Ֆիշինգ և սոցիալական ինժեներիա

Խարդախության մեխանիզմները
և պաշտպանական որոշումները

Phishing, scams & social engineering



Սկզբնական իրավիճակ

Դուք ունեք 30 վայրկյան որոշելու համար

01 «Տեղեկագրերի հասանելիությունը կփակվի 15 րոպեից»

02 Ուղարկող՝ «Համալսարանի ՏՏ բաժին»

03 Պահանջ՝ մուտք գործել և հաստատել հաշիվը

Հիմնական հասկացությունները

Սոցիալական ինժեներիան փոխում է մարդու որոշումը

01 Սոցիալական ինժեներիա՝ վստահության ու վարքի շահարկում

02 Ֆիշինգ՝ վստահելի աղբյուրի նմանակմամբ խաբուսիկ հաղորդակցություն

03 Scam՝ խարդախ սխեմա, որի նպատակը կարող է լինել փողը

04 Հնարավոր արդյունքներ՝ գաղտնաբառ, գումար, թույլտվություն, մուտք

Հոգեբանական ճնշման մեխանիզմները

Հարձակվողը փորձում է արագացնել որոշումը

01 Հեղինակություն՝ ղեկավար, բանկ, պետական մարմին

02 Շտապողականություն՝ «մինչև օրվա վերջը»

03 Վախ կամ շահույթ՝ հաշվի կորուստ, մրցանակ, եկամուտ

04 Գաղտնիություն և աստիճանական ներգրավում

Թիրախի մասին տեղեկությունը

Ծանոթ մանրամասները կարող են գալ բաց աղբյուրներից

01 Spear phishing՝ անհատականացված թիրախավորում

02 Smishing՝ SMS, vishing՝ ձայնային հաղորդակցություն

03 QR և չաթեր՝ նույն խնդրանքի այլ ալիքներ

04 Բաց տվյալները կարող են հարմարեցնել հարձակման պատմությունը

URL հասցեի կառուցվածքը

Որոշիչը հասցեի host մասն է

01 scheme://host/path?query#fragment

02 https://mail.university.example/login

03 https://university.example.attacker.test/login

04 Վերջին օրինակի host-ը պատկանում է attacker.test-ին

Դոմենների վերլուծության վարժություն

Ո՞ւր կգնա զննարկիչը

01 A https://login.university.example/

02 B https://university.example.attacker.test/

03 C https://attacker.test/university.example

04 D https://university.example@attacker.test/

HTTPS և վստահության տեսքը

Գաղտնագրված կապը չի հաստատում խնդրանքի օրինականությունը

01 HTTPS-ը պաշտպանում է կապը տվյալ հոսթի հետ

02 Կեղծ էջն էլ կարող է ունենալ վավեր TLS վկայական

03 Լոգոն, լավ լեզուն և գեղեցիկ էջը հեշտ է կրկնօրինակել

04 Վստահելի ծառայության իրական էջում էլ կարող են չարաշահել գործողությունը

Նամակի ուղարկողի շերտերը

Երևացող անունը և վավերացված դոմենը տարբեր տվյալներ են

01 Display name՝ օգտվողին երևացող անուն

02 From՝ հաղորդագրության հեղինակային հասցե

03 Reply-To՝ պատասխանի ուղղություն

04 Return-Path և Authentication-Results՝ տեխնիկական հետքեր

SPF DKIM և DMARC

Ի՞նչն է հաստատում յուրաքանչյուր մեխանիզմը

01 SPF՝ ուղարկող սերվերի թույլատրումը envelope դոմենի համար

02 DKIM՝ ստորագրություն ստորագրող դոմենի անունից

03 DMARC՝ From դոմենի համապատասխանեցում և քաղաքականություն

04 DMARC pass-ը չի հաստատում նամակի պահանջի անվտանգությունը

Նամակի վերլուծության գործնական օրինակ

Չորս ապացույց և մեկ որոշում

01 Ուղարկող՝ «Հաշվապահություն»

02 Reply-To-ն արտաքին դոմենում է

03 Պահանջվում են անձնագրի և քարտի տվյալներ

04 Վերջնաժամկետ՝ 10 րոպե, ստուգումն արգելվում է

SMS QR և առաքման խաբեությունը

Փոքր վճարումը կարող է մեծ տվյալ պահանջել

01 «Առաքանին պահվում է, վճարեք 390 դրամ»

02 QR-ը պահում է տվյալ, հաճախ՝ հղում

03 Հեռախոսը կարող է դուրս մնալ աշխատանքային պաշտպանության շերտերից

04 Վճարման կարիքը ստուգվում է առաքման պաշտոնական միջավայրում

Ցուցադրում Safe Browsing և ICANN

Երկու գործիք՝ տարբեր հարցերի համար

01 Safe Browsing՝ հայտնի վտանգի մասին ազդանշան

02 ICANN Lookup՝ գրանցման տվյալներ, երբ հասանելի են

03 Նոր դոմենը կամ թաքնված տվյալը առանձին դատավճիռ չեն

04 Մաքուր արդյունքը պահանջի օրինականության ապացույց չէ

Google Safe Browsing

ICANN Lookup

Ցուցադրում VirusTotal և urlscan

Հետազոտման գործիքներն էլ ունեն գաղտնիության սահմաններ

01 VirusTotal՝ տարբեր շարժիչների ու տվյալների համադրում

02 urlscan՝ էջի վարք, ցանցային կապեր և պատկեր

03 0 հայտնաբերում ≠ անվտանգություն

04 Գաղտնի հղումները և ֆայլերը չեն ուղարկվում հանրային ստուգման

Իրական դեպք Cloudflare 2022

Ֆիշինգի հաջող սեղմումը կարող է չդառնալ հաջող մուտք

01 Աշխատակիցները ստացան ներքին մուտքին նման SMS-ներ

02 Որոշ աշխատակիցներ մուտքագրեցին տվյալները

03 Պարտադիր FIDO2 անվտանգության բանալիները կանգնեցրին մուտքը

04 Արագ հաղորդումը օգնեց արձագանքել

MFA մեթոդների տարբերությունները

Միանգամյա կոդը դեռ կարելի է խաբեությամբ փոխանցել

01 SMS և TOTP՝ հարձակվողը կարող է խնդրել կամ փոխանցել կոդը

02 Push հաստատումներ՝ հնարավոր է ճնշում և շփոթություն

03 Number matching՝ նվազեցնում է որոշ սխալ հաստատումներ

04 FIDO2 և WebAuthn՝ ֆիշինգին դիմակայող մուտքի հիմք

AiTM և session cookie

Մուտքի արդյունքն էլ կարող է լինել թիրախ

01 Օգտվողը շփվում է միջնորդ էջի հետ

02 Միջնորդը փոխանցում է մուտքի փոխազդեցությունը

03 Հարձակվողը ստանում է սեսիայի օգտագործման հնարավորություն

04 Վերականգնումը ներառում է սեսիաների ու token-ների հետկանչ

Passkey և դոմենի հետ կապումը

WebAuthn-ը ստուգում է ծառայության նույնականացումը

01 Համապատասխան բանալին կապված է ծառայության RP ID-ի հետ

02 Զննարկիչն ու ծառայությունը ստուգում են origin և RP ID սահմանները

03 Գաղտնի բանալին սովորական գաղտնաբառի պես չենք փոխանցում

04 Հաշվի վերականգնումն ու սարքի պաշտպանությունը շարունակում են կարևոր մնալ

OAuth consent phishing

Իսկական մուտքի էջը կարող է տանել սխալ թույլտվության

01 «PDF դիտարկիչը» խնդրում է կարդալ ձեր նամակները

02 Թույլտվությունների ցանկը գործարքի բովանդակությունն է

03 Հավելվածի անունը կամ verified publisher-ը բավարար երաշխիք չեն

04 Հետկանչը ներառում է հավելվածի թույլտվությունների հեռացում

Device code phishing

Ճիշտ հասցե, բայց ուրիշի նախաձեռնած մուտք

01 Ճանոթ ծառայության իրական մուտքի էջ

02 Հաղորդագրությամբ ստացված սարքի կոդ

03 Օգտվողը հաստատում է անծանոթ նախաձեռնությունը

04 Պաշտպանություն՝ հոսքի սահմանափակում և գործողության իմաստի ստուգում

ClickFix և կեղծ CAPTCHA

Ստուգման պատրվակով հրահանգի կատարում

01 «Հաստատեք, որ ռոբոտ չեք»

