային ոլորտում բախվում են մեծ ռիսկերի: ՔՀԿ-ները բախվում են նույն հարձակումներին, ինչ Հայաստանում համացանցի մյուս բոլոր օգտատերերը: Այնուամենայնիվ, նրանց աշխատանքի բնույթը ցույց է տալիս, որ նրանք բախվում են ավելի մեծ ռիսկերի, երբ դառնում են չթիրախավորված հարձակումների զոհ (5):

Ըստ ԶԼՄ բազմազանության ինստիտուտի «Թվային անվտանգության միջադեպերը Հայաստանի քաղաքացիական հասարակության դեմ 2019-2020 թթ.» զեկույցի(6)՝ արձանագրվել են հարձակումների հետևյալ տեսակները.

- **Վեբ կայքերի կոտրում.** ներխուժում վեբ սերվերներ՝ շահագործման, խոցելիության, սխալ կոնֆիգուրացիայի և այլ ուղիների միջոցով:
- **DDoS (ծառայության բաշխված մերժում/Distrib uted Denial of Service) հարձակումներ.** համացանցի տրաֆիկի հոսքի միջոցով թիրախավորված սերվերների ծանրաբեռնում՝ օրինական մուտքը խափանելու նպատակով:
- **Ֆիշինգ.** վստահելի անձ ներկայանալն էլեկտրոնային փոստի կեղծման և ակնթարթային հաղորդագրությունների միջոցով՝ գաղտնի տեղեկատվություն ստանալու նպատակով:
- **Էլեկտրոնային փոստի ցանցահեներ.** ներառում են կոպիտ ուժի հարձակումներ, գաղտնաբառերի արտահոսք կամ գաղտնաբառի վերականգնման փորձեր:
- **Ֆիզիկական հարձակումներ.** կազմակերպությունների գրասենյակներ ներխուժելու փորձեր՝ համակարգիչներ, սերվերներ և թվային սարքավորումներ գողանալու նպատակով:
- **Վնասակար ծրագիր.** ակտիվիստների Android հեռախոսներում առկա լրտեսական ծրագիր է, որը փորձում է թիրախներին վարակել էլեկտրոնային փոստին կցված վիրուսային ֆայլերի միջոցով:
- **Զանգվածային լուսաբանում և ոտնձգություն.** կիբերբուլլինգ, ոտնձգություն և զանգվածային լուսաբանում հասարակական կազմակերպությունների ղեկավարների, լրագրողների և ակտիվիստների սոցիալական մեդիայի էջերի վերաբերյալ:

Հայաստանի քաղաքացիական հասարակությունը քաղաքական մարտահրավերների և արագ փոփոխվող կիբերլանդշաֆտի պայմաններում բախվում է շարունակական զգոնության և թվային անվտանգության ուժեղացված միջոցներ ձեռնարկելու խիստ անհրաժեշտությանը:

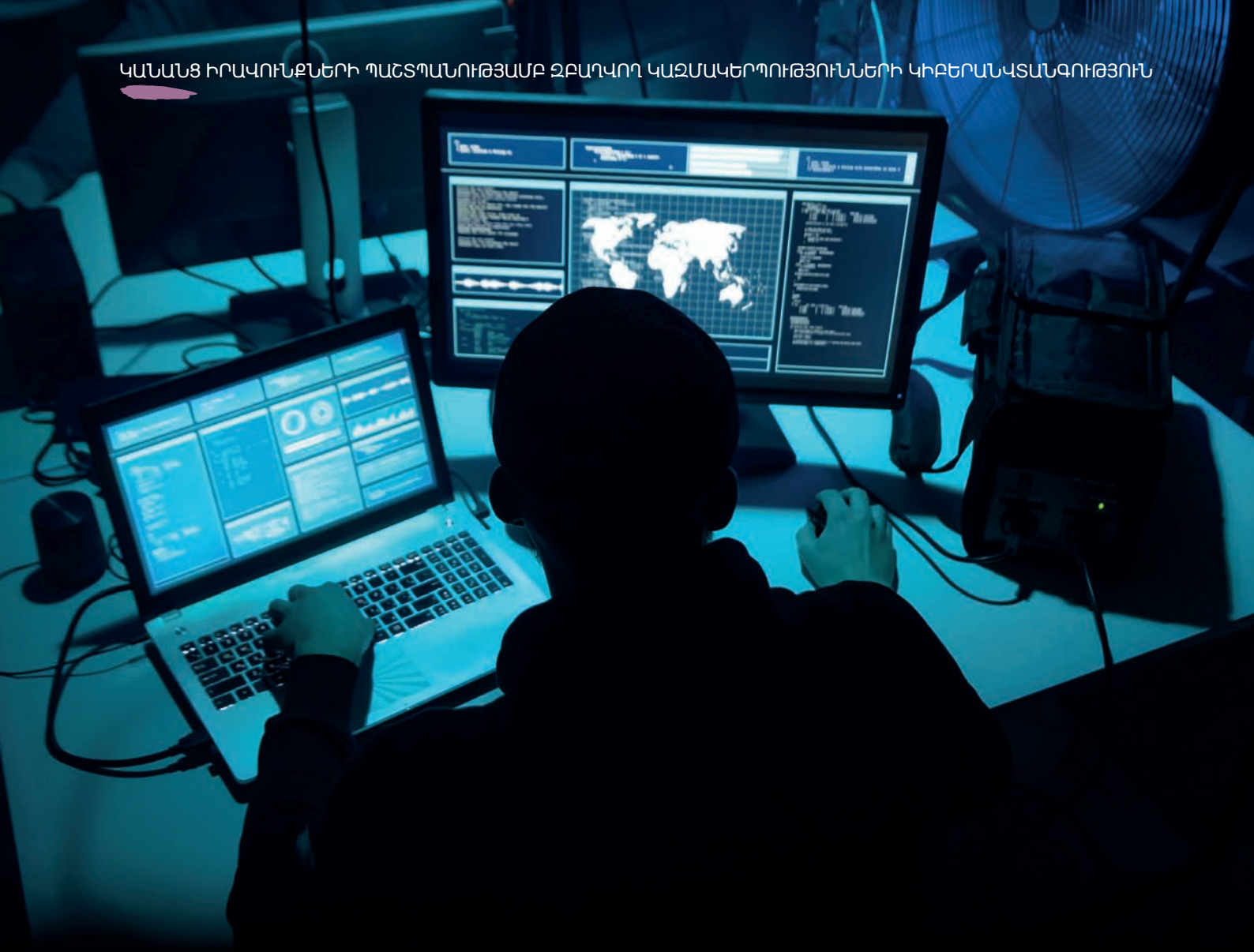
Կիբերսպառնալիքների գենդերային վերլուծություն

Կիբերսպառնալիքները վերածվել են համատարած խնդրի, որն ազդում է մարդկանց վրա ամբողջ աշխարհում: Ցավոք, կանայք հաճախ կրում են այդ սպառնալիքների ծանրությունը՝ բախվելով եզակի մարտահրավերների և դառնալով խոցելի: Ամբողջ աշխարհում կիբերբռնությունը կանանց նկատմամբ հրատապ խնդիր է, որը ներառում է կիբերոտնձգություններ, վրեժխնդիր պոռնոգրաֆիա և բռնի ենթատեքստով առցանց հարձակումներ (7, 8, 9): Այս հարձակումները հաճախ վերածվում են լուրջ սպառնալիքների, ինչի վառ օրինակ են Բոսնիա և Հերցեգովինայում սպանության սպառնալիքներով կին լրագրողներին ուղղված միջադեպերը (10):

2023 թ-ի Գենդերն ու մարդու իրավունքները կիբերանվտանգության ազգային մակարդակի մոտեցումների ԿԽՀՑ ուսումնասիրությունն ընդգծում է գենդերային հիմնահարցեր ներառելու կարևորությունը քաղաքականության մշակման գործում (11): Ըստ այս մոտեցման՝ կանայք և կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունները կարող են բախվել եզակի մարտահրավերների, որոնք պահանջում են համապատասխան վերլուծություններ և առաջարկներ:

Ըստ ԿԽՀՑ զեկույցի՝ կիբերանվտանգության դեմ գենդերային մոտեցում կիրառելու առավելություններն են.

1. Ընդունել, որ կանայք և մարգինալացված խմբերը տարբեր կերպ են օգտագործում համացանցը և ոչ համամասնորեն են տուժում կիբերհարձակումներից: Կիբերանվտանգության քաղաքականության մշակման և տեխնոլոգիաների զարգացման գործում նրանց հատուկ կարիքներն ու ներկայացուցչությունը հաճախ անտեսվում են:
2. Կանանց և այլ մարգինալացված խմբերի համար կիբերանվտանգության դրույթների հասանելիության բարելավումը և նախկինում գոյություն ունեցող խտրական հասարակական կառույցների պատճառով արտակարգ իրավիճակների արձագանքման և իրավական միջոցների սահմանափակումների վերացումը:
3. Կիբերանվտանգության քաղաքականության ոչ զգայուն կետերի վերացումը՝ հաշվի առնելով գենդերային հիմնահարցերը և մարդակենտրոն ու գենդերազգայուն մոտեցումը:



Կանայք Հայաստանում, ինչպես և իրենց համաշխարհային գործընկերները, բախվում են կիբերսպառնալիքների, որոնք բխում են անվտանգության սովորական նկատառումներից: Ազդեցությունը խորն է. այն անդրադառնում է ոչ միայն անձնական անվտանգության վրա, այլև սահմանափակում է խոսքի ազատությունը և նվազեցնում վստահության մակարդակը (12, 13): Safe YOU հավելվածը և այլ միջոցները, որոնց նպատակն է ռեսուրս տրամադրել գենդերային բռնության դեմ պայքարի համար, ցույց են տալիս, թե ինչպես կարելի է տեխնոլոգիան օգտագործել հայ կանանց հզորացնելու նպատակով (14):

Հայաստանի ԼԳԲՏՔ+ համայնքը նույնպես բախվում է համատարած խտրականության՝ ազդելով ՔՀԿ-ների արդյունավետության վրա ողջ երկրում (15):

Կիբերանվտանգության և գենդերային իրավունքների փոխհատումը պահանջում է մշտական ուշադրություն և գործողություններ՝ ամբողջ աշխարհում կանանց համար ավելի անվտանգ թվային տարածք ստեղծելու համար: Կիբեռանվտանգության ոլորտում գենդերային ուղղվածությամբ հետագա հետազոտություններն ու նախաձեռնությունները կարող են առաջարկել ներհայեցումներ հայաստանյան համատեքստում կանանց վրա ունեցած ազդեցության վերաբերյալ:

Քանի որ Հայաստանը ենթարկվում է թվային վերափոխման, քաղաքացիական հասարակությունը, մասնավորապես կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունները, պետք է կողմնորոշվեն կիբերլանդշաֆտի բարդություններում՝ իրենց կարևորագույն աշխատանքի անխոչընդոտ լինելն ապահովելու համար:

Արդյո՞ք ես իսկապես թիրախ եմ

Անշուշտ: Իրականում, բոլորն էլ թիրախ են:

Այստեղ նպատակը խուճապ կամ վախ սերմանելը չէ: Այնուամենայնիվ, չափազանց կարևոր է լինել իրատեսական և հստակ պատկերացում կազմել կիբերսպառնալիքների և հանցավոր գործունեության մասին: Զինվելով այս գիտելիքներով՝ Դուք կկարողանաք հաղթահարել այս մարտահրավերները և պաշտպանել ոչ միայն Ձեզ, այլև Ձեր գործընկերներին, շահառուներին և Ձեր աշխատանքը:

Անկախ նրանից՝ Դուք մարդասեր եք, ակտիվիստ թե Հայաստանում կանանց իրավունքների պաշտպան, Ձեր ուշադրության կենտրոնում ամենայն հավանականությամբ կլինեն փոփոխություններին սատարելը, օրենսդրության մեջ գենդերային հեռանկարների լոբբինգը և Ձեր համայնքներում իրազեկության մակարդակի բարձրացումը:

Կիբերսպառնալիքները կարող են չանհանգստացնել Ձեզ, և, իհարկե, չի ակնկալվում, որ իրավիճակներին արձագանքեք ինչպես կիբերհանցագործ: Սակայն, գենդերային ասպեկտը քաղաքականության և օրենքների մեջ ներառելն այնքան կարևոր է, որքան ներկայիս աշխարհում կիբերիրազեկվածությունը Ձեր բոլոր գործողություններում կիրառելը:

> «Պաշտպանելով Ձեզ, Ձեր գործընկերներին և Ձեր կազմակերպությունը՝ Դուք պաշտպանում եք ոչ միայն տվյալները, այլև ապահովում եք այն դրական ազդեցությունը, որն ունեք և կշարունակեք ունենալ հասարակության վրա»

