

“Bravo Endirim Kartı” phishing hücumunun planlaşdırılması və icrası

11.05.2025

Kim tərəfindən: Nikitina Almaz

Kimə: Qasımov Zaur

Mündəricat

Hücumun məqsədi.....	3
Hədəf.....	3
Hücum tipi.....	3
İcra prosesi.....	4
Qurbanların reaksiyaları.....	10
Nəticə.....	12

1.Hücumun Məqsədi

Bu təcrübənin əsas məqsədi kibertəhlükəsizlik sahəsində fişinq (phishing) hücumlarının necə həyata keçirildiyini dərinlən anlamaq, onların texniki və psixoloji mexanizmlərini öyrənmək, həmçinin bu cür hücumlara qarşı fərdi səviyyədə hansı müdafiə tədbirlərinin görülmə biləcəyini praktik formada təhlil etməkdir.

Bu təcrübə çərçivəsində real həyatdakı fişinq ssenariləri modelləşdirilmiş, qurban kimi seçilən şəxs üçün inandırıcı bir veb sahifə hazırlanaraq ona sosial mühəndislik üsulu ilə təzyiq göstərilmişdir. Təcrübə iştirakçısının şəxsi və maliyyə məlumatlarını könüllü şəkildə daxil etməsi üçün dizayn edilmiş bu ssenari, informasiya təhlükəsizliyi biliklərinin yalnız nəzəri yox, praktik formada mənimsənilməsinə şərait yaratmışdır.

Digər məqsədlər:

- Sosial mühəndislik texnikalarının insan davranışlarına təsirini müşahidə etmək;
- Real fişinq hücumunun dizaynı və tətbiqi prosesində istifadə olunan vasitələrlə tanış olmaq (domain alma, veb sayt qurulması, mesajların göndərilməsi və s.);
- İnsanlara texnoloji savadsızlığın təhlükəli nəticələrini göstərərək maarifləndirmə aparmaq.

Sonda məqsəd yalnız texniki bilikləri artırmaq deyil, həm də təhlükəsizliyin şəxsi və ictimai məsuliyyət olduğunu aşılamaqdır.

2.Hədəf

- **Qurban:** Simulyasiya məqsədilə yaxın ətrafım seçildi.
- **Məqsəd:** Onların kart məlumatlarını və əlaqə vasitələrini ələ keçirmək və sonradan ona phishing haqqında məlumat verərək maarifləndirmək.