02 Էջը խնդրում է բացել Run կամ Terminal

03 Clipboard-ից հրահանգը կարող է վնասաբեր լինել

04 Դասի ընթացքում որևէ հրահանգ չենք պատճենում ու գործարկում

Facebook բանկ և վաճառքի հարթակ

Պատմությունը փոխվում է, զգայուն քայլը կրկնվում է

01 «Ձեր էջը կջնջվի հեղինակային իրավունքի խախտման համար»

02 «Վճարումը ստանալու համար գրեք քարտի գաղտնի կոդը»

03 «Բանկի անվտանգությունից ենք, հաստատեք մուտքը»

04 Ստուգումը կատարվում է ծառայության սեփական հավելվածում

Business Email Compromise

Գումարը կարող է կորել առանց կեղծ կայքի

01 Գործընկերոջ իրական նամակագրության շարունակություն

02 «Մեր բանկային հաշիվը փոխվել է»

03 Հնարավոր է՝ վավերացված իրական հաշիվ

04 Հայտնի համարով հաստատում և երկրորդ հաստատող

Ձայնային խաբեություն և AI

Ծանոթ ձայնը ինքնության բավարար ապացույց չէ

01 Ընտանիքի արտակարգ դեպքի պատմություն

02 Ղեկավարի անունից շտապ վճարման պահանջ

03 Caller ID-ն և տեսազանգի պատկերը կարող են մոլորեցնել

04 Հետադարձ կապ՝ արդեն հայտնի անկախ համարով

Task scam և կեղծ եկամուտ

Էկրանին երևացող շահույթը դեռ ստացվող գումար չէ

01 Անսպասելի «աշխատանք»՝ like, rating, optimization

02 Սկզբնական փոքր վճարումը վստահություն է ստեղծում

03 Հետո պահանջվում է սեփական գումարի ներդրում

04 «Մնաց մի վճար» պահանջը կարող է շարունակել կորուստը

Կենդանի վարժություն Google Jigsaw

Որոշումը պետք է ունենա ապացույց

01 2 օրինակ՝ միասնական վերլուծությամբ

02 Մինչև ընտրությունը՝ ո՞ր գործողությունն է պահանջվում

03 Հետո՝ ո՞ր դոմենը կամ հասցեն է կարևոր

04 Վերջում՝ ի՞նչ անկախ քայլով կստուգեինք

phishingquiz.withgoogle.com

Խմբային դեպքի քննություն

Մատակարարի հաշիվը փոխվել է

01 Իրական նամակագրության մեջ նոր հաշվեհամար

02 Ուղարկողի հասցեն նույնն է, DMARC pass

03 Զանգողը պնդում է՝ «վճարեք հիմա»

04 Խմբի արդյունք՝ որոշում, անկախ ստուգում և տեղեկացում

Միջադեպից հետո միայն հղում եմ բացել

Պատասխանը կախված է իրական գործողությունից

01 Փակել էջը և այլ քայլ չանել

02 Գրանցել ժամը, հասցեն և ինչ է տեղի ունեցել

03 Ստուգել ներբեռնումներն ու զննարկչի թույլտվությունները

04 Աշխատանքային սարքի դեպքում արագ տեղեկացնել SS թիմին

Միջադեպից հետո հաշվի մուտք եմ տվել

Գաղտնաբառ սեսիա և թույլտվություն՝ առանձին շերտեր

01 Վստահելի սարքից բացել ծառայության պաշտոնական մուտքը

02 Փոխել գաղտնաբառը և կրկնօգտագործված գաղտնաբառերը

03 Հետ կանչել սեսիաները, ստուգել MFA և վերականգնումը

04 Վերանայել հավելվածները, forwarding կանոնները և մուտքերը

Միջադեպից հետո գումար կամ սարքի վերահսկում եմ տվել

Ֆինանսական և տեխնիկական արձագանքները սկսվում են արագ

01 Փոխանցում՝ անհապաղ կապ ֆինանսական հաստատության հետ

02 Կասկածելի հեռակա մուտք՝ սարքի մեկուսացում և SS թիմ

03 Ապացույցներ՝ հաղորդագրություն, ժամ, գործարքի համար

04 «Կվերադարձնեմ գումարը» նոր առաջարկը ևս ստուգվում է

Կազմակերպության պաշտպանության շերտերը

Կանոնը պետք է գործի նաև մեկ սխալից հետո

01 Տեխնիկական՝ պաշտպանված մուտք, թարմացումներ, mail controls

02 Գործընթացային՝ վճարման փոփոխության անկախ հաստատում

03 Իրավասություններ՝ նվազագույն անհրաժեշտ մուտք

04 Մարդկային՝ հեշտ հաղորդում և առանց նվաստացման արձագանք

Ստուգման սովորություն և օգտակար չափումներ

Պաշտպանության արդյունքը մի click rate-ով չի չափվում

01 Հարցում՝ ո՞վ է խնդրում և ի՞նչ եմ թույլատրում

02 Ստուգում՝ անկախ հայտնի կապ կամ պաշտոնական միջավայր

03 Չափում՝ որքան արագ և հստակ են հաղորդում

04 Արդյունք՝ կանխված մուտք, փոխանցում և սահմանափակված վնաս

haveibeenpwned.com

Գիտելիքի ստուգում

Յուրաքանչյուր պնդման համար՝ պատճառ և գործողություն

01 1 HTTPS-ը հաստատում է կայքի ազնվությունը

02 2 DMARC pass-ը բացառում է BEC-ը

03 3 Ճիշտ մուտքի էջում ամեն կոդ կարելի է հաստատել

04 4 Գաղտնաբառ փոխելուց հետո բոլոր մուտքերը վերանում են

Վերջնական գործողությունների ուղեցույց

Զգայուն խնդրանքը հաստատվում է անկախ ճանապարհով

01 Դադար՝ մինչև հասկանաք պահանջվող գործողությունը

02 Ստուգում՝ հայտնի կապով կամ պաշտոնական միջավայրում

03 Հաղորդում՝ արագ, ճշգրիտ, ապացույցը պահպանելով

04 Վերականգնում՝ ըստ գաղտնաբառի, սարքի, token-ի կամ գումարի

Ցուցադրման կայքեր և աղբյուրներ

Ակտիվ հղումներ · ամբողջական հասցեները՝ նշումներում

CISA CISA — Phishing infographic

FBI FBI — Business Email Compromise

MAIL Microsoft Learn — Email authentication

DMARC Microsoft Learn — DMARC

CF Cloudflare — SMS phishing case, 2022

MITM Microsoft — AiTM and cookie theft, 2022

MFA CISA — Implementing phishing resistant MFA

Աղբյուրներ և ընթերցանություն

Ակտիվ հղումներ · ամբողջական հասցեները՝ նշումներում

NIST NIST SP 800-63B-4 — Authenticators

OAUTH Microsoft Learn — Consent phishing

DEVICE Microsoft — Storm-2372 device code phishing, 2025

CAPTCHA FTC — CAPTCHA scam, June 2026

VOICE FTC — AI voice cloning and family emergency scams

TASK FTC — Task scams, 2025

QR FTC — Unexpected package QR scam

Աղբյուրներ և ընթերցանություն

Ակտիվ հղումներ · ամբողջական հասցեները՝ նշումներում

QUIZ Google/Jigsaw — Phishing Quiz

SAFE Google — Safe Browsing

ICANN ICANN — RDAP and Lookup

VT VirusTotal — Private scanning and standard uploads

SCAN urlscan — Scan visibility

HIBP Have I Been Pwned