Sosial Mühəndislik Hücumlarının İstifadəçi Davranışına Manipulyativ Təsir Mexanizmlərinin Analizi

Gülər Həmzəzadə
Azərbaycan Memarlıq və İnşaat Universiteti, Bakı, Azərbaycan
hemzezadeguler@gmail.com

***Xülasə*— Müasir rəqəmsal mühitdə kibercinayətlərin xarakteri dəyişərək texniki zəifliklərdən daha çox insan faktoruna yönəlmişdir. Sosial mühəndislik hücumları istifadəçi davranışını manipulyasiya etməyə əsaslanır və bu prosesdə dizayn mühüm rol oynayır. Məqalədə istifadəçi interfeysinin vizual dizaynı (UI dizaynı) elementlərinin – vizual strukturun, rənglərin, şriftlərin və interfeys komponentlərinin istifadəçi psixologiyasına təsiri təhlil olunur. Xüsusilə vizual illüziya, URL spoofing və interfeys təqlidi kimi metodlar araşdırılır. Google Docs fişinq hücumu real nümunə kimi təqdim edilərək dizayn manipulyasiyasının praktik təsiri göstərilir.**

Açar sözlər*— *sosial mühəndislik; kibertəhlükəsizlik; dizayn; fişinq; vizual manipulyasiya; insan faktoru.

I. GİRİŞ

Rəqəmsal transformasiya nəticəsində informasiya sistemlərinin mürəkkəbliyi artmış, bununla yanaşı kibercinayətlərin forması da dəyişmişdir. Əgər əvvəlki mərhələdə kiberhücumlar əsasən texniki boşluqlara yönəlirdisə, müasir dövrdə kiberhücumların əhəmiyyətli hissəsi insan davranışının manipulyasiyası üzərində qurulur. Bu kontekstdə sosial mühəndislik hücumları xüsusi aktuallıq kəsb edir.

Sosial mühəndislik hücumlarının effektivliyi insanın qərarvermə mexanizmlərinin xüsusiyyətləri ilə bağlıdır. nsanlar çox vaxt informasiyanı analitik deyil, intuitiv şəkildə emal edir və vizual elementlərə əsaslanaraq qərar verir. Bu xüsusiyyət "koqnitiv qısayollar" (heuristics) kimi tanınır və hücumçular tərəfindən aktiv şəkildə istismar olunur [1].

Dizayn isə bu prosesdə yalnız estetik funksiya daşımır, həm də psixoloji təsir vasitəsinə çevrilir. İstifadəçilər tanış interfeyslərə, loqolara və rəng sxemlərinə daha çox güvənirlər. Bu isə kibercinayətkarlara saxta mühit yaradaraq istifadəçiləri aldatmaq imkanı verir. Problemin mahiyyəti ondan ibarətdir ki, dizayn elementləri istifadəçi təhlükəsizliyini təmin etmək əvəzinə, əksinə, təhlükə mənbəyinə çevrilə bilir.

II. SOSİAL MÜHƏNDİSLİKDƏ İNTERFEYS DİZAYNIN PSİXOLOJİ VƏ MANİPULYATİV ROLU

Sosial mühəndislik hücumlarında istifadəçi interfeysinin vizual dizaynı (UI dizaynı) elementləri istifadəçinin qərarvermə prosesinə birbaşa təsir edən əsas psixoloji manipulyasiya vasitələrindən biridir. Koqnitiv psixologiya göstərir ki, insan beyninin qərarvermə sistemi iki əsas mexanizm üzərində qurulub: sürətli, intuitiv düşünmə və analitik, yavaş düşünmə. Sosial mühəndislik hücumları əsasən birinci mexanizmə yönələrək istifadəçinin emosional və vizual stimullara əsaslanan sürətli qərarlar verməsini təmin edir [1].

Daniel Kahnemanın nəzəriyyəsinə görə, insanlar qeyri-müəyyən və zaman təzyiqi altında olduqda analitik düşünməni minimuma endirir və vizual etibar siqnallarına əsaslanırlar [1]. Bu səbəbdən fişinq hücumları adətən vaxt məhdudiyyəti ("account will be suspended in 24 hours"), təhlükə mesajları ("unauthorized login detected") və vizual etibar elementləri ilə birlikdə təqdim olunur.

Robert Cialdininin təsir və inandırma prinsiplərinə əsasən, insanlar səlahiyyət (authority), sosial sübut (social proof) və məhdudluq (scarcity) kimi siqnallara avtomatik reaksiya verirlər [2]. Sosial mühəndislik interfeyslərində "Verified", "Secure", "Official Notice" kimi etiketlərin istifadəsi bu psixoloji mexanizmləri aktivləşdirərək istifadəçinin şübhə etmədən hərəkət etməsinə səbəb olur.

A. Rəng psixologiyası və vizual manipulyasiya

Rənglər insan emosional vəziyyətinə və davranışına güclü təsir göstərən vizual stimullardır. Araşdırmalar göstərir ki, mavi rəng etibar, sabitlik və peşəkarlıq hissi yaradır və bu səbəbdən maliyyə və texnologiya sektorlarında geniş istifadə olunur [3]. Kibercinayətkarlar da bu assosiasiyanı təqlid edərək saxta login səhifələrində eyni rəng palitrasından istifadə edirlər.

Yaşıl rəng isə təhlükəsizlik, icazəlilik və davametmə assosiasiyaları yaradır. Bu səbəbdən "Confirm", "Continue" və "Secure Payment" kimi düymələr çox vaxt yaşıl rəngdə dizayn olunur və istifadəçini hərəkətə keçməyə təşviq edir [3].

B. Koqnitiv yüklənmə və qərar yorğunluğu vasitəsilə manipulyasiya

Sosial mühəndislik hücumlarında istifadəçinin koqnitiv resurslarının məqsədli şəkildə yüklənməsi kibercinayətkarlar tərəfindən geniş istifadə olunan effektiv manipulyasiya strategiyasıdır. Koqnitiv yüklənmə nəzəriyyəsinə görə, insan beyninin eyni anda emal edə biləcəyi informasiya məhduddur və bu məhdudiyyət aşıldıqda qərarvermə keyfiyyəti azalır [4]. Kibercinayətkarlar istifadəçini çoxsaylı vizual elementlər, təcili xəbərdarlıqlar və paralel mesajlarla qarşı-qarşıya qoyaraq onun analitik düşünməsini zəiflədir və daha sürətli, intuitiv qərar verməyə yönləndirirlər.

Bununla yanaşı, qərar yorğunluğu (decision fatigue)

DOI: 10.25045/forensic.gov.2026.90

fenomeni də bu hücumlarda mühüm rol oynayır. Araşdırmalar göstərir ki, ardıcıl qərarlar vermək insanın diqqətini və özünü nəzarət qabiliyyətini azaldır, nəticədə sonrakı qərarlar daha impulsiv olur [5]. Bu məqsədlə kibercinayətkarlar istifadəçini "verify email", "confirm identity", "update password" kimi ardıcıl addımlardan ibarət saxta interfeyslərə yönləndirirlər.

Eyni zamanda, zəif strukturlaşdırılmış və manipulyativ dizayn istifadəçinin hərəkətləri düzgün qiymətləndirməsini çətinləşdirir. Bu cür interfeyslər istifadəçidə çaşqınlıq yaradır və yanlış qərar vermə ehtimalını artırır [6]. Nəticədə koqnitiv yüklənmə və qərar yorğunluğu birlikdə istifadəçinin idrak qabiliyyətini zəiflədərək onu manipulyasiyaya daha açıq hala gətirir.

C. Dark Patterns və manipulyativ UX dizayn

Müasir sosial mühəndislik yalnız klassik fişinq ilə məhdudlaşmır, həm də "dark patterns" adlanan manipulyativ istifadəçi interfeysi dizayn texnikalarından istifadə edir. "Dark patterns" istifadəçini şüurlu qərarından fərqli istiqamətə yönləndirmək üçün nəzərdə tutulmuş UX dizayn strategiyalarıdır.

Məsələn:

- Saxta təhlükəsizlik xəbərdarlıqları ("Your device is infected" pop-up-ları)
- Gizlədilmiş "cancel" düymələri (unsubscribe option-un görünməz edilməsi)
- Avtomatik seçimlər (default opt-in checkbox-lar)
- Saxta təcili vəziyyət mesajları ("Only 2 minutes left to secure your account")

Bu elementlər istifadəçinin diqqətini manipulyasiya edərək rasional qərarverməni zəiflədir və impulsiv davranışı gücləndirir [7].

D. Fişinq interfeyslərinin dizayn təqlidi

Müasir fişinq səhifələri real xidmətlərin UI dizaynını yüksək dəqiqliklə təqlid edir. Buraya aşağıdakılar daxildir:

- Brend loqolarının surətlərinin çıxarılması;
- Orijinal font və ikonların istifadəsi;
- HTTPS kilid simvolunun saxtalaşdırılması;
- Minimal dizayn və "clean UI" yanaşması.

Edward Tuftenin informasiya dizaynı nəzəriyyəsinə görə, yüksək vizual sadəlik və iyerarxiya istifadəçinin diqqətini kritik elementlərə yönləndirir [8]. Kibercinayətkarlar bu prinsipi manipulyativ şəkildə istifadə edərək istifadəçinin URL və təhlükəsizlik indikatorlarını yoxlamamasına səbəb olurlar.

Sosial mühəndislik hücumlarında dizayn istifadəçi davranışına birbaşa təsir edən əsas komponentlərdən biri olduğundan, eləcə də istifadəçilərin qərarvermə prosesi tez-tez emosional və vizual stimullara əsaslandığından dizayn elementləri manipulyasiya aləti kimi çıxış edir.

III. VİZUAL İLLÜZİYA VƏ URL SPOOFİNG:TEXNİKİ VƏ PSİXOLOJİ YANAŞMA

Vizual illüziya sosial mühəndislik hücumlarında ən geniş istifadə olunan texnikalardan biridir. İnsan beyni mətnləri hərflər üzrə deyil, bütöv vizual struktur kimi qəbul edir. Bu səbəbdən kiçik simvol dəyişiklikləri çox vaxt fərq edilmir.

Bu texnika "homograph attack" kimi tanınır və müxtəlif simvolların oxşarlığından istifadə etməyə əsaslanır. Məsələn:

- microsoft.com → rnicrosoft.com ("m" əvəzinə "r" və "n")
- apple.com → app1e.com ("l" əvəzinə "1")
- google.com → go0gle.com ("o" əvəzinə "0")
- paypal.com → paypaI.com ("l" əvəzinə böyük "I")
- amazon.com → amaz0n.com ("o" əvəzinə böyük "0")

Bu cür dəyişikliklər istifadəçi tərəfindən çox vaxt fərq edilmir və nəticədə istifadəçi saxta sayta daxil olur. Bu proses yalnız texniki deyil, həm də psixoloji əsaslara söykənir. İstifadəçi tanış söz formasını gördükdə avtomatik olaraq onu düzgün kimi qəbul edir.

Bundan əlavə, kibercinayətkarlar istifadəçiləri aldatmaq üçün yalnız saxta domenlərdən deyil, həm də alt domenlərin və mürəkkəb URL strukturlarının psixoloji təsirindən geniş şəkildə istifadə edirlər. Bu üsul vizual inandırıcılıq və struktur manipulyasiyası üzərində qurulur.

Məsələn, "secure-login.google.com.fake-site.ru" kimi bir URL ilk baxışda etibarlı Google giriş səhifəsi kimi görünə bilər. İstifadəçi adətən ünvanın başlanğıc hissəsinə, xüsusilə "google.com" ifadəsinə diqqət yetirdiyi üçün, əslində əsas domenin "fake-site.ru" olduğunu fərq etməyə bilər. Burada "google.com" yalnız alt domen kimi istifadə olunur [9].

Bu tip hücumlarda cinayətkarlar tez-tez brend adlarını URL-in daxilində yerləşdirərək saxta güvən hissi yaradır, uzun və qarışıq yol strukturları ilə əsas domeni gizlədir, həmçinin oxşar yazılışlı domenlərdən istifadə edərək istifadəçini çaşdırırlar. Bəzi hallarda isə TLS/SSL sertifikatından (HTTPS) istifadə etməklə saytın guya təhlükəsiz olduğu təəssüratını formalaşdırırlar, lakin bu, saytın legitim olmasına zəmanət vermir.

IV. TƏCRÜBİ NÜMUNƏ: GOOGLE DOCS FİŞİNQ HÜCUMU

2017-ci ildə baş vermiş Google Docs fişinq hücumu sosial mühəndislik və dizayn manipulyasiyasının ən təsirli real nümunələrindən biri hesab olunur. Hücum qısa zaman ərzində qlobal miqyasda yayılmış və milyonlarla istifadəçini hədəfə almışdır [10]. Hadisənin diqqətçəkən tərəfi texniki mürəkkəblikdən çox, istifadəçi etibarının və vizual dizaynın ustalıqla istismar olunması idi (Şəkil 1).

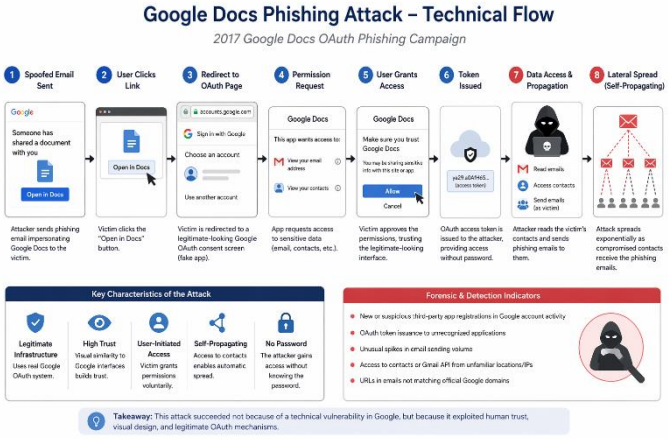
Hücumun mexanizmi yüksək səviyyədə sosial mühəndislik prinsiplərinə əsaslanırdı. İstifadəçilərə Google Docs xidmətindən gəlirmiş kimi görünən elektron poçtlar göndərilirdi. Bu mesajlar vizual baxımdan tam legitim təsir bağışlayırdı: rəsmi loqolar, mavi rəng palitrası, tipik düymə strukturu və interfeys elementləri orijinal dizaynla demək olar ki, identik idi. Bu cür yüksək səviyyəli vizual uyğunluq istifadəçidə etibarın ötürülməsi effekti (trust transfer) effekti yaradırdı [11].

Mesajın məzmunu da psixoloji baxımdan diqqətlə hazırlanmışdı. İstifadəçiyə guya ona sənəd paylaşımı edildiyi bildirilir və "Open in Docs" kimi tanış çağırış elementi təqdim olunurdu. Bu, istifadəçinin gündəlik davranış vərdişlərini (habitual interaction) aktivləşdirərək düşünmədən klik etməsinə səbəb olurdu. Klikdən sonra istifadəçi real Google login səhifəsinə çox bənzəyən, lakin əslində saxta olan icazə səhifəsinə yönləndirilirdi.

Hücumun ən təhlükəli və innovativ tərəfi isə OAuth əsaslı icazə mexanizminin istismar edilməsi idi. İstifadəçidən Google Docs kimi təqdim olunan saxta tətbiqə giriş icazəsi verməsi tələb olunurdu. İstifadəçi bu icazəni təsdiqlədikdə, kibercinayətkarlar onun elektron poçt kontaktlarına çıxış əldə edir və hücum avtomatik şəkildə istifadəçinin adından digər şəxslərə yayılırdı [12]. Bu, klassik parol oğurluğundan fərqli olaraq, legitim API icazələrinin manipulyasiyası ilə həyata keçirilən daha mürəkkəb hücum modeli idi.

Bu hadisədə dizayn manipulyasiyası həlledici rol oynamışdır. İstifadəçilər URL və təhlükəsizlik indikatorlarını yoxlamaq əvəzinə vizual uyğunluğa güvənmiş və nəticədə saxta interfeysi real sistem kimi qəbul etmişlər. Tədqiqatlar göstərir ki, istifadəçilər təhlükəsizlik qərarlarını çox vaxt texniki yoxlamalardan çox vizual siqnallar əsasında verirlər [13]. Bu da göstərir ki, hücumun uğuru texniki zəiflikdən deyil, insan faktorunun və dizaynın effektiv istismarından qaynaqlanmışdır.

Bundan əlavə, bu hücum "scalable social engineering" nümunəsi kimi də qiymətləndirilir. Yəni bir istifadəçinin komprometasiya olunması avtomatik olaraq digər istifadəçilərə hücumun yayılmasına səbəb olur. Bu cür zəncirvari yayılma modeli sosial mühəndislik hücumlarının təsir radiusunu eksponent şəkildə artırır və onları ənənəvi texniki hücumlardan daha təhlükəli edir [14].



Şəkil 1. Google Docs hücumunun vizual təsviri.

V. METODOLOGİYA

Bu tədqiqatda sosial mühəndislik hücumlarında dizaynın manipulyativ rolunun sistemli şəkildə araşdırılması üçün kompleks metodoloji yanaşma tətbiq edilmişdir. Araşdırma həm nəzəri, həm empirik, həm də tətbiqi səviyyələri əhatə edir və müxtəlif metodların inteqrasiyası vasitəsilə nəticələrin obyektivliyi və etibarlılığı təmin olunmuşdur. Tədqiqatın əsas məqsədi dizayn elementlərinin istifadəçi davranışına təsir mexanizmlərini müəyyənləşdirmək və bu təsirin kibertəhlükəsizlik kontekstində necə istismar olunduğunu təhlil etməkdir.

Metodoloji çərçivə əsasən keyfiyyət yönümlü yanaşmaya əsaslansa da, müəyyən mərhələlərdə kəmiyyət göstəricilərindən də istifadə edilmişdir. Bu yanaşma sosial mühəndislik kimi kompleks və çoxfaktorlu fenomenin daha dərindən anlaşılmasına imkan verir. Xüsusilə istifadəçi davranışının psixoloji və vizual stimullara reaksiyası interpretativ analiz vasitəsilə qiymətləndirilmişdir.

Məlumatların toplanması prosesi çoxmənbəli yanaşma əsasında həyata keçirilmişdir. İlk növbədə, sosial mühəndislik və kibertəhlükəsizlik sahəsində mövcud olan elmi ədəbiyyat sistemli şəkildə təhlil edilmişdir. Bu çərçivədə istifadəçi psixologiyası, qərarvermə mexanizmləri, UI/UX dizayn prinsipləri və fişinq hücumları ilə bağlı akademik mənbələr öyrənilmişdir. Eyni zamanda, real kibertəhlükə hadisələri və açıq mənbələrdə (open-source intelligence) yayımlanan hesabatlar araşdırılmışdır ki, bu da nəzəri yanaşmaların praktik kontekstdə yoxlanmasına imkan yaratmışdır.

Araşdırmanın mühüm hissəsini təşkil edən metodlardan biri müqayisəli interfeys analizidir. Bu mərhələdə orijinal və saxta veb interfeyslər vizual və funksional baxımdan müqayisə edilmişdir. Analiz zamanı rəng palitrası, şrift seçimi, düymələrin yerləşdirilməsi, loqo istifadəsi və ümumi dizayn strukturu kimi elementlər diqqət mərkəzində olmuşdur. Bu yanaşma göstərmişdir ki, yüksək vizual oxşarlıq istifadəçi etibarını artıran əsas faktorlardan biridir və hücumların uğur ehtimalını əhəmiyyətli dərəcədə yüksəldir.

Bununla yanaşı, vizual illüziya və URL manipulyasiyası texnikalarının analizi də aparılmışdır. Bu prosesdə müxtəlif saxta domen nümunələri üzərində semantik və qrafik oxşarlıqlar araşdırılmış, istifadəçi tərəfindən qəbul edilən vizual strukturun necə təhrif olunduğu müəyyən edilmişdir. Analiz göstərir ki, istifadəçilər çox vaxt simvol səviyyəsində deyil, ümumi forma səviyyəsində qavrayış həyata keçirirlər ki, bu da homoqraf hücumlarının effektivliyini izah edir.

Tədqiqatın praktik hissəsində real hadisə təhlili (case study) mühüm yer tutur. Xüsusilə Google Docs fişinq hücumu nümunəsi üzərində aparılan analiz dizayn manipulyasiyasının real mühitdə necə tətbiq olunduğunu göstərmək məqsədi daşıyır. Bu hadisə çərçivəsində hücumun strukturu, istifadə olunan dizayn elementləri və istifadəçi reaksiyaları təhlil edilmişdir. Bu yanaşma nəzəri nəticələrin real ssenarilərlə uyğunluğunu yoxlamağa imkan vermişdir.

Əlavə olaraq, istifadəçi davranışının modelləşdirilməsi üçün koqnitiv yanaşmadan istifadə edilmişdir. Bu mərhələdə insanın qərarvermə prosesində istifadə etdiyi heuristik mexanizmlər nəzərə alınmış və onların dizayn vasitəsilə necə manipulyasiya edildiyi izah olunmuşdur. Xüsusilə "etibar heuristikası" və "vizual uyğunluq effekti" kimi anlayışlar bu kontekstdə əsas rol oynamışdır.

Nəticələrin etibarlılığını təmin etmək məqsədilə triangulyasiya metodundan istifadə edilmişdir. Bu metod müxtəlif məlumat mənbələrinin və analiz üsullarının birləşdirilməsini nəzərdə tutur. Beləliklə, həm nəzəri mənbələr, həm real hadisələr, həm də vizual analiz nəticələri qarşılıqlı şəkildə yoxlanılmış və ümumiləşdirilmişdir.

Ümumilikdə tətbiq olunan metodologiya sosial mühəndislik hücumlarında dizaynın rolunu kompleks şəkildə araşdırmağa imkan vermişdir. Bu yanaşma həm nəzəri anlayışların dərinləşdirilməsinə, həm də praktik təhlükəsizlik tədbirlərinin formalaşdırılmasına töhfə verir.

NƏTİCƏ

Aparılmış tədqiqatın nəticələri göstərir ki, sosial mühəndislik hücumlarında dizayn yalnız əlavə estetik element kimi deyil, əksinə, hücumun əsas strukturunu formalaşdıran strateji manipulyasiya vasitəsi kimi çıxış edir. Vizual uyğunluq prinsipi, simvol səviyyəsində aparılan kiçik dəyişikliklər və interfeys təqlidi istifadəçinin qərarvermə prosesini birbaşa təsir göstərir və onun kritik düşünmə mexanizmini zəiflədir.

Araşdırma göstərir ki, istifadəçilər rəqəmsal mühitdə informasiyanı qiymətləndirərkən daha çox vizual siqnallara və tanış dizayn elementlərinə əsaslanırlar. Bu isə "etibar illüziyası" yaradır və istifadəçinin təhlükəni dərk etmədən hərəkət etməsinə səbəb olur. Nəticə etibarilə, dizaynın psixoloji təsir gücü sosial mühəndislik hücumlarının effektivliyini artıran əsas faktorlardan birinə çevrilir.

Eyni zamanda, simvol manipulyasiyası və URL spoofing kimi texnikaların geniş istifadəsi göstərir ki, kibercinayətkarlar yalnız texniki boşluqlardan deyil, insan qavrayışının məhdudiyyətlərindən də istifadə edirlər. İstifadəçinin mətnləri bütöv forma kimi qavraması kiçik dəyişikliklərin çox vaxt nəzərdən qaçmasına səbəb olur və bu da təhlükənin aşkarlanmasını çətinləşdirir.

Sosial mühəndislik hücumlarının qarşısının alınması yalnız texniki təhlükəsizlik həlləri ilə mümkün deyil. Firewall, antivirus və şəbəkə monitorinq sistemləri müəyyən səviyyədə qoruma təmin etsə də, insan faktoruna yönəlmiş hücumlar bu müdafiə mexanizmlərini asanlıqla aşaraq istifadəçi səviyyəsində uğur qazana bilir. Buna görə də kibertəhlükəsizlik strategiyaları daha geniş yanaşma tələb edir.

İstifadəçilərin fişinq hücumlarını tanıma bacarıqlarının artırılması, şübhəli interfeyslərin identifikasiyası və vizual təhlükələrin dərk edilməsi hücumların effektivliyini əhəmiyyətli dərəcədə azalda bilər. Eyni zamanda, təhlükəsiz dizayn prinsiplərinin tətbiqi, məsələn, interfeyslərdə daha aydın autentifikasiya siqnalları, standartlaşdırılmış xəbərdarlıq elementləri və istifadəçi yönümlü təhlükəsizlik indikatorları bu sahədə mühüm rol oynayır.

Digər vacib məqam ondan ibarətdir ki, müasir kibertəhlükəsizlik yanaşmaları dizayn və psixologiyanın inteqrasiyasına əsaslanmalıdır. İnsan davranışının vizual və emosional stimullara reaksiyası nəzərə alınmadan yaradılan təhlükəsizlik sistemləri tam effektiv ola bilmir. Buna görə də UI/UX dizayn prinsipləri ilə kibertəhlükəsizlik mexanizmlərinin birgə işlənməsi zəruridir.

Nəticə etibarilə, sosial mühəndislik hücumları kontekstində dizayn yalnız texniki interfeys komponenti deyil, həm də psixoloji təsir aləti kimi çıxış edir. Bu səbəbdən gələcək tədqiqatlarda insan-kompüter qarşılıqlı təsirinin daha dərindən öyrənilməsi, vizual qavrayış mexanizmlərinin analizi və adaptiv təhlükəsizlik dizayn modellərinin hazırlanması mühüm istiqamət kimi çıxış etməlidir.

ƏDƏBİYYAT

[1] D. Kahneman, Thinking, Fast and Slow. New York, NY, USA: Farrar, Straus and Giroux, 2011.

[2] R. B. Cialdini, Influence: The Psychology of Persuasion. New York, NY, USA: Harper Business, 2007.

[3] A. J. Elliot and M. A. Maier, "Color psychology: Effects of perceiving color on psychological functioning in humans," Annu. Rev. Psychol., vol. 65, pp. 95–120, Jan. 2014.

[4] J. Sweller, "Cognitive load during problem solving," Cogn. Sci., vol. 12, no. 2, pp. 257–285, 1988.

[5] R. F. Baumeister and J. Tierney, Willpower: Rediscovering the Greatest Human Strength. New York, NY, USA: Penguin Press, 2011.

[6] D. A. Norman, The Design of Everyday Things, revised ed. New York, NY, USA: Basic Books, 2013.

[7] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in Proc. CHI Conf. Human Factors Comput. Syst. (CHI '18), Montreal, QC, Canada, 2018, pp. 1–14.

[8] E. R. Tufte, Envisioning Information. Cheshire, CT, USA: Graphics Press, 1990.

[9] M. Jakobsson and S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Hoboken, NJ, USA: Wiley, 2006.

[10] "Protecting against phishing attacks," Google Security Blog, 2017. [Online]. Available: https://security.googleblog.com

[11] B. Krebs, "Phishing attack impersonates Google Docs," Krebs on Security, May 2017. [Online]. Available: https://krebsonsecurity.com

[12] "Alert (TA17-132A): Google Docs Phishing Campaign," US-CERT (CISA), Tech. Rep., May 2017.

[13] NIST, "Security and privacy considerations for end users," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2019.

[14] ENISA, "Threat Landscape Report," European Union Agency for Cybersecurity, Athens, Greece, Tech. Rep., 2020.

Analysis of Manipulative Influence Mechanisms of Social Engineering Attacks on User Behavior

Gular Hamzazade
Azerbaijan University of Architecture and Construction,
Baku, Azerbaijan
hemzezadeguler@gmail.com

Abstract- In the modern digital environment, the nature of cyber threats has shifted from technical vulnerabilities to a greater focus on the human factor. Social engineering attacks are based on manipulating user behavior, and design plays a crucial role in this process. This article analyzes the impact of design elements - such as visual structure, colors, typography, and interface components on user psychology. In particular, methods such as visual illusion, URL spoofing, and interface imitation are examined. The Google Docs phishing attack (2017) is presented as a real case study to demonstrate the practical impact of design manipulation.

Keywords- social engineering; cybersecurity; design; phishing; visual manipulation; human factor.