Ծանոթանանք Լիլիթի և Անահիտի հետ

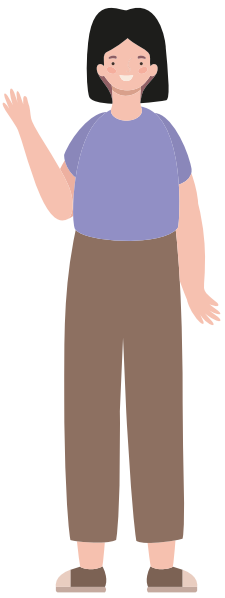
Լիլիթը՝ կանանց իրավունքների նվիրյալ պաշտպանը, իր օրերը նվիրում է դրական փոփոխությունների խթանմանը: Նրա առօրյան ներառում է հանդիպումներ կանանց տեղական կազմակերպությունների հետ, ինչպես նաև գենդերային հավասարության խթանումը և երիտասարդ ակտիվիստների առաջնորդության ռազմավարությունների մշակումը: Նա բազմաթիվ երեկոներ է անցկացնում համայնքի իրազեկման ծրագրերում, որտեղ կիսվում է պատմություններով՝ կանանց ոգեշնչելու համար: Լիլիթի օրը շահերի պաշտպանության, կրթության և ոգեշնչող զրույցների խառնուրդ է:

Անահիտը՝ նվիրյալ խաղաղաշինարարը և համայնքի ղեկավարը, կենտրոնանում է ժողովրդական նախաձեռնությունների վրա: Ակտիվորեն ներգրավված լինելով երկխոսությունն ու փոխըմբռնումը խրախուսելու գործում՝ Անահիտը հաճախ ղեկավարում է համայնքային սեմինարներ և կազմակերպում է խաղաղաշինությանը միտված միջոցառումներ՝ տարածելով միաբանության գաղափարը տարբեր խմբերում: Նրա հանձնառությունը տարածվում է նաև հակամարտությունների կարգավորման շուրջ երեկոյան քննարկումների վրա՝ ներգրավելով համայնքի անդամներին: Նրա սովորական օրը լեցուն է հանդիպումներով, աշխատաժողովներով և համատեղ ջանքերով՝ խաղաղ և ներառական հասարակություն կառուցելու համար:

Լիլիթ

ԿԱՆԱՆՑ ԻՐԱՎՈՒՆՔՆԵՐԻ ՊԱՇՏՊԱՆ

Աշխատանքի պատմություն. Լիլիթը Հայաստանում կանանց իրավունքների պաշտպանության կարկառուն ակտիվիստ է, որը նվիրաբերել է իր կարիերան գենդերային հավասարության և արդարության զարգացման գործին: Նրա աշխատանքն ուղղված է հետպատերազմական տարածաշրջաններում կանանց հզորացնելուն՝ նպաստելով կայուն խաղաղությանը:

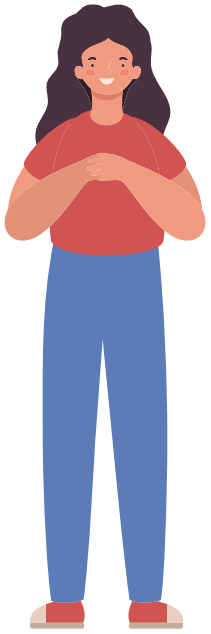


Ապրելակերպ. Լիլիթը խորապես ներգրավված է համայնքի կառուցման նախաձեռնություններում և խաղաղության երկխոսություններում: Ներառականությանն ու սոցիալական արդարությանը նվիրվածության շնորհիվ նա հարգանքի է արժանացել կանանց իրավունքների պաշտպանների շրջանում:

Անահիտ

ԽԱՂԱՂԱՇԻՆԱՐԱՐ և ՀԱՄԱՅՆՔԻ ՂԵԿԱՎԱՐ

Աշխատանքի պատմություն. Անահիտը պատերազմի, բռնության և սոցիալական անհավասարությունների դեմ ուղղված նախաձեռնություններում ակտիվորեն ներգրավված նվիրյալ խաղաղաշինարար է: Նա իր սեփական խաղաղաշինական նախաձեռնության համահիմնադիրն է, որը խթանում է երկխոսություն ու փոխըմբռնում:



Ապրելակերպ. Անահիտը վարում է համայնքային աշխատաժողովներ՝ ընդգծելով խաղաղ գործընթացներում կանանց ներգրավվածության կարևորությունը: Նրա կենտրոնացումը մասսայական ջանքերի վրա ցույց է տալիս, թե ինչպես են փոխհատվում խաղաղաշինությունը և կանանց իրավունքները:

Ինչու՞ թիրախավորել ակտիվիստներին, խաղաղաշինարարներին և համայնքի ղեկավարներին:

Կիբերհանցագործները թիրախավորում են այսպիսի գործառույթ ունեցող անհատներին՝ հասարակության մեջ նրանց ազդեցիկ դիրքերի պատճառով: Վերջիններիս ջանքերը՝ միտված դրական փոփոխություններին, նրանց դարձնում են հավանական սպառնալիք հակառակ շահեր ունեցողների համար: Բացի այդ, նրանց աշխատանքի բնույթը հաճախ ներառում է զգայուն տեղեկատվություն՝ դարձնելով նրանց գրավիչ թիրախներ:

ԿԻԲԵՐՀԱՐՁԱԿՈՒՄՆԵՐԻ ՏԵՍԱԿՆԵՐԸ՝ ՊԱՐԶԵՑՎԱԾ

Չթիրախավորված հարձակում.
- Վիրուսային սպառնալիքի ամենատարածված ձևը:
- Չի մատնանշում կոնկրետ անհատներ կամ կազմակերպություններ:
- Կիբերհանցագործները նպատակ ունեն թիրախավորելու հնարավորինս շատ համակարգիչներ, անհատներ և կազմակերպություններ:
- Վնասակար ծրագրերը, որդերը կամ վիրուսներն էլեկտրոնային հաղորդագրության միջոցով առանց խտրականության ուղարկվում են բազմաթիվ հասցեների:
- Չթիրախավորված կիբերհարձակումներն ավելի հեշտ է իրականացնել, բայց դրանք ավելի քիչ կործանարար են, քան թիրախավորված հարձակումները:

Թիրախավորված հարձակում.
- Ուղղված է անձի կամ կազմակերպության դեմ:
- Կիբերհանցագործները գործում են հատուկ նպատակով՝ առանձնացնելով հետաքրքրող թիրախը:
- Այս հարձակումների իրականացումը տևում է ամիսներ և կարող է ներառել սոցիալական ճարտարագիտություն, ֆիշինգ, մշակված վնասակար ծրագրակազմ, կայուն քարոզարշավներ և բոտնետներ:
- Թիրախները կառավարական մարմիններից և ռազմական բազաներից բացի ներառում են նաև կազմակերպություններ, մեդիա, հաղորդակցություն և կարևոր ենթակառուցվածքներ:

Այս հասկացությունների ըմբռնումը Ձեզ հնարավորություն կտա արդյունավետորեն ղեկավարել թվային տիրույթը:

Դուք հավանաբար կհարցնեք՝ «Ինչո՞ւ պետք է կիբերհանցագործները փորձեն թիրախավորել ինձ»: Հարցը տեղին է, հատկապես նրանց համար, ովքեր նվիրված են մարդասիրական գործին, ակտիվիզմին կամ կանանց իրավունքների պաշտպանությանը: Կիբերհարձակումների դրդապատճառները կարող են տարակուսելի թվալ, բայց դրանք հասկանալը շատ կարևոր է:

ԲԱՑԱՀԱՅՏՎԱԾ ԴՐԴԱՊԱՏՃԱՌՆԵՐԸ. ԻՆՉՈ՞Ւ ԹԻՐԱԽԱՎՈՐԵԼ ՀԵՆՑ ՁԵԶ:

1. Ազդեցություն և խաթարում.
Ձեր կենսական դերը. որպես ակտիվիստ, խաղաղաշինարար կամ համայնքի ղեկավար՝ Ձեր առաքելությունն է ձևավորել հասարակական կարծիք և ազդել քաղաքականության վրա:

Կիբերսպառնալիք. կիբերհանցագործները կարող են իրենց աչքը պահել Ձեզ վրա՝ խաթարելու Ձեր ազդեցիկ աշխատանքը: Թիրախավորելով Ձեզ՝ նրանք նպատակ ունեն ստեղծելու քաոս՝ խարխլելով Ձեր հովանավորած դրական նախաձեռնությունները:

2. Զգայուն տեղեկատվության ձեռքբերում.
Կրիտիկական տվյալների կառավարում. Ձեր ամենօրյա աշխատանքում Դուք հաճախ առնչվում եք սոցիալական խնդիրների հետ կապված զգայուն տեղեկատվության հետ:

Կիբերսպառնալիք. կիբերհանցագործները կարող են ձգտել գողանալ կամ մանիպուլացնել այս տվյալները՝ հանուն իրենց շահերի: Անկախ նրանից՝ դա անձնական շահի, թե հասարակական կարծիքը ղեկավարելու համար է, Ձեր արժեքավոր տեղեկատվությունը դառնում է թիրախ:
Ձեր կիբերանվտանգությունն ամրապնդելու առաջին քայլն այս շարժառիթները հասկանալն է:

«Մեր դերը՝ որպես կիբերանվտանգության փորձագետներ, Ձեզ պաշտպանելն է պատահական զոհ լինելուց (չթիրախավորված հարձակում): Եթե ցանցահենն իրապես թիրախավորում է Ձեզ, նա, ամենայն հավանականությամբ, կգտնի ճանապարհ կամ խոցելի կողմ, և այստեղ մեր գործը դա հնարավորինս հետաձգելն է»:

Վլադ Մազուրեակ՝ կիբերանվտանգության փորձագետ:

Ձեր կարծ ուղեցույցը՝ կիբերհանցագործների տեսակների վերաբերյալ

Հակտիվիստներ
(ԱՅՈ՛, ՆՐԱՆՔ ԻՍԿԱՊԵՍ ԳՈՅՈՒԹՅՈՒՆ ՈՒՆԵՆ):

Դրդապատճառ. քաղաքական կամ սոցիալական պատճառներով պայմանավորված:
Առաքելություն. պաշտպանել իրենց օրակարգը կամ բողոքել նկատելի անարդարությունների դեմ:
Սիրված կիբերհարձակումներ. վեբ կայքերի վնասում, զգայուն տեղեկատվության արտահոսք կամ առցանց գործունեության խափանում:

Ձեր աշխատանքի բնույթն իսկապես կարող է Ձեզ դարձնել հակտիվիստների թիրախ: Եղե՛ք տեղեկացված և զգոն:

Պետության կողմից հովանավորվող դերակատարներ
(ՕՏԱՐԵՐԿՐՅԱ ԿԱՄ ՆԵՐՔԻՆ):

Ներգրավվածություն. կառավարությունների կամ պետության կողմից հովանավորվող անձինք:
Նպատակ. ճնշել այլախոհությունը և վերահսկել ընդդիմության գործունեությունը:
Ռիսկի մակարդակ. առաջադեմ հնարավորությունները մեծ վտանգ են ներկայացնում ինչպես անհատների, այնպես էլ կազմակերպությունների համար:

Ակտիվիստների, խաղաղաշինարարների և համայնքի ղեկավարների դեմ կիբերսպառնալիքների հետևում թաքնված դրդապատճառները հասկանալն առանցքային դեր ունի: Այն Ձեզ հնարավորություն է տալիս ճանաչելու հնարավոր սպառնալիքները և նախաձեռնելու քայլեր՝ կիբերանվտանգության կայուն միջոցառումներ մշակելու համար:

Հանցավոր կազմակերպություններ
(ԱՄԵՆ ԻՆՉ ՓՈՂԻ ՀԱՄԱՐ):

Նպատակ. ընդլայնել իրենց հանցավոր գործունեությունները, ինչ էլ որ դրանք լինեն:
Մեթոդ. գողանալ անձնական տվյալներ՝ շահույթ ստանալու նպատակով վաճառելու համար:

Ուշադիր եղեք, քանի որ Ձեր արժեքավոր տվյալները կարող են շահութաբեր թիրախ դառնալ այս կազմակերպությունների համար:

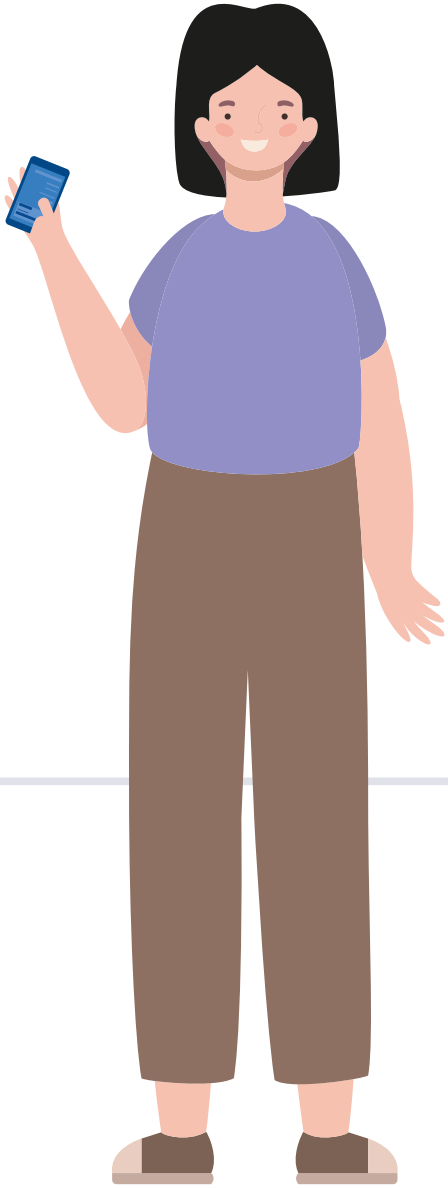
ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏԱՅԱԼԸ.

1 **Համընդհանուր խոցելիություն.** բոլորն էլ կարող են ենթարկվել կիբերհարձակումների: Ձեր մասնագիտական դերը կարող է բարձրացնել այս ռիսկը:
2 **Թիրախավորված հարձակումներն ընդդեմ չթիրախավորվածների.** հիմնական տարբերությունը մտադրությունն է: Թիրախավորված հարձակումներն ուղղված են կոնկրետ անձանց դեմ, մինչդեռ չթիրախավորվածներն ավելի լայն ցանց են ներառում:
3 **Տարբեր կիբերհանցագործությունների դրդապատճառներ.** գոյություն ունեն կիբերհանցագործների տարբեր տեսակներ, որոնցից յուրաքանչյուրն առաջնորդվում է յուրահատուկ օրակարգով և շարժառիթներով:
4 **Ամբողջական պաշտպանություն.** Ձեր կիբերանվտանգությունն առաջնահերթություն դարձնելը պաշտպանում է ոչ միայն Ձեզ, այլև Ձեր գործընկերներին, շահառուներին և կազմակերպությանը:

Հիշեք, որ այս հիմնական ասպեկտները հասկանալը ոչ միայն ամրապնդում է Ձեր անհատական պաշտպանությունը, այլև նպաստում է Ձեր մասնագիտական էկոհամակարգի կոլեկտիվ անվտանգությանը:

«Ճանաչի՛ր թշնամուդ, ճանաչի՛ր ինքդ քեզ և հարյուրավոր ճակատամարտեր առանց աղետի կհաղթես»

Սուն Ցզի



ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Հայտնի ակտիվիստ Լիլիթը ֆիշինգային էլեկտրոնային հաղորդագրություն է ստացել, որում գրողը նշում է, թե ինքն իրավապաշտպան կազմակերպությունից է, որի հետ Լիլիթը համագործակցում է: Էլեկտրոնային հաղորդագրությունը հորդորում էր Լիլիթին բացել հղումը՝ անվտանգության խախտման պատճառով իր հավատարմագրերը թարմացնելու համար:

Ի՞նչ տեսակի կիբերհարձակման զոհ է նա դարձել:

1. Թիրախավորված հարձակում՝ նրա տվյալները գողանալու համար:
2. Չթիրախավորված հարձակում՝ նրա տվյալները գողանալու համար:
3. Թիրախավորված հարձակում հանցավոր կազմակերպության կողմից:
4. Չթիրախավորված հարձակում հանցավոր կազմակերպության կողմից:

Պատասխանները կարող եք գտնել վերջին գլխում՝ Կիբերպատասխաններ

Անվտանգ համացանցային որոնումներ՝ կբայլե՞ք մարդաշատ փողոցով՝ Ձեր պայուսակը բաց

Պատկերացրեք՝ աշխատանքի գնալիս զբոսնում եք Երևանի աշխույժ փողոցներից մեկով: Հավաստիանալը, որ Ձեր պայուսակն ապահով փակված է, փողոցն անցնելուց առաջ երկու կողմը հայացք գցելն ու շրջակայքում ամեն ինչին ուշադիր լինելը Ձեզ համար սովորություն դարձած կլինի: Նույնիսկ թվացյալ ապահով տարածքներում իրազեկվածության պահպանումը, զգուշավորությունը և ռիսկի նվազեցմանն ուղղված ակտիվ միջոցներ ձեռնարկելը դառնում են արմատացած սովորություններ:

Նույն սկզբունքները կիրառվում են առցանց աշխարհում: Համացանցի անվտանգ օգտագործումն արտացոլում է փողոցներով ապահով զբոսանքի սկզբունքները՝ շեշտը դնելով իրազեկվածության, զգուշավորության և ռիսկի նվազեցմանն ուղղված նախածեռնողական քայլերի վրա:

Ինքնակատարելագործվեք՝ թվային ոլորտում ավելի զգոն դառնալու համար: Կիբերհանցագործներն օգտագործում են ավելի ու ավելի բարդ տեխնիկա՝ խաբելու և տվյալներ գողանալու համար: Թեև ի սկզբանե դժվար կարող է լինել, այս գործելակերպերի ընդունումը նման է այն սովորություններին, որոնք Դուք օգտագործում եք փողոցում կողմնորոշվելու կամ Ձեր բնակարանից դուրս գալու ժամանակ. անընդհատ կիրառության միջոցով դրանք դառնում են Ձեր սովորությունը:

Տեսակ	Ապահով զբոսանք փողոցում	Համացանցի ապահով օգտագործում
Զգոնություն և իրազեկվածություն	Ուշադիր եղեք Ձեր շրջակայքին, խուսափեք վատ լուսավորված տարածքներից և զգույշ եղեք անծանոթ մարդկանցից:	Զգուշացեք ֆիշինգային խարդախություններից և կեղծ կայքերից:
Անվտանգության վերիֆիկացում	Ընտրեք անվտանգ ճանապարհներ և ստուգեք շրջակայքի վստահելիությունը՝ ֆիզիկական ապահովության համար:	Ստուգեք վեբ կայքերի իսկությունը՝ նախքան անձնական տեղեկություններ տրամադրելը:
Կանխարգելիչ միջոցառումներ	Կանխարգելիչ միջոցներ կիրառեք, ինչպիսիք են դռները կողպելը, պայուսակը փակելը և թանկարժեք իրերն ապահով տեղում պահելը:	Օգտագործեք անվտանգության գործիքներ, թարմացրեք վեբ զննարկիչները (բրաուզեր) և կիրառեք գաղտնիության խիստ կարգավորումներ:
Հավատարմություն կանոններին և ուղեցույցներին	Ենթարկվեք ճանապարհային երթևեկության կանոններին և հետևեք փողոցում տեղադրված նշաններին և ուղեցույցներին:	Հետևեք կիբերանվտանգության կիրառման լավագույն փորձին և պահպանեք առցանց կանոնները:
Անվտանգության պարբերական ստուգումներ	Պարբերաբար ստուգեք կողպեքները, դռները և շրջակայքը՝ ֆիզիկական անվտանգության համար:	Պարբերաբար թարմացրեք օպերացիոն համակարգերը, վեբ զննարկիչները և անվտանգության ծրագրակազմերը՝ առցանց անվտանգության համար:

Չեր կարծ ուղեցույցը՝ կեղծ կայքերի հայտնաբերման համար

1 **Ստուգեք URL-ը.** ստուգեք կայքի URL-ը՝ տառասխալների, լրացուցիչ նիշերի կամ անսովոր դոմենների առկայությունը պարզելու համար:
- **Օրինական՝** https://www.example.com
- **Ֆիշինգ՝** https://www.exaample.com (ուղղագրական սխալ),
https://www.example.pf (անսովոր դոմեն)

2 **Փնտրեք HTTPS-ը.** հավաստիացեք, որ կայքն օգտագործում է HTTPS-ը HTTP-ի փոխարեն: S-ը մատնանշում է տվյալների փոխանցման համար գաղտնագրված անվտանգ կապը:
- **Օրինական՝** https://www.securewebsite.com
- **Ֆիշինգ՝** http://www.insecurewebsite.com (բացակայում է անվտանգության S-ը)

3 **Ստուգեք վեբ կայքի դիզայնը.** զգույշ եղեք վատ նախագծված կամ բազմաթիվ թռուցիկներով կայքերից:
- **Օրինական.** պրոֆեսիոնալ դասավորություն, հետևողական բրենդինգ:
- **Ֆիշինգ.** աղքատիկ դիզայն, անհամապատասխան լոգոներ, բազմաթիվ թռուցիկներ:

4 **Ստուգեք կոնտակտային տվյալները.** օրինական վեբ կայքերը տրամադրում են հստակ կոնտակտային տվյալներ: Մի վստահեք, եթե ոչ մեկը հասանելի չէ կամ եթե մանրամասները վստահություն չեն ներշնչում:
- **Օրինական.** իրական կոնտակտային էջ՝ վավեր հասցեով, հեռախոսահամարով և էլեկտրոնային փոստով:
- **Ֆիշինգ.** չկան կոնտակտային տվյալներ կամ առկա են կասկածելի մանրամասներ, ինչպես օրինակ՝ ընդհանուր էլեկտրոնային հասցե:

5 **Սահեցրեք հղումների վրայով.** մկնիկը սահեցրեք հղումների վրայով՝ նպատակակետ URL-ի նախադիտման համար: Խուսափեք էլ. փոստի հղումների վրա սեղմելուց, փոխարենն ուղղակիորեն մուտքագրեք URL-ը:
- **Օրինական.** հղման վրայով մկնիկով սահեցնելը ցույց է տալիս ցուցադրվող տեքստին համապատասխանող նախադիտում:
- **Ֆիշինգ.** մկնիկը սահեցնելով բացահայտվում է այլ նպատակակետ URL, օրինակ՝ http://www.trustworthy.com (ցուցադրվում է), բայց տանում է դեպի http://www.phishingsite.com:

Կեղծ կայքերի բացատրություն՝ պարզեցված

Ի՞նչ են դրանք. կեղծ կայքերն առցանց անօրինական հարթակներ են, որոնք նախատեսված են այցելուներին խաբելու համար, որպեսզի վերջիններս տրամադրեն անձնական կամ ֆինանսական տեղեկատվություն:
Ինչպե՞ս. ստեղծելով կայքեր, որոնք նմանակում են արժանահավատ անձանց՝ նպատակ ունենալով խարդախորեն ստիպել օգտատերերին բացահայտել զգայուն տվյալներ:
Ո՞րտեղ. բանկեր, էլեկտրոնային առևտրի խանութներ, ծանոթությունների կայքեր և այլն:

Ձեր կարճ ուղեցույցը՝ ֆիշինգ խարդախությունները հայտնաբերելու համար

1 **Կանոնավոր կերպով ստուգեք Ձեր օգտհաշիվները.** ֆիշինգ հանդիսացող էլ. հաղորդագրությունը կարող է կասկածելի գործողություններ իրականացնել Ձեր օգտահաշվի վրա՝ հորդորելով բացել հղումը՝ խնդիրը լուծելու համար:
Օրինակ՝ «Շտապ. Ձեր օգտահաշիվը վտանգված է: Սեղմեք այստեղ՝ վերիֆիկացնելու համար»:

2 **Էլեկտրոնային հաղորդագրություններ, որոնք պահանջում են հրատապ գործողություններ.** ֆիշերները հրատապության զգացում են առաջացնում:
Օրինակ՝ «Ձեր հաշիվը կկասեցվի, քանի դեռ չեք հաստատել Ձեր տվյալները 24 ժամվա ընթացքում: Սեղմեք հիմա՝ խափանումներից խուսափելու համար»:
Օրինակ՝ «Գործի անցեք՝ Ձեր պարգևը ստանալու համար, քանի դեռ ժամկետը չի լրացել»:

3 **Վատ քերականությամբ և ոչ պրոֆեսիոնալ ուղղագրությամբ նամակներ.** օրինական կազմակերպությունները պահպանում են պրոֆեսիոնալ հաղորդակցությունը:
Օրինակ՝ «Հարգելի օգտատեր, Ձեր օգտահաշիվը խափենվել է: Խնդրում ենք թարմացնել Ձեր գաղտնաբառն անվտանգությանն համար»:
Օրինակ՝ «Սեղմեք այստեղ Ձեր բացառիկ մրցանակն ստանալու համար»-ի փոխարեն՝ «Սեղմեք այստեղ Ձեր բացառիկ մրցանակն ստանալու համար»:

4 **Հանրային էլեկտրոնային փոստի դոմենի օգտագործում.** ֆիշինգ հանդիսացող էլեկտրոնային հաղորդագրությունները կարող են օգտագործել էլեկտրոնային փոստի ընդհանուր դոմեններ:
Օրինակ՝ «service@gmail.com»՝ «service@legitimatecompany.com»-ի փոխարեն:

5 **Ստուգեք էլեկտրոնային փոստի հասցեն.** կիբերհանցագործները նմանակում են օրինական էլեկտրոնային փոստի հասցեները:
Օրինակ՝ «support@paypa1.com»՝ «support@paypal.com»-ի փոխարեն:

6 **Ընդհանուր թեմայի տող.** ֆիշինգ էլեկտրոնային հաղորդագրությունները հաճախ անորոշ թեմաներ ունեն:
Օրինակ՝ «Կարևոր տեղեկատվություն»՝ առանց հաղորդագրության բնույթը նշելու:

Ֆիշինգ խարդախություններ՝ պարզեցված

Ի՞նչ է դա: Ֆիշինգ խարդախությունները կեղծարար փորձեր են՝ խաբեության միջոցով անհատներին ստիպելու, որպեսզի բացահայտեն այնպիսի զգայուն տեղեկատվություն, ինչպիսիք են օգտանունները, գաղտնաբառերը կամ ֆինանսական մանրամասները, որոնք այնուհետև կարող են օգտագործվել նենգ նպատակներով:
Ինչպե՞ս: էլեկտրոնային հաղորդագրություններում, նամակագրություններում կամ հաղորդակցության այլ ձևերում ներկայանալով որպես արժանահավատ սուբյեկտներ:
Որտե՞ղ: էլեկտրոնային հաղորդագրություններ, սոցիալական ցանցեր, WhatsApp-ի նամակագրություն և այլն:

Իրական կյանքում ֆիշինգ հանդիսացող էլեկտրոնային հաղորդագրությունների ամենատարածված թեմաներն են.

Google. Դուք հիշատակվել եք փաստաթղթում.
«Ռազմավարական ծրագրի նախագիծ».
HR. Կարևոր է. դրես կոդի փոփոխություններ
HR. Արձակուրդային քաղաքականության թարմացում
Adobe Sign. Ձեր կատարողականի վերանայում
Շտապ անհրաժեշտ է իրականացնել գաղտնաբառի ստուգում
Ընդունեք Ձեր գնահատականը

Ֆիշինգն ավելի ու ավելի տարածված է դառնում կիբերհանցագործների շրջանում.

Աշխարհում ուղարկված բոլոր էլեկտրոնային հաղորդագրությունների մոտավորապես **1,2** տոկոսը ֆիշինգի փորձեր են:
Աշխարհում կազմակերպությունների **81** տոկոսը նկատել է էլեկտրոնային հաղորդագրությունների միջոցով ֆիշինգի հարձակումների աճ:
Ֆիշինգի խարդախությունները կազմում են տվյալների բոլոր հոսքերի գրեթե **36** տոկոսը, ինչպես նշված է Verizon-ի 2022 թվականի տվյալների հոսքերի մասին զեկույցում:

Կեղծ վեբ կայքերն ընդդեմ ֆիշինգ խարդախությունների. նման, բայց տարբեր

Կեղծ վեբ կայքերն անօրինական առցանց հարթակներ են, որոնք նախատեսված են այցելուներից խաբեության միջոցով անձնական կամ ֆինանսական տեղեկատվություն ստանալու համար՝ հաճախ արժանահավատ անձանց նմանակելով:

Մյուս կողմից՝ ֆիշինգ խարդախությունները ներառում են նենգ գործողություններ, ինչպիսիք են ապակողմնորոշիչ էլեկտրոնային հաղորդագրությունը կամ հաղորդակցությունը, որտեղ գրոհողները ներկայանում են որպես հեղինակավոր աղբյուրներ, որպեսզի խաբեությամբ անհատներին ստիպեն բացահայտել զգայուն տեղեկատվություն:

Համացանցի ապահով օգտագործումը նման է բանուկ փողոցներով ապահով քայլելուն: Զգոնության, իրազեկվածության և ռիսկերի դեմ կանխարգելիչ միջոցառումների սկզբունքները, որոնք արմատացած են մեր ամենօրյա ֆիզիկական ապահովության սովորույթներում, իրենց արձագանքն են գտնում թվային աշխարհում:

ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏԱՅԱԼՆԵՐԸ.

1. Ինչպես ֆիզիկական սովորությունները, այնպես էլ թվային պրակտիկաները կիրառման արդյունքում դառնում են սովորական:
2. Զգուշացեք ֆիշինգ խարդախություններից և խարդախությամբ զբաղվող կայքերից:
3. Ստուգեք կայքերի անվտանգությունը նախքան անձնական տվյալներով կիսվելը:
4. Օգտագործեք անվտանգության գործիքներ, թարմացրեք վեբ զննարկիչները և կիրառեք գաղտնիության խիստ կարգավորումներ:
5. Կանոնավոր կերպով թարմացրեք օպերացիոն համակարգերը, վեբ զննարկիչները և անվտանգության ծրագրերը:

> Այժմ առցանց աշխարհն ավելի ապահով է Ձեզ և Ձեր շրջապատի բոլոր մարդկանց համար

ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Հետևյալ էլեկտրոնային հաղորդագրությունների թեմաներից որո՞նք են սովորաբար կապված լինում ֆիշինգ հանդիսացող էլեկտրոնային հաղորդագրությունների հետ: (Ընտրեք բոլոր հնարավոր տարբերակները)

1. Ձեր հաշիվը վտանգված է: Վերիֆիկացրեք հենց հիմա:
2. Շտապ. անհապաղ անհրաժեշտ է աշխատավարձի ցուցակի թարմացում:
3. Նորությունների բաժանորդագրության հաստատում:
4. Անվճար նվեր: Սեղմեք՝ մրցանակը վերցնելու համար:
5. Կարևոր. վերանայեք և հաստատեք փաստաթուղթը:
6. Անվտանգության ծանուցում: Անհայտ մուտքի ակտիվության
   հայտնաբերում:
7. Շնորհավորում ենք, Դուք շահել եք վիճակախաղը:

Պատասխանները կարող եք գտնել վերջին գլխում՝ Կիբերպատասխաններ

Հանրային Wi-Fi՝ դրախտ կիբերհանցագործների համար

Խորհուրդ մասնագետից. Եթե պատրաստ չեք ի լուր աշխարհի հայտնել այդ տեղեկատվությունը, ապա մի կիսվեք դրանով հանրային Wi-Fi ցանցի միջոցով:

Անահիտն իր ամենամտերիմ ընկերուհու՝ Լիլիթի հետ վայելում է հիանալի ընթրիք իրենց սիրելի ռեստորանում՝ երկար ժամանակ իրար չտեսնելուց հետո: Նրանք աշխույժ զրուցում են՝ մտերմիկ կատակներով և պատմում իրենց ամառային արկածների մասին: Ապա զրույցին հաջորդում է աշխատանքի քննարկումը, քանի որ նրանք մտադիր են աշխատել ընդհանուր նախագծի վրա:

Զրույցի ընթացքում Անահիտն ու Լիլիթը անձնական տվյալներ են փոխանակում իրենց հիմնած ապաստարանի գտնվելու վայրի մասին, որտեղ ապաստան են տրամադրում գենդերային բռնության ենթարկված կանանց: Նրանք քննարկում են՝ ինչպես օգնել ապաստարանի բնակիչներին՝ ծրագրեր կազմելով հաջորդ օրվա այցելության վերաբերյալ:

Հիմա պատկերացրե՛ք, որ այս ամբողջ զրույցը հայտնի է դառնում հանրությանը. ռեստորանում գտնվողները լսում են նրանց:

Թեև սա կարող է չափազանցություն թվալ, բայց այն ներկայացնում է հանրային Wi-Fi ցանցերի խոցելիությունը: Ցանցի յուրաքանչյուր օգտատեր ձեռք է բերում փոխանցված տվյալների անսահմանափակ հասանելիություն:

Wi-Fi թեժ կետին միանալը հնարավորություն է տալիս ցանցի տիրոջը վերահսկել առցանց գործունեությունը, որոշ դեպքերում նույնիսկ հետևել ֆիզիկական տեղաշարժին:

Հաշվի առեք սրճարանում աշխատելու, աշխատանքային համակարգչով գաղտնի ինֆորմացիա փոխանցելու, էլեկտրոնային հասցեներով փոխանակվելու կամ էլ գաղտնի տվյալներով կիսվելու հետևանքները: Այս բոլոր տվյալները հանրային Wi-Fi ցանցում դառնում են տեսանելի և հասանելի՝ այն վերածելով ցանցահենների պոտենցիալ խաղահրապարակի:

CHRIS LIVERANI | UNSPLASH

Որոշ զգայուն տեղեկատվություն ուսումնասիրելու կամ գաղտնաբառով պաշտպանված հաշիվներ մուտք գործելու անհրաժեշտության համար կան մի քանի անվտանգ մեթոդներ.

1. Ստեղծեք և օգտագործեք թեժ կետ

Զգայուն տեղեկատվությանը տիրապետելիս կամ գաղտնաբառով պաշտպանված հաշիվներ մուտք գործելիս՝ անձնական թեժ կետի ստեղծումը կարող է ուժեղացնել անվտանգությունը: Հետևեք այս քայլերին.

ա. Ակտիվացրեք թեժ կետը

- Մտեք հեռախոսի կարգավորումներ բաժինը:
- Գտեք «Hotspot» կամ «Tethering» բաժինը:
- Միացրեք թեժ կետը և ստեղծեք հուսալի գաղտնաբառ:

բ. Միացրեք սարքերը

- Միացրեք Ձեր համակարգիչը կամ այլ սարքեր թեժ կետին:
- Հավաստիացեք, որ թեժ կետը պաշտպանված է գաղտնաբառով՝ հավելյալ անվտանգության համար:

գ. Մուտք գործեք անձնական տվյալների բաժին

- Միանալուց հետո ապահով ուսումնասիրեք զգայուն տվյալները կամ մուտք գործեք գաղտնաբառով պաշտպանված հաշիվներ:

Ուշադրություն. սրանք ընդհանուր ուղեցույցներ են և կարող են տարբերվել՝ կախված Ձեր սարքից և օպերացիոն համակարգից:

2. Օգտագործեք ՎՄՑ (Վիրտուալ մասնավոր ցանց)

ՎՄՑ-ի (VPN) կիրառումն առցանց գործունեությունն ապահովելու արդյունավետ միջոց է, հատկապես հանրային Wi-Fi-ից օգտվելիս: Ահա կարճ ուղեցույց Windows-ի և Mac-ի համար:

ա. Ընտրեք ՎՄՑ մատակարար

- Ընտրեք հայտնի ՎՄՑ ծառայություն և բացեք օգտահաշիվ:

բ. Ներբեռնեք և տեղադրեք

- Ներբեռնեք ՎՄՑ-հաճախորդը Ձեր օպերացիոն համակարգի համար:
- Տեղադրեք ծրագրակազմը՝ հետևելով տրված հրահանգներին:

գ. Միացեք սերվերին

- Գործարկեք ՎՄՑ հավելվածը:
- Ընտրեք սերվերի գտնվելու վայրը և անվտանգ կապ հաստատեք:

դ. Զգայուն տվյալների հասանելիություն ձեռք բերեք

- Միացված ՎՄՑ-ով անվտանգ մուտքագրեք զգայուն տվյալներ հանրային ցանցերում:

Ուշադրություն. սրանք ընդհանուր ուղեցույցներ են և կարող են տարբերվել՝ կախված Ձեր սարքից և օպերացիոն համակարգից:

3. Սպասեք, մինչև կարողանաք օգտվել վստահելի մասնավոր Wi-Fi ցանցից

Բարձր զգայունության տվյալների հետ գործ ունենալիս՝ ամենաանվտանգ տարբերակը վստահելի մասնավոր Wi-Fi ցանցից օգտվելն է: Ընդհանրապես հանրային ցանցերից խուսափելը վերացնում է դրանց հետ կապված ռիսկերը:

Հիշեք, որ Ձեր տվյալների անվտանգությունը հույժ կարևոր է, և ճիշտ մեթոդի ընտրությունը կախված է գաղտնիության և հրատապության մակարդակից:

Ի՞ՆՉ Է ՎՄՑ-Ն

ՎՄՑ-ն կամ վիրտուալ մասնավոր ցանցը Ձեր անտեսանելի թվային թիկնոցն է: ՎՄՑ-ի հետ Ձեր տվյալները ձեռք են բերում գաղտնաբառով պաշտպանված քողարկում՝ դառնալով նույնքան անվտանգ, որքան կարևոր առաքելություն կատարող գաղտնի գործակալը:

ՈՒՇԱԴՐՈՒԹՈՒՆ

ՎՄՑ ՄԱՏՉԱԿԱՐԱՐ ԸՆՏՐԵԼԻՍ ԿԱՐԵՎՈՐ Է ՀԱՇՎԻ ԱՌՆԵԼ՝

Անվտանգության և գաղտնիության առանձնահատկությունները. հավաստիացեք, որ ՎՄՑ-ն ունի հուսալի գաղտնագրում, չի հավաքագրում տվյալները և ապահովում է հավելյալ անվտանգություն՝ Ձեր տվյալները պաշտպանելու համար:

Սերվերային ցանց և տեղակայումներ. բազմազան և տարածված սերվերային ցանցը բարելավում է Ձեր առցանց գործունեությունը: Ընտրեք ամբողջ աշխարհում ռազմավարականորեն տեղակայված սերվերներով ՎՄՑ:

Միացման արագություն. ընտրեք ՎՄՑ, որն ապահովում է կապի բարձր և հուսալի արագություն, որը կարևոր է անխափան հսկողության և հեռարձակման համար:

Առանձնահատկություններ և ֆունկցիոնալություն. գնահատեք ՎՄՑ-ի կողմից առաջարկվող լրացուցիչ հնարավորությունները, ինչպիսիք են վթարային անջատիչները, պառակտված թունելավորումը և ընդհանուր ֆունկցիոնալությունը:

Գին. թեև անվճար ՎՄՑ-ն գայթակղիչ է թվում, բայց վճարովի ծառայությունները հաճախ ապահովում են ավելի լավ անվտանգություն և ֆունկցիոնալություն: Ընտրեք ՎՄՑ, որը հարմար է Ձեր բյուջեին և որի որակը համապատասխանում է գնին:

ՈՒՇԱԴՐՈՒԹՈՒՆ

Չնայած հարմարությանը՝ հանրային Wi-Fi-ը շատ ռիսկեր է պարունակում

Կիբերհանցագործները կարող են հափշտակել Ձեր սարքի և Wi-Fi ռոուտերի միջև եղած տվյալները՝ հավաքելով պոտենցիալ զգայուն տեղեկատվություն:

Գաղտնագրության բացակայությունը նշանակում է, որ հանրային Wi-Fi-ով փոխանցվող տվյալներն ավելի խոցելի են գաղտնալսման համար:

Կիբերհարձակվողները կարող են ստեղծել շփոթեցնող անուններով Wi-Fi թեժ կետեր՝ գրավելով օգտատերերին դեպի վիրուսային ցանցեր:

Ցանցահենները կարող են օգտագործել ցանցի վերահսկման գործիքներ՝ տվյալների փաթեթները ձեռք բերելու և վերլուծելու համար՝ ստանալով գաղտնի տվյալներ:

ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏԱՔՐՔԻՐ.

1. Հանրային Wi-Fi ցանցերից օգտվելու հետևանքով օգտատերերը ենթարկվում են հավանական կիբերհարձակումների, քանի որ ցանցի յուրաքանչյուր օգտատեր ձեռք է բերում փոխանցված տվյալների անսահմանափակ հասանելիություն:
2. Բարձր գաղտնիության տվյալների հետ գործ ունենալիս՝ ամենաանվտանգ տարբերակը վստահելի մասնավոր Wi-Fi ցանցից օգտվելն է:
3. Հաշվի առեք, որ պետք է կարգավորեք և օգտագործեք թեժ կետը կամ ՎՄՑ-ն:
4. Անվտանգության ճիշտ մեթոդի ընտրությունը կախված է գաղտնիության և հրատապության մակարդակից:

ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Հարց 1. Ի՞նչ հավանական ռիսկեր ունի հանրային Wi-Fi ցանցը:
ա. Ինֆորմացիայի սահմանափակ հասանելիություն
բ. Բարելավված անվտանգություն
գ. Բաց լինելը կիբերհարձակվողների համար
դ. Օգտատերերի ֆիզիկական տեղաշարժի հետևում

Հարց 2. Ինչպե՞ս է ՎՄՑ-ն բարելավում հանրային Wi-Fi-ի անվտանգությունը:
ա. Ցուցադրելով գաղտնի տվյալները
բ. Սահմանափակելով առցանց գործունեությունը
գ. Ստեղծելով անվտանգ կապ
դ. Խուսափելով հանրային ցանցերից

Պատասխանները կարող եք գտնել վերջին գլխում՝ Կիբերպատասխաններ

Ի՞նչ ընդհանրություն կա Ձեր տան բանալիների և գաղտնաբառերի միջև

«Գաղտնաբառերը նման են ներքնազգեստի. ցույց մի՛ տվեք մարդկանց, հաճախ փոխե՛ք և մի՛ փոխանցեք անծանոթներին»:

- ՔՐԻՍ ՊԻՐԻԼՈ

Խորհուրդ մասնագետից. Խուսափեք օգտագործել միևույն գաղտնաբառը մի քանի օգտահաշիվների համար:

Մի օր՝ կեսօրին, երբ Լիլիթը քայլում էր Երևանի աշխույժ փողոցներով, հայտնվում է անսպասելի իրավիճակում. նա հասկանում է, որ կորցրել է բանալիները: Խուճապի է մատնվում, քանի որ վախենում է, որ իր ֆիզիկական անվտանգությունը կարող է վտանգվել: Լիլիթն այժմ իրեն ապահով չի զգում իր տանը քնելիս, քանի որ իր տունը գողության վտանգի տակ է: Լիլիթն արագ հետ է գնում եկած ճանապարհով և փնտրում բանալիները փողոցներում, սակայն չի գտնում: Այսպիսով, հասկանալով իրավիճակի վտանգավորությունը՝ Լիլիթն անմիջապես զանգահարում է ոստիկանություն, հայտնում կորած բանալիների մասին, կանչում է փականագործին, որպեսզի փոխի կողպեքը և խնդրում է բանալիների մի քանի օրինակ՝ մեկը տալով վստահելի անձի:

Այժմ մտորեք հետևյալի մասին. այնպես, ինչպես Լիլիթի բանալիները բացում են նրա տան դուռը, այդպես էլ գաղտնաբառերը հանդիսանում են թվային արժեքավոր իրերի՝ բանկային հաշիվների, էլեկտրոնային հաղորդագրությունների, հաղորդակցության, անձնական տեղեկատվության, աշխատանքային տվյալների, շահառուների, անձնական հաղորդակցության և այլնի բանալիներ:

Գաղտնաբառ կոտրելու համար պահանջվող ժամանակ	
7 ՆԻՇ	.29 միլիվայրկյան
8 ՆԻՇ	1 - 5 ժամ
9 ՆԻՇ	11 ժամ - 5 օր
10 ՆԻՇ	3 - 4 ամիս
11 ՆԻՇ	1 տասնամյակ
12 ՆԻՇ	2 դար

Աղբյուր 17. https://www.verveit.com/blog/is-your-password-strong-enough/

Ուժեղ և անվտանգ գաղտնաբառեր ստեղծելու Ձեր կարճ ուղեցույցը

Խուսափեք պարզ գաղտնաբառերից.

Խուսափեք հեշտ գուշակվող գաղտնաբառերից, ինչպիսիք են «password123» կամ պարզ բառերը: Անվտանգությունը բարձրացնելու համար ընտրեք չկրկնվող համակցություններ:

Լավ օրինակ. Tr3ndyP@ssw0rd! (բարդ և չկրկնվող)
Վատ օրինակ. Password123 (պարզ և հաճախ օգտագործվող)

Օգտագործեք տարբեր նիշեր.

Օգտագործեք մեծատառերի և փոքրատառերի, թվերի և հատուկ նիշերի համադրություն՝ գաղտնաբառը բարդացնելու համար:

Լավ օրինակ. F!reDraGon87# (Ներառում է տարբեր տեսակի նիշեր)
Վատ օրինակ. password1234 (Բազմազան և բարդ չէ)

Երկարությունը կարևոր է.

Ստեղծեք երկար գաղտնաբառեր, քանի որ դրանք հիմնականում առավել անվտանգ են: Փորձեք օգտագործել նվազագույնը 12 նիշ:

Լավ օրինակ. S3cur3L0ngP@ssw0rd! (երկար է և բարդ)
Վատ օրինակ. ShortPwd! (չափազանց կարճ է ուժեղ անվտանգություն ապահովելու համար)

Տարբերվող գաղտնաբառ յուրաքանչյուր օգտահաշվի համար.

Խուսափեք օգտագործել միևնույն գաղտնաբառը մի քանի օգտահաշիվների համար: Տարբեր հարթակներում չկրկնվող գաղտնաբառերը բարելավում են ընդհանուր անվտանգությունը:

Խուսափեք անձնական տեղեկություն տրամադրելուց.

Մի՛ տրամադրեք անձնական տվյալներ, ինչպիսիք են անունը, ծննդյան օրը կամ հասցեն: Այս տեղեկատվությունը հեշտությամբ հասանելի է և կարող է շահագործվել հարձակվողների կողմից:

Լավ օրինակ. B3l0v3dPet#R0v3r (ներառում է անձնական տվյալներ, բայց ոչ բացահայտ կերպով)
Վատ օրինակ. JohnsDog123 (ուղղակիորեն կապված է անձնական տվյալների հետ)

Կանոնավոր կերպով թարմացրեք գաղտնաբառերը.

Պարբերաբար փոխեք գաղտնաբառերը վտանգի ռիսկը նվազեցնելու համար: Հիշեցումներ միացրեք դրանք մի քանի ամիսը մեկ թարմացնելու համար:

Միացրեք 2ԳՆ (երկգործոն նույնականացում) կամ ԲՄ (բազմակի նույնականացում).

Երկգործոն նույնականացումը (2ԳՆ) ապահովում է լրացուցիչ անվտանգություն և բացի գաղտնաբառերից օգտատերերից նաև պահանջում է տրամադրել նույնականացման երկրորդ ձև, օրինակ՝ ժամանակավոր կոդ, որն ուղարկվում է իրենց բջջային հեռախոսին: Սա զգալիորեն նվազեցնում է անօրինական մուտքի ռիսկը, նույնիսկ եթե գաղտնաբառերը վտանգված են:

Օգտագործեք գաղտնաբառերի կառավարիչ.

Եթե ունեք բազմաթիվ օգտահաշիվներ և պետք է հետևեք Ձեր բոլոր գաղտնաբառերին, օգտագործեք գաղտնաբառերի կառավարիչ: Ընտրեք վստահելի գաղտնաբառերի կառավարիչ. ահա կիբերփորձագետների կողմից առաջարկվող ամենաանվտանգ գաղտնաբառերի կառավարիչներից մի քանիսը:

1Password. Հայտնի է իր առանձնահատուկ և ինտուիտիվ դիզայնով:

Փորձագետի խորհուրդ. համարվում է գաղտնաբառերի լավագույն կառավարիչը, որն առաջարկում է հավասար հնարավորություններ, ինտուիտիվություն և մատչելիություն:

Bitwarden. Բաց կոդով գաղտնաբառերի կառավարիչ՝ անվտանգության վրա մեծ շեշտադրումով:

Փորձագետի խորհուրդ. հայտնի է իր անվտանգության միջոցներով և տարբեր հարթակներում տեղակայվելու ունակությամբ:

NordPass. Մշակվել է NordVPN-ի ստեղծողների կողմից, որն առաջարկում է կայուն անվտանգության առանձնահատկություններ:

Փորձագետի խորհուրդ. համարվում է 2024 թվականի գաղտնաբառերի կառավարման լավագույն ընտրություններից մեկը:

ԳԱՂՏՆԱԲԱՌ ԹԵ՞ ԱՆՑԱԲԱՌ

Գաղտնաբառը սովորաբար նիշերի համակցություն է, ներառյալ տառեր, թվեր և նշաններ, որոնք օգտագործվում են օգտատիրոջ ինքնությունը հաստատելու համար: Այն սովորաբար ավելի կարճ և ավելի բարդ է:

Մյուս կողմից, անցաբառը բառերի ավելի երկար հաջորդականություն է կամ նախադասություն: Այն հիշելն ավելի հեշտ է՝ չնայած երկարությանը:

Ո՞րն է ավելի անվտանգ: Գաղտնաբառի կամ անցաբառի անվտանգությունը կախված է տարբեր գործոններից, ներառյալ երկարությունը և բարդությունը: Ընդհանուր առմամբ, առավել անվտանգ են ավելի երկար և բարդ գաղտնաբառերը կամ անցաբառերը: Անցաբառերը հաճախ ավելի լավ անվտանգություն են ապահովում՝ շնորհիվ իրենց երկարության և առօրյա խոսքի տարրերի օգտագործման:

Նիշերի քանակ	Միայն թվեր	Փոքրատառեր	Մեծատառեր և փոքրատառեր	Թվեր, փոքրատառեր, մեծատառեր	Թվեր, մեծատառեր, փոքրատառեր, նշաններ
4	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես
5	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես
6	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես	վայրկենապես
7	վայրկենապես	վայրկենապես	1 վրկ	2 վրկ	4 վրկ
8	վայրկենապես	վայրկենապես	28 վրկ	2 րոպե	5 րոպե
9	վայրկենապես	3 վրկ	24 րոպե	2 ժամ	6 ժամ
10	վայրկենապես	1 րոպե	21 ժամ	5 օր	2 շաբաթ
11	վայրկենապես	32 րոպե	1 ամիս	10 ամիս	3 տարի
12	1 վրկ	14 ժամ	6 տարի	53 տարի	226 տարի
13	5 վրկ	2 շաբաթ	332 տարի	3 հզր տարի	15 հզր տարի
14	52 վրկ	1 տարի	17 հզր տարի	202 հզր տարի	1 մլն տարի
15	9 րոպե	27 տարի	898 հզր տարի	12 մլն տարի	77 մլն տարի
16	1 ժամ	713 տարի	46 մլն տարի	779 մլն տարի	5 մլրդ տարի
17	14 ժամ	18 հզր տարի	2 մլրդ տարի	48 մլրդ տարի	380 մլրդ տարի
18	6 օր	481 հզր տարի	126 մլրդ տարի	2 տրլն տարի	26 տրլն տարի

Աղբյուր 18. https://tech.co/password-managers/how-long-hacker-crack-password

ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏևՅԱԼԸ.

1. Ե՛վ տան բանալիները, և՛ գաղտնաբառերը կարևոր են անվտանգության համար, ընդ որում անօրինական մուտքերը ռիսկ են հանդիսանում ֆիզիկական և թվային անվտանգության համար:
2. Օգտագործեք հուսալի գաղտնաբառեր կամ անցաբառեր՝ Ձեր օգտահաշիվները պաշտպանելու համար: Անվտանգությունը բարձրացնելու համար օգտագործեք եզակի համակցություններ, տարատեսակ նիշեր և ավելի երկար գաղտնաբառեր (առնվազն 12 նիշ):
3. Կիրառեք լրացուցիչ անվտանգության միջոցներ, ինչպիսին է երկգործոն նույնականացումը (2ԳՆ) գաղտնաբառերից զատ պաշտպանության լրացուցիչ շերտ ավելացնելու համար:

ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Իրավիճակ.
Անահիտը մտահոգիչ ծանուցում է ստանում տվյալների արտահոսքի արդյունքում անձնական տեղեկատվության անօրինական հասանելիության վերաբերյալ: Խուճապի մատնված՝ նա գիտակցում է անհապաղ քայլեր ձեռնարկելու անհրաժեշտությունը՝ իրավիճակը շտկելու և գաղտնի տվյալները պաշտպանելու համար:

Թեստային հարց.
Ի՞նչ քայլեր պետք է ձեռնարկի Անահիտը տվյալների արտահոսքի արդյունքում անօրինական հասանելիության մասին ծանուցումը ստանալուց հետո:
Ա. Անտեսի ծանուցումը. դա կարող է կեղծ ահազանգ լինել:
Բ. Կապ հաստատի ներգրավված ընկերության հետ և բացատրություն պահանջի:
Գ. Փոխի վտանգված օգտահաշվի գաղտնաբառերը և միացնի երկգործոն նույնականացում:
Դ. Կիսվի ծանուցմամբ սոցիալական ցանցերում՝ մյուսներին հնարավոր ռիսկերի մասին զգուշացնելու համար:

Պատասխանները կարելի է գտնել վերջին գլխում՝ Կիբերպատասխաններ

Վնասակար ծրագիր՝ վիրուս, որը թուլացնում է Ձեր համակարգչի իմունային համակարգը

Երկուշաբթի առավոտ է, և Լիլիթը պատրաստվում է երկօրյա դասընթաց անցկացնել Երևանի երիտասարդ ակտիվիստների համար, որոնք պաշտպանում են կանանց իրավունքները սոցիալական ցանցերում և իրենց համայնքներում: Սակայն, ի հայտ է գալիս անսպասելի հակառակորդը՝ վիրուսը: Նրա մարմին է ներթափանցում տհաճ վիրուս՝ պատճառելով հիվանդություն, ջերմություն և թուլություն:

Վիրուսի տարածման հետ մեկտեղ Լիլիթի իմունային համակարգն սկսում է պայքարել: Արյան սպիտակ բջիջները՝ նրա մարմնի պաշտպանները, հավաքվում են, որպեսզի բացահայտեն և չեզոքացնեն սպառնալիքը: Բայց միևնույն ժամանակ, Լիլիթի էներգիան արագորեն նվազում է՝ ազդելով նրա առանցքային դերը կատարելու ունակության վրա: Ի վիճակի չլինելով անցկացնել դասընթացը՝ նա հետաձգում է այն մինչ իր իմունային համակարգը կարողանա չեզոքացնել վիրուսը:

Նույն կերպ վնասակար ծրագրերը ներթափանցում են Ձեր համակարգիչ՝ վտանգելով ֆայլերը և դանդաղեցնելով ֆունկցիոնալությունը:

Տեսակ	Վնասակար ծրագիրը համակարգչում	Վիրուսը մարդու մարմնում
Էություն	Վնասակար ծրագրակազմը նախատեսված է ծրագրերը վնասելու և համակարգերը շահագործելու համար:	Կենդանի օրգանիզմներում ինֆեկցիոն հարուցիչները հանգեցնում են հիվանդության:
Ձև	Տարբեր ձևեր, ներառյալ վիրուսներ, որդեր, Տրոյաններ և այլն:	Հիվանդության պատճառ հանդիսացող տարբեր վիրուսներ (օր.՝գրիպ):
Փոխանցում	Տարածվում է վիրուսակիր ֆայլերից, վեբ կայքերից և ներբեռնումներից:	Տարածվում է անմիջական շփման միջոցով, օդակաթիլային ճանապարհով:
Կրկնօրինակում	Կրկնօրինակվում է համակարգչային համակարգում հետագա տարածման համար:	Կրկնապատկվում է հիվանդի բջիջներում՝հիվանդությունը տարածելու համար:
Մտադրություն	Կարող է հանգեցնել տվյալների հափշտակման, համակարգի խափանման կամ լրտեսության:	Առաջացնում է տարբեր աստիճանի ծանրության հիվանդություններ:
Հայտնաբերում	Հայտնաբերվում է հակավիրուսային ծրագրակազմի և կիբերանվտանգության գործիքների միջոցով:	Ախտորոշվում է բժշկական անալիզների և հետազոտությունների միջոցով:
Կանխարգելում	Կանխարգելվում է հակավիրուսի, միջցանցային էկրանի և թարմացումների միջոցով:	Կանխարգելվում է պատվաստումների, հիգիենայի և իմունային առողջության միջոցով:
Ազդեցությունը համակարգի վրա	Դանդաղեցնում, խափանում է աշխատանքը կամ վնասում է տվյալները:	Ի հայտ է բերում միջինից մինչև ծանր հիվանդության ախտանիշներ:
Լուծում	Պահանջում է վնասակար ծրագրերի հեռացման գործիքներ և համակարգի վերականգնում:	Բժշկական և դեղորայքային բուժում, ինչպես նաև օժանդակ խնամք:
Զարգացում	Անընդհատ զարգանում է նոր ձևերով և տեխնիկայով:	Զարգանում է մուտացիաների արդյունքում՝ առաջացնելով վիրուսի նոր շտամներ:
Ծագում	Մշակված է կիբերհանցագործների կամ չարակամ անձանց կողմից:	Լինում է մարդածին և բնածին:

Ո՞ՐՆ Է ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԻ և ՎԻՐՈՒՍԻ ՏԱՐԲԵՐՈՒԹՅՈՒՆԸ

Վնասակար ծրագիրը լայն տերմին է, որը ներառում է ցանկացած վնասակար ծրագրակազմ՝ համակարգիչը կամ ցանցը վնասելու համար: Այն ներառում է տարբեր տեսակներ, ինչպիսիք են վիրուսները, Տրոյանները և դրամաշորթ ծրագիրը: Մյուս կողմից, վիրուսը վնասակար ծրագրի հատուկ տեսակ է, որը կրկնօրինակվում է ինքնուրույն և տարածվում այլ ֆայլերի կամ համակարգերի վրա: Ըստ էության, բոլոր վիրուսները վնասակար ծրագրեր են, բայց ոչ բոլոր վնասակար ծրագրերն են վիրուս:

Վնասակար ծրագիրը վնասակար ծրագրակազմի կրճատ ձևն է: (Այո, նրանք նույնպես մականուններ ունեն):

Դա հավաքական տերմին է տարբեր վնասակար ծրագրերի համար, որոնք նախատեսված են համակարգիչները վնասելու, տեղեկատվություն գողանալու կամ նորմալ գործունեությունը խաթարելու համար:

Հիմա կարող եք մտածել, թե ինչու կիբերհանցագործները պետք է թիրախավորեն Ձեզ կամ Ձեր կազմակերպությանը վնասակար ծրագրերով:

1 **Քաղաքական լրտեսություն.** ցանցահենները կարող են զբաղվել քաղաքական լրտեսությամբ՝ քաղաքական գործերին և մարդու իրավունքներին առնչվող կանանց վերաբերյալ տեղեկություններ հավաքելու համար՝ շահագործելով կազմակերպությունների զգայուն տվյալները (22):

2 **Ակտիվության խաթարում.** վնասակար դերակատարները կարող են նպատակ ունենալ խափանելու կանանց իրավունքների պաշտպանության խմբերի գործունեությունը՝ նրանց համակարգերը վարակելով վնասակար ծրագրերով: Սա կարող է խանգարել փոփոխությունների քարոզչության նրանց կարողությանը:

3 **Ավելի մեծ հարձակումների համար հիմքի ձեռքբերում.** ցանցահենները հաճախ օգտագործում են սկզբնական վնասակար ինֆեկցիաները ցանցում տեղ գրավելու համար: Մուտք գործելով նրանք կարող են ընդլայնել իրենց հասանելիությունը և սկսել ավելի լայնածավալ հարձակումներ՝ հավանական վտանգի ենթարկելով կազմակերպության ողջ ենթակառուցվածքը (23):

4 **Քաղաքական կամ սոցիալական օրակարգեր.** սպառնալիք հանդիսացող դերակատարները կարող են վնասակար ծրագրեր կիրառել՝ որոշակի քաղաքական կամ սոցիալական օրակարգեր խթանելու համար, ինչպիսիք են ապատեղեկատվություն տարածելը կամ կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունների գործունեությունը վարկաբեկելը (24):

ԱՐԴՅՈ՞Ք ՍԱ ՆՇԱՆԱԿՈՒՄ Է, ՈՐ ԿԱՆ ՆԱԵ ԱՅԼ ՏԵՍԱԿԻ ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԱԿԱԶՄԵՐ: ԱՅՈ, ԲԱՎԱԿԱՆԻՆ ՇԱՏ...

Լրտեսական ծրագրեր. թվային լրտեսների պես անաղմուկ հետևում են և գողանում տեղեկատվությունը:

Գովազդային ծրագրեր. նման են նյարդայնացնող թռուցիկ բաժանողների, որոնք Ձեզ անհանգստացնում են անցանկալի գովազդներով:

Դրամաշորթ ծրագիր. թվային առևանգողի պես Ձեր ֆայլերն արգելափակում են, մինչև փրկագին վճարեք:

Որդ. վարակ տարածողների պես ինքնուրույն կրկնօրինակվում են և շահագործում խոցելիությունը:

Տրոյան. խաբուսիկ նվերների պես ի հայտ են գալիս օրինական ծրագրակազմի կերպարանքով

Ի՞ՆՉ Է ՄԻՋՑԱՆՑԱՅԻՆ ԷԿՐԱՆԸ

Միջցանցային էկրանը նման է Ձեր համակարգչային ցանցի անվտանգության աշխատակցին:

- Այն դիտարկում և վերահսկում է մուտքի և ելքի տրաֆիկը՝ հանդես գալով որպես պաշտպանիչ պատնեշ:
- Այն ներս է թողնում լավ բաները և արգելափակում վատերը, օրինակ՝ կիբերսպառնալիքները:
- Միջցանցային էկրանները կարող են լինել կա՛մ գործիքակազմեր, կա՛մ ծրագրակազմեր և առանցքային դեր են խաղում անվտանգ առցանց միջավայրի պահպանման գործում:

ՈՒՇԱԴՐՈՒԹՈՒՆ

Ինչպե՞ս պաշտպանել Ձեզ (այսինքն՝ Ձեր համակարգիչը) վնասակար ծրագրերից:

Բացի դժվար կոտրվող գաղտնաբառեր օգտագործելուց և կասկածելի հղումներ չբացելուց, կան քիչ, բայց կարևոր քայլեր, որոնք պետք է անեք.

- Տեղադրեք վստահելի հակավիրուսային և հակալրտեսական ծրագրեր՝ վնասակար ծրագրերի սպառնալիքները հայտնաբերելու և վերացնելու համար:
- Ապահովեք ծրագրակազմի թարմացումները, որը ներառում է օպերացիոն համակարգեր, հավելվածներ և հակավիրուսային ծրագրեր:
- Օգտագործեք միջցանցային էկրան՝ ցանցի մուտքային և ելքային տրաֆիկը վերահսկելու համար, և որպես հավելյալ արգելք վնասակար ծրագրերի դեմ:

ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Հարց 1. Ո՞րն է լրտեսական ծրագրերի հիմնական նպատակը:

Ա. Համակարգի արդյունավետության բարձրացում
Բ. Տեղեկության դիտարկում և հափշտակում
Գ. Ֆայլերի արգելափակում մինչև փրկագին վճարելը
Դ. Վարակների տարածում և ինքնակրկնօրինակում

Հարց 2. Ինչո՞ւ են կիբերհանցագործները քաղաքական լրտեսությամբ զբաղվում վնասակար ծրագրերի միջոցով:

Ա. Համակարգի արդյունավետությունը բարձրացնելու համար
Բ. Ակտիվությունը խափանելու համար
Գ. Ավելի մեծ հարձակումների հիմք ձեռք բերելու համար
Դ. Կոնկրետ քաղաքական կամ սոցիալական օրակարգերն առաջ մղելու համար

Պատասխանները կարելի է գտնել վերջին գլխում՝ Կիբերպատասխաններ

ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏԱՅԱԼԸ

Լիլիթի պայքարը վիրուսի դեմ արտացոլում է վնասակար ծրագրերի ազդեցությունը համակարգիչների վրա՝ թե՛ խաթարելով դրանց բնականոն աշխատանքը, թե՛ առաջացնելով ֆունկցիոնալության դանդաղեցում:

Վնասակար ծրագիրը վնասակար ծրագրակազմի տարբեր տեսակների համապարփակ տերմին է:

Կիբերհանցագործներն ակտիվիստներին թիրախավորում են վնասակար ծրագրերով՝ հիմք ստեղծելու քաղաքական լրտեսության, ակտիվության խանգարման, կոնկրետ քաղաքական և սոցիալական օրակարգերի առաջմղման և ավելի մեծ հարձակումների համար:

Ապահով եղեք՝ տեղադրելով հակավիրուսային և հակալրտեսական ծրագրեր, թարմացրեք ծրագրակազմը և օգտագործեք միջցանցային էկրան:

Մի քանի թվային տվյալներ վնասակար ծրագրի տարբեր տեսակների մասին

Համաշխարհային մասշտաբով բոլոր կազմակերպությունների **72,7** տոկոսը 2023 թվականին դարձել է դրամաշորթ ծրագրի հարձակման զոհ՝ ընդգծելով կիբերանվտանգության վրա ունեցած զգալի ազդեցությունը:

2020 թվականին կազմակերպությունների **61** տոկոսն իր վրա կրեց մի աշխատակցից մյուսը վնասակար գործողությունների տարածման ազդեցությունը: Մինչև 2021 թվականն այս թիվը հասավ **7** տոկոսի՝ ընդգծելով վնասակար ծրագրերից տուժելու դեպքերի աճող հաճախականությունը:

Գովազդային ծրագրերը կազմել են 2022 թվականին հայտնաբերված բոլոր բջջային սպառնալիքների **25,28** տոկոսը, ինչը ցույց է տալիս, որ դա տարածված սպառնալիքի հայտնի տեսակ է:

Աղբյուր
(19) https://www.cobalt.io/blog/cybersecurity-statistics-2024
(20) https://www.comparitech.com/antivirus/malware-statistics-facts/
(21) https://terranovasecurity.com/blog/cyber-security-statistics/

Պաշտպանեք Ձեր սարքերը, կազմակերպությունը և շահառուներին

Կիբերանվտանգության ճանապարհը կարող է դժվար թվալ: Սովորությունների փոփոխությունը կարող է ժամանակատար և աշխատատար լինել, սակայն այն կարևոր է զգայուն տեղեկատվությունը, ինքներդ Ձեզ, Ձեր գործընկերներին և ամենակարևորը Ձեր շահառուներին պաշտպանելու համար:

Սույն ուղեցույցը նպատակ ունի ապահովելու գործնական քայլեր սարքերի անվտանգության ապահովման, իրազեկության խթանման և կազմակերպության ներսում կիբերանվտանգության կայուն միջոցառումների իրականացման համար:

> Արդյունավետ լինելու համար կիբերանվտանգության ուսուցումը պետք է հանգեցնի վարքագծի փոփոխության:

ANRAS VAS | UNSPLASH

ՎԱՐՔԱԳԾԱՅԻՆ ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ՝ ԲԱՐԵԼԱՎՎԱԾ ԿԻԲԵՐԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԱՄԱՐ

Տեխնիկական միջոցառումներից բացի, վարքագծի փոփոխության խթանումը կենսական նշանակություն ունի կիբերանվտանգության կայուն դիրքորոշման համար:

1. Անվտանգ որոնման սովորություններ
- Աշխատակիցներին խորհուրդ տվեք ուշադիր ուսումնասիրել URL-ները, խուսափել կասկածելի հղումներ բացելուց և ստուգել կայքերի օրինականությունը:
- Օգտագործեք վեբ զտման գործիքներ՝ վիրուսային կայքերի մուտքն արգելափակելու համար

2. Երկգործոն նույնականացում (2ԳՆ)
- Խթանեք 2ԳՆ-ի օգտագործումը՝ օգտահաշիվներին և համակարգերին պաշտպանության լրացուցիչ շերտ ավելացնելու համար:
- Խրախուսեք կենսաչափական նույնականացման ընդունումը ուժեղացված անվտանգության համար

3. Միջադեպերի հաղորդման մշակույթ
- Խրախուսեք այնպիսի մշակույթի ձևավորումը, որտեղ աշխատակիցներն ազատ են ցանկացած կասկածելի գործունեության կամ անվտանգության միջադեպի մասին անհապաղ հայտնել:
- Ստեղծեք միջադեպերի արձագանքման հստակ ծրագիր՝ արդյունավետ լուծման համար:

Առաջնահերթություն տալով կիբերանվտանգությանը՝ կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունները կարող են ամրապնդել իրենց թվային ապահովությունը և պաշտպանել իրենց անգնահատելի աշխատանքը: Կրթության, փուլային իրականացման և վարքագծային փոփոխությունների խթանման համադրությունը կնպաստի ճկուն և անվտանգ կիբերմիջավայրի ստեղծմանը:

ՍԿՍԵՑԻՆՔ. ԿԻԲԵՐՍՈՎՈՐՈՒԹՅՈՒՆՆԵՐԻ ՔԱՅԼ ԱՌ ՔԱՅԼ ՓՈՓՈԽՈՒԹՅՈՒՆ

1. Աշխատակիցների վերապատրաստում
- Անցկացրեք կիբերանվտանգության իրազեկման դասընթացներ՝ աշխատակիցներին ծանոթացնելու ընդհանուր սպառնալիքներին, ֆիշինգային հարձակումներին և առցանց անվտանգ վարքագծի կարևորությանը:
- Սկսեք հիմնական հասկացություններից՝ նախքան կիբերանվտանգության ավելի բարդ օրինակների մեջ խորանալը:

2. Կանոնավոր կերպով թարմացվող դասընթացներ
- Պլանավորեք կիբերանվտանգության կանոնավոր կերպով թարմացվող դասընթացներ՝ գիտելիքներն ամրապնդելու և աշխատակիցներին առաջացող սպառնալիքների վերաբերյալ իրազեկելու համար:
- Խրախուսեք բաց հաղորդակցությունը՝ թույլ տալով աշխատակիցներին կիսվել մտահոգություններով և հարցեր տալ:

3. Փուլային իրականացում
- Իրականացրեք կիբերանվտանգության միջոցառումներ փուլ առ փուլ՝ աշխատակիցներին չծանրաբեռնելու համար:
- Սկսեք հիմնարար նյութերից, ինչպիսիք են գաղտնաբառի հիգիենան, և աստիճանաբար անցեք ավելի առաջադեմ միջոցների:

ԿԻԲԵՐԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ԻՐԱԿԱՆԱՑՈՒՄ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՄԱԿԱՐԴԱԿՈՎ

1. Հակավիրուսային ծրագրակազմի տեղադրում
- Օգտագործեք հեղինակավոր հակավիրուսային ծրագրակազմեր՝ վիրուսային սպառնալիքները հայտնաբերելու և վերացնելու համար:
- Կանոնավոր կերպով թարմացրեք հակավիրուսային տվյալների բազաները՝ վերջին սպառնալիքներից պաշտպանվելու համար:

2. Ծրագրակազմի և գործիքակազմի կանոնավոր թարմացումներ
- Կանոնավոր կերպով թարմացրեք օպերացիոն համակարգերը և հավելվածները՝ խոցելիությունը շտկելու համար:
- Հնարավորության դեպքում միացրեք ավտոմատ թարմացումները՝ հայտնի շահագործողներից ժամանակին պաշտպանվելու համար:
- Հավաստիացեք, որ բոլոր գործիքակազմերի բաղադրիչները, ներառյալ ռոուտերները և IoT սարքերը, ունեն ծրագրային ապահովման վերջին թարմացումները՝ անվտանգության խնդիրները լուծելու համար:

3. Միջցանցային էկրանների կիրառություն
- Միացրեք միջցանցային էկրանները ինչպես առանձին սարքերում, այնպես էլ ցանցային ենթակառուցվածքում:
- Կոնֆիգուրացրեք միջցանցային էկրանները՝ դիտարկելու և վերահսկելու մուտքային և ելքային ցանցի տրաֆիկը՝ բարձրացնելով ընդհանուր անվտանգությունը:

4. Աշխատակիցների համար թույլտվությունների կարգավորում
- Կիրառեք նվազագույն արտոնությունների սկզբունքը՝ աշխատակիցներին տալով միայն իրենց դերի համար անհրաժեշտ թույլտվությունները:
- Կանոնավոր կերպով վերանայեք և թարմացրեք թույլտվությունները՝ կազմակերպական փոփոխություններին և աշխատակիցների դերերին համապատասխանեցնելու համար:

5. Գաղտնագրման օգտագործում
- Խրախուսեք գաղտնագրման օգտագործումն զգայուն հաղորդակցությունների և տվյալների պահպանման համար:
- Իրականացրեք ծայրից ծայր գաղտնագրումը հաղորդագրությունների հարթակների համար՝ գաղտնի խոսակցությունները պաշտպանելու նպատակով:

6. Տվյալների կանոնավոր պահեստավորում
- Ընդգծեք տվյալների կանոնավոր պահեստավորման կարևորությունը փրկագնային ծրագրերի հարձակումների կամ տվյալների կորստի ազդեցությունը մեղմելու համար:
- Պահպանեք պահեստավորումներն ապահով կերպով, նախընտրելի է անցանց կամ ամպային միջավայրում և կանոնավոր կերպով փորձարկեք վերականգնման գործընթացները:

ՍՏՈՒԳԵՔ ՁԵՐ ԳԻՏԵԼԻՔՆԵՐԸ

Հարց. ո՞րն է կիբերանվտանգության ուսուցման առաջնային նպատակը:

Ա) Բարելավել սարքի գեղագիտական կողմը
Բ) Հանգեցնել վարքագծի փոփոխության
Գ) Անտեսել կիբերանվտանգության միջոցառումները
Դ) Կենտրոնանալ միայն բարդ օրինակների վրա

Հարց. ո՞րն է առաջարկվող մոտեցումը կազմակերպչական մակարդակում կիբերանվտանգության միջոցառումների իրականացման համար:

Ա) Առաջատար միջոցառումների անհապաղ իրականացում
Բ) Պատահականության սկզբունքով միջոցառումների ներդրում
Գ) Փուլային իրականացում՝ սկսած հիմնարար
Դ) Հենվելով բացառապես աշխատողներին ընձեռնված թույլտվությունների վրա

Հարց. կիբերանվտանգության ո՞ր միջոցն է ենթադրում աշխատակիցներին միայն իրենց դերի համար անհրաժեշտ թույլտվությունների տրամադրումը:

Ա) Գաղտնագրում
Բ) Միջցանցային էկրաններ
Գ) Կանոնավոր պահեստավորումներ
Դ) Թույլտվությունների կարգավորում

Պատասխանները կարելի է գտնել վերջին գլխում՝ Կիբերպատասխաններ

ԵԹԵ ԱՅՍ ԲԱԺՆԻՑ ԱՌԱՆՁՆԱՑՆԵՆՔ ՄԻ ՔԱՆԻ ԱՌԱՆՑՔԱՅԻՆ ԿԵՏԵՐ, ԱՊԱ ԴՐԱՆՔ ԿԼԻՆԵՆ ՀԵՏԱՅԱԼԸ.

Առաջնահերթություն տվեք կիբերանվտանգությանը. ընդունեք կիբերանվտանգության դժվար ճանապարհը և հասկացեք զգայուն տեղեկատվությունը պաշտպանելու համար սովորությունները փոփոխելու անհրաժեշտությունը:

Արդյունավետ վերապատրաստում. հավաստիացեք, որ կիբերանվտանգության վերապարաստման արդյունքները փոխում են վարքագիծը՝ անցկացնելով իրազեկման դասընթացներ՝ սկսելով հիմնական հասկացություններից և ներառելով կանոնավոր կերպով թարմացվող դասընթացներ:

Փուլային իրականացում. կիբերանվտանգության միջոցներն աստիճանաբար ներդրեք կազմակերպչական մակարդակում՝ սկսած հիմնարար նյութերից, ինչպիսիք են հակավիրուսային ծրագրերի տեղադրումը և անցումն ավելի առաջադեմ քայլերի:

Տեխնիկական միջոցառումներ. կիրառեք հակավիրուսային ծրագրեր, կանոնավոր թարմացումներ, միջցանցային էկրաններ և գաղտնագրում՝ ինչպես առանձին սարքերի, այնպես էլ ցանցային ենթակառուցվածքի համար:

Վարքագծային փոփոխություններ. ընդլայնեք կիբերանվտանգության մշակույթը անվտանգ որոնման սովորությունների, երկգործոն նույնականացման և միջադեպերի կայուն զեկուցման միջոցով:

ԻՐԱՎԻՃԱԿԱՅԻՆ ՎԱՐԺՈՒԹՅՈՒՆ. ՖԻՇԻՆԳԻ ՍԻՄՈՒԼՅԱՑԻԱ և ԱՌԱՋՆԱՀԵՐԹ ԱՐՁԱԳԱՆՔ

Սիմուլացրեք ֆիշինգի բարդ հարձակումը, որն ուղղված է աշխատակիցներին՝ գնահատելու կազմակերպության կարողությունը՝ հայտնաբերելու, արձագանքելու և առաջնահերթություն տալու կիբերանվտանգության գործողություններին:

Վարժության քայլեր

1. Ֆիշինգային էլեկտրոնային հաղորդագրության սիմուլյացիա
- Պատահականության սկզբունքով ընտրված աշխատակիցներին ուղարկեք իրատեսական ֆիշինգային էլեկտրոնային հաղորդագրություններ:
- Ստեղծեք իրավիճակներ, որոնք կրկնօրինակում են ֆիշինգի սովորական մարտավարությունը, ինչպիսիք են հրատապ հարցումները, գայթակղիչ առաջարկները կամ ներքին քողարկված հաղորդակցությունները:

2. Աշխատակիցների պատասխանները
- Հետևեք, թե ինչպես են աշխատակիցներն արձագանքում ֆիշինգային էլեկտրոնային հաղորդագրություններին:
- Գնահատեք՝ արդյոք նրանք ճանաչում են ֆիշինգի փորձը, անհապաղ հաղորդում են դրա մասին, թե դառնում են հարձակման զոհ:

3. Անվտանգության թիմի ծանուցում
- Տեղեկացրեք կիբերանվտանգության թիմին սիմուլացված ֆիշինգային հարձակման մասին:
- Գնահատեք թիմի արձագանքման ժամանակը և արդյունավետությունը ֆիշինգի փորձը վերլուծելու և հաստատելու հարցում:

4. Միջադեպի արձագանքման առաջնահերթություն
- Ելնելով ֆիշինգի հարձակման ծանրությունից՝ առաջնահերթություններ նշանակեք միջադեպերի արձագանքման գործողություններին:
- Ստուգեք կազմակերպության կարողությունը՝ առաջնահերթություն սահմանելու և ռեսուրսներն արդյունավետորեն բաշխելու համար:

5. Հաղորդակցություն և վերապատրաստում
- Տեղեկացրեք աշխատողներին սիմուլացված միջադեպի մասին՝ ընդգծելով ֆիշինգի սպառնալիքների դեմ զգոնության կարևորությունը:
- Տրամադրեք թիրախավորված ուսուցում ֆիշինգի փորձերի ճանաչման և հաղորդման վերաբերյալ:

6. Հետվարժական վերլուծություն
- Իրականացրեք վարժությունների մանրակրկիտ վերլուծություն՝ բացահայտելով բարելավման ոլորտները:
- Գնահատեք կազմակերպության կիբերանվտանգության ուսուցման արդյունավետությունը և համապատասխանաբար կարգավորեք առաջնահերթությունները:

Սույն իրավիճակային վարժությունը կենտրոնանում է ֆիշինգի հարձակումներին արձագանքելու առաջնահերթության վրա, որը կիբերանվտանգության տարածված սպառնալիք է: Այն օգնում է կազմակերպություններին գնահատել իրենց պատրաստակամությունը՝ դիմակայելու անվտանգության զարգացող մարտահրավերներին:

«Կիբերանվտանգության ոլորտում Դուք կարող եք ունենալ լավագույն պաշտպանությունը (հակավիրուսային ծրագիր, ՎՄՑ և այլն...), և դա դեռ բավարար չէ: Մարդիկ ամենաթույլ օղակն են: Մարդկային մեկ սխալը կարող է պաշտպանական համակարգի խափանման պատճառ դառնալ»:

- Դավիթ Ղոնղաձե՝ կիբերանվտանգության փորձագետ:

Ամփոփում

Ամփոփելով կիբերանվտանգության սույն ուղեցույցը, որը հարմարեցված է Հայաստանում կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպություններին, հարկ է նշել, որ թվային անվտանգության և մարդու իրավունքների պաշտպանության առանցքային փոխհատումը պետք է հստակ լինի: Զգայուն տեղեկատվության և թվային ակտիվների պահպանումը պարզապես լավագույն տարբերակ չեն. դրանք էական նախապայման են մարդու իրավունքների պահպանման տեսանկյունից:

Կիբերսպառնալիքների զարգացող մասշտաբն ընդգծում է կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպությունների կողմից վարքագծի հարացուցային փոփոխություն մշակելու հրատապությունը: Կիբերանվտանգության ուժեղ միջոցառումները, որոնք ներառում են իրական ժամանակի դիտարկում և ակտիվ լուծումներ, հնարավոր ռիսկերի դեմ թվային ենթակառուցվածքն ուժեղացնելու գործում ժամանակի հրամայական են:

Իրական աշխարհում այնպիսի անհատներ, ինչպիսիք են Լիլիթը և Անահիտը, կարող են ամբողջությամբ նվիրվել կանանց իրավունքների պաշտպանությանը, լայնամասշտաբ նախաձեռնություններն առաջնորդելու և վերապատրաստելու՝ առանց կիբերսպառնալիքների վերաբերյալ անհանգստանալու: Սակայն, մեր աշխարհի իրականությունը պահանջում է զուգահեռ արշավ՝ կիբերանվտանգության փոփոխությունների և կազմակերպչական մակարդակում ավելի անվտանգ գործելակերպերի ինտեգրման համար:

Պատկերացրեք Անահիտին և Լիլիթին, ովքեր ծանր շաբաթվա ավարտին լիցքաթափվում են իրենց սիրելի ռեստորանում: Մանրակրկիտ կիբերգնահատում կատարելով և կիբերանվտանգության առաջնահերթ միջոցառումների վերաբերյալ վերապատրաստվելով՝ նրանք այժմ զինված են՝ պաշտպանելու իրենց թիմերին, ինչպես նաև իրենց շահառուներին:

Սույն ուղեցույցը նախատեսված չէ վախ սերմանելու համար, ավելի շուտ, այն հանդես է գալիս որպես գործնական աղբյուր՝ զինելով Հայաստանում կանանց իրավունքների պաշտպանությամբ զբաղվող կազմակերպություններին թվային օվկիանոսում անվտանգ նավարկելու համար՝ անհրաժեշտ գիտելիքներով և գործիքներով: Դրանով նրանք կարող են կենտրոնանալ գենդերային հավասարության և մարդու իրավունքների առաջխաղացման իրենց առանցքային առաքելության վրա:

SINCERELY MEDIA | UNSPLASH

Ձեր կիբերպատասխանները

Գլուխ. Արդյո՞ք ես իսկապես թիրախ եմ

Ճիշտ պատասխանն է Ա. Թիրախավորված հարձակում՝ նրա տվյալները գողանալու համար: Բացահայտելով այն կազմակերպությունը, որի հետ Լիլիթը համագործակցում է, և ձևացնելով, թե ներկայացնում է այն, որ նամակ ուղարկի իրեն, նշանակում է, որ կիբերհարձակվողները կատարել են իրենց հետազոտությունները և հատուկ թիրախավորել Լիլիթին: Խնդրելով նրան թարմացնել իր հավատարմագրերը՝, նրանք նպատակ էին հետապնդում գողանալու նրա օգտանունն ու գաղտնաբառը և կոտրելու նրա օգտահաշիվները:

Գլուխ. Անվտանգ համացանցային որոնումներ՝ կքայլեի՞ք մարդաշատ փողոցով՝ Ձեր պայուսակը բաց

Պատասխան. Ճիշտ պատասխաններն են՝ 1, 2, 4, 5, 6, 7: Միակ սխալ պատասխանը 3-ն է: Թեև «Նորություններին բաժանորդագրության հաստատում» վերնագրով նամակը կարող է լինել ֆիշինգային էլեկտրոնային հաղորդագրության վերնագիր, մյուս բոլոր էլեկտրոնային հաղորդագրությունների թեմաները հրատապության զգացում են առաջացնում և վախ տարածում՝ անհապաղ գործողություններ սկսելու համար: Այս էմոցիոնալ մտաշահարկումը սովորական մարտավարություն է, որն օգտագործվում է ցացնցահեների կողմից՝ անհատներին մղելով բացել ֆիշինգային էլեկտրոնային հաղորդագրության հղումները:

Գլուխ. Հանրային Wi-Fi՝ դրախտ կիբերհանցագործների համար

1-ին հարցի պատասխանն է Գ. Բաց լինելը կիբերհարձակվողների համար: Ամենակարևոր վտանգը, որ ներկայացնում են հանրային Wi-Fi ցանցերը, կիբերհարձակումն է: Որոշ դեպքերում այս բացահայտումը թույլ է տալիս նրանց հետևել Ձեր ֆիզիկական տեղաշարժին:

2-րդ հարցի պատասխանն է Գ. Ստեղծելով անվտանգ կապ: ՎՄՑ-ն ուժեղացնում է անվտանգությունը հանրային Wi-Fi-ում՝ վերահղելով Ձեր համացանցային կապը մասնավոր սերվերի միջոցով՝ անհասանելի դարձնելով Ձեր իրական IP հասցեն և թաքցնելով Ձեր առցանց գործունեությունը:

Գլուխ. Ի՞նչ ընդհանրություն կա Ձեր տան բանալիների և գաղտնաբառերի միջև

Իրավիճակային թեստի հարցի պատասխանն է Գ. Փոխի վտանգված օգտահաշվի գաղտնաբառերը և միացնի երկգործոն նույնականացում: Եթե նրա գաղտնաբառը վտանգի է ենթարկվել և արտահոսել է տվյալների խախտման արդյունքում, դա նշանակում է, որ կիբեր ցանցահենները հասանելիություն ունեն դեպի նրա օգտանուն և գաղտնաբառեր: Անահիտը պետք է անհապաղ փոխի վտանգված օգտահաշվի գաղտնաբառը և ակտիվացնի երկգործոն նույնականացումը՝ պաշտպանության լրացուցիչ շերտի համար:

Գլուխ. Վնասակար ծրագիր՝ վիրուս, որը թուլացնում է Ձեր համակարգչի իմունային համակարգը

1-ին հարցի պատասխանն է Բ. Տեղեկության դիտարկում և հափշտակում: Լրտեսական ծրագրերի հիմնական նպատակը նման է թվային լրտեսների նպատակին, այն է՝ անաղմուկ դիտարկել և հափշտակել տեղեկատվություն:

2-րդ հարցի պատասխանն է Բ. Ակտիվությունը խափանելու համար: Ցանցահենները կարող են զբաղվել քաղաքական լրտեսությամբ՝ ակտիվիստների, խաղաղաշինարարների և կազմակերպությունների վերաբերյալ տեղեկություններ հավաքելու համար՝ օգտագործելով զգայուն տվյալները՝ ակտիվությունը խափանելու համար:

Գլուխ. Պաշտպանեք Ձեր սարքերը, կազմակերպությունը և շահառուներին

1-ին հարցի պատասխանն է Բ. Հանգեցնել վարքագծի փոփոխության: Կիբերանվտանգության վերաբերյալ ցանկացած դասընթացի առաջնային նպատակն է խրախուսել մարդկանց փոխել իրենց վարքագիծն այնպես, որ այն նպաստի կազմակերպության բոլոր աշխատակիցների համար ավելի անվտանգ աշխատանքային միջավայրի ստեղծմանը:

2-րդ հարցի պատասխանն է Գ. Փուլային իրականացում՝ սկսած հիմնարար գործելակերպից: Առաջարկվող մոտեցումն է սկսել քայլ առ քայլ՝ այնպիսի հիմունքներից, ինչպիսիք են անվտանգ որոնումը համացանցում և ֆիշինգային էլեկտրոնային հաղորդագրությունների ճանաչումը: Այնուհետև կարող եք անցնել գաղտնագրված էլեկտրոնային հաղորդագրություններին, միջցանցային էկրաններին, ՎՄՑ-ներին և այլ ավելի բարդ թեմաներին:

3-րդ հարցի պատասխանն է Դ. Թույլտվությունների կարգավորում:

Աղբյուրներ

https://cyberhub.am/wp-content/uploads/2023/12/Armenia-Digital-Threat-Landscape-Report.pdf

https://www.1lurer.am/en/2023/09/23/Significant-increase-in-cyber-attacks-recorded-in-Armenian-domain-of-the-Internet-NSS/1001145

https://csometer.info/updates/armenia-amended-ogp-action-plan-2022-2024-improve-public-participation-opportunities

https://mdi.am/wp-content/uploads/2021/02/Digital%20security%20incidents%20against%20the%20Armenian%20Civil%20Society%20in%202019%20-%202020_Artur%20Papyan.pdf

https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights

https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf

https://ge.boell.org/en/2022/12/18/armenias-peace-and-security-womens-participation-and-feminist-perspectives

https://blogs.worldbank.org/europeandcentralasia/safe-you-app-armenian-women-use-technology-tackle-gender-based-violence

https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations

https://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma

https://www.amnesty.org/en/latest/campaigns/2015/08/how-governments-are-using-spyware-to-attack-free-speech/

https://tech.co/password-managers/how-long-hacker-crack-password#:~:text=A%2010%2Ddigit%20password%20that,hacker%20up%20to%20two%20weeks

https://www.verveit.com/blog/is-your-password-strong-enough/

https://www.cobalt.io/blog/cybersecurity-statistics-2024

https://www.comparitech.com/antivirus/malware-statistics-facts/

https://terranovasecurity.com/blog/cyber-security-statistics/

https://www.linkedin.com/pulse/breaking-down-tactics-used-hackers-exploit-womens-rights-middle

https://www.sciencedirect.com/science/article/pii/S245195882200001X

https://www.ibm.com/topics/threat-actor

INSTITUTE FOR
WAR & PEACE REPORTING

iwpr.net

IWPR United Kingdom
48 Gray's Inn Road,
London WC1X 8LT
Tel +44 (0)20 7831 1030

IWPR United States
1156 15th Street NW Suite 329,
Washington, DC 20005
Tel +1 202 393 5641

IWPR Netherlands
iwpr-nl@iwpr.net