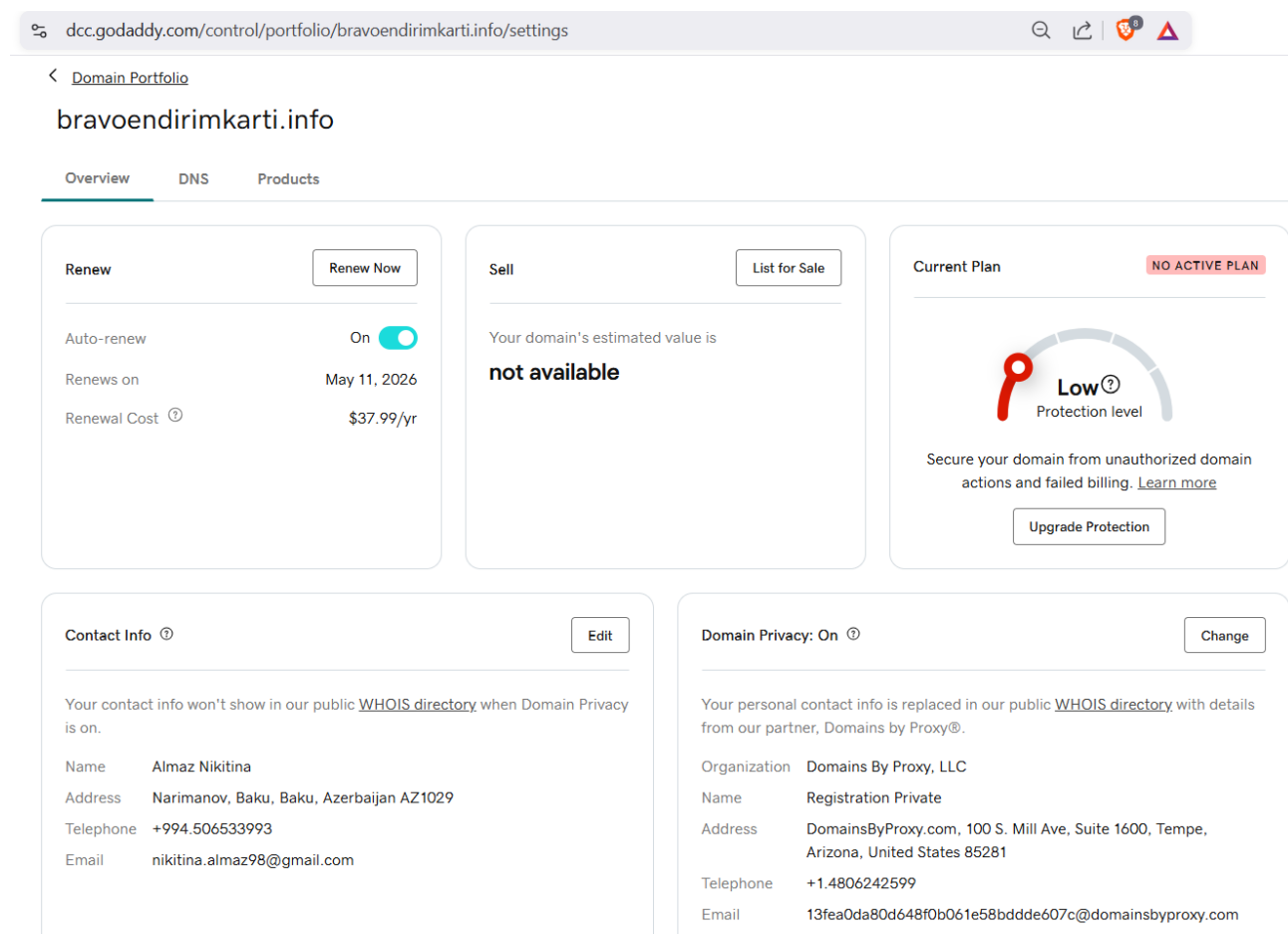
3.Hücum Tipi

Bu simulyasiya **spear-phishing** (hədəfli fişinq) hücumu kimi hazırlanıb. Hücum ssenarisində istifadəçiyə Bravo Supermarketin guya 200 AZN-lik hədiyyə kartı kampaniyasında qalib gəldiyi bildirilir və onu məlumatlarını daxil etməyə təşviq edən saxta veb sahifəyə yönləndirilir.

4. İcra prosesi

4.1. Domenin alınması

Simulyasiya çərçivəsində istifadə ediləcək fişinq səhifəsinin real domen üzərindən yayımlanması üçün ilk növbədə **GoDaddy** platformasından xüsusi fişinq məqsədilə seçilmiş bir domen (bravoendirimkarti.info) qeydiyyatdan keçirilmişdir. Domenin peşəkar görünməsi və istifadəçilərə daha inandırıcı təsir bağışlaması üçün **məşhur marka (Bravo)** adı daxil edilmiş və **.info** kimi universal, lakin qeyri-kommersiya izlenimi verən domen uzantısından istifadə olunmuşdur. Bu, səhifənin "kampaniya saytı" kimi görünməsini asanlaşdırırdı.



Screenshot of the GoDaddy domain settings page for **bravoendirimkarti.info**.

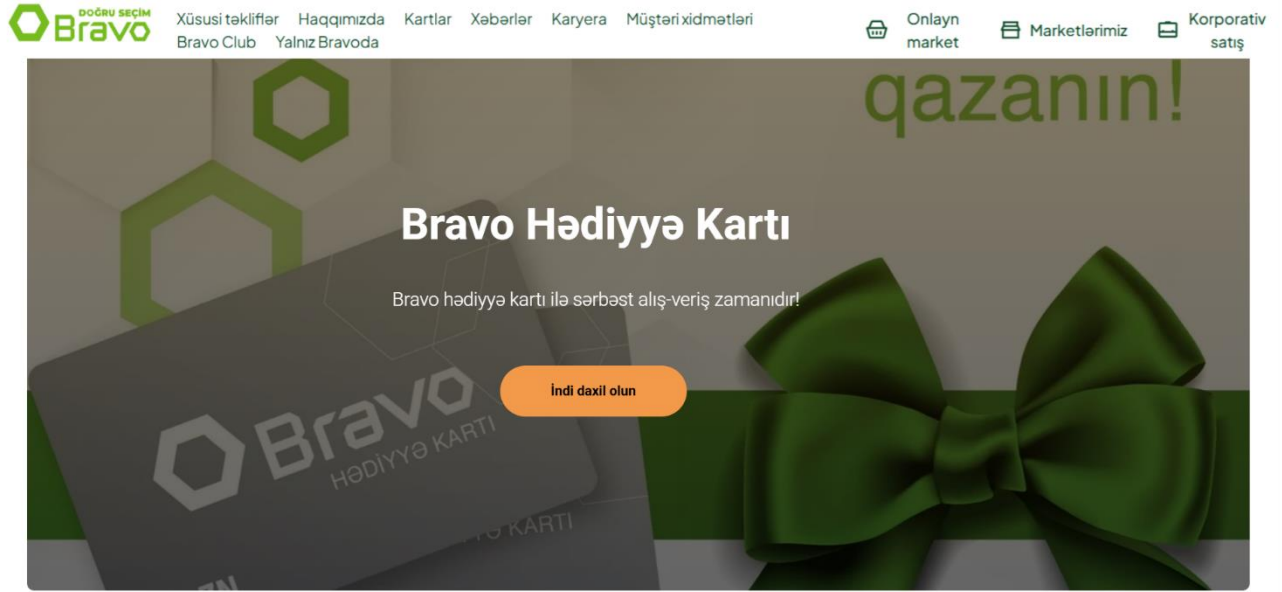
The page shows the following sections:

- Renew:** Includes a "Renew Now" button, an "Auto-renew" toggle (On), "Renews on" date (May 11, 2026), and "Renewal Cost" (\$37.99/yr).
- Sell:** Includes a "List for Sale" button. The domain's estimated value is **not available**.
- Current Plan:** Shows a "NO ACTIVE PLAN" status. A gauge indicates a "Low" protection level. A message states: "Secure your domain from unauthorized domain actions and failed billing. [Learn more](#)". An "Upgrade Protection" button is present.
- Contact Info:** Includes an "Edit" button. The contact information is: Name: Almaz Nikitina, Address: Narimanov, Baku, Baku, Azerbaijan AZ1029, Telephone: +994.506533993, Email: nikitina.almaz98@gmail.com.
- Domain Privacy:** Includes a "Change" button. The privacy details are: Organization: Domains By Proxy, LLC, Name: Registration Private, Address: DomainsByProxy.com, 100 S. Mill Ave, Suite 1600, Tempe, Arizona, United States 85281, Telephone: +1.4806242599, Email: 13fea0da80d648f0b061e58bddde607c@domainsbyproxy.com.

4.2. Veb səhifənin hazırlanması

- Sayt dizaynı üçün **Tilda.cc** platformasından istifadə etdim.

- Rəsmi **Bravo Supermarket** saytına bənzər dizayn və interfeys yaratdım.



- Saytda istifadəçinin daxil etməsi üçün aşağıdakı sahələr yerləşdirildi:
 - Ad, soyad
 - Elektron poçt
 - Mobil nömrə
 - Kart nömrəsi
 - Son istifadə tarixi
 - CVV kodu

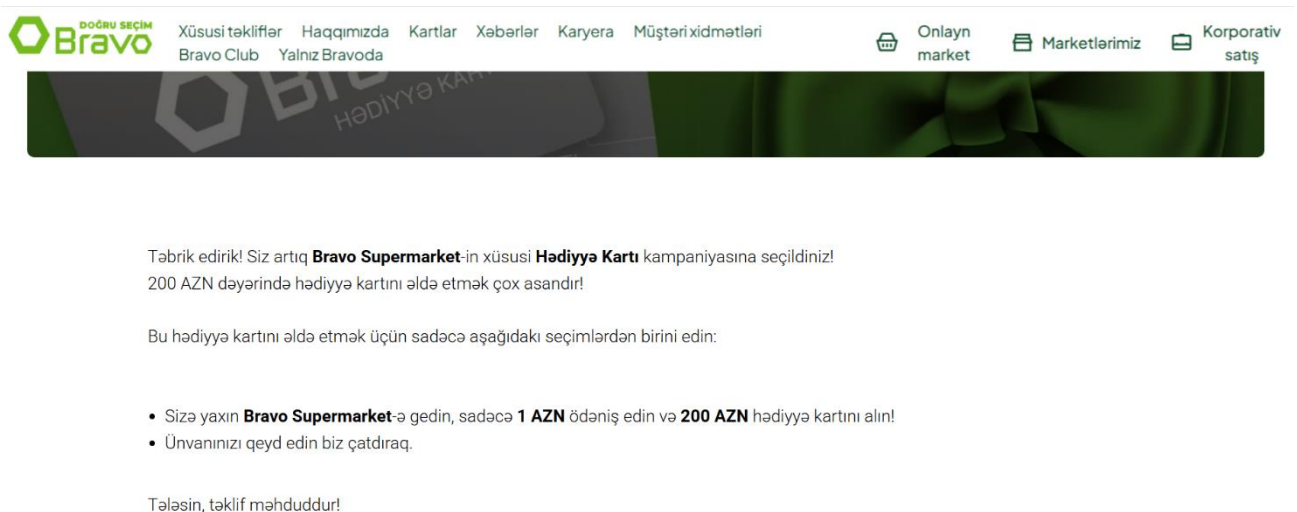
The image shows a registration form on the Bravo Supermarket website. The form is located below the navigation bar and consists of several input fields. The first field is labeled 'Ad Soyad' and contains the placeholder text 'Ad Soyad'. The second field is labeled 'E-poçt' and contains the placeholder text 'E-poçt'. The third field is labeled 'Əlaqə nömrəsi' and contains the placeholder text 'Əlaqə nömrəsi'. The fourth field is labeled 'Kart Məlumatları' and contains the placeholder text '0000 0000 0000 0000'. Below this field is a 'Date' field. The final field is labeled 'CVV'. At the bottom of the form is a black button with the text 'Göndər'.

- Saytın görünüşü real görünməsi üçün SSL nişanları, Bravo loqosu və kampaniya şəkilləri ilə gücləndirildi.



4.3. İstifadəçiyə seçim təqdim olundu

- Saytda istifadəçiyə 2 seçim təklif olundu:
 1. Kartı onlayn sifariş etmək
 2. Bravo filialına yaxınlaşıb şəxsən almaq



- Məqsəd: istifadəçinin öz istəyi ilə kart məlumatlarını daxil etməsinə nail olmaq.

4.4. Domenin sayta qoşulması

Domen alındıqdan sonra onu **Tilda.cc** platformasında hazırlanmış fişinq səhifəsinə yönləndirmək üçün aşağıdakı texniki addımlar yerinə yetirilmişdir:

- GoDaddy idarəetmə panelində DNS ayarlarına daxil olunaraq:
 - **A rekord** olaraq Tilda-nın verdiyi IP adresi (176.57.65.48) əlavə edildi.
 - **CNAME rekord** olaraq www üçün **bravoendirimkarti.info** ünvanı qeyd olundu.
- Tilda interfeysində “Domain connection” bölməsində domen adı daxil edilərək bağlantı quruldu.
- Tilda sistemində domen bağlantısının aktiv olduğunu bildirən status təsdiqləndikdən sonra sayt real domen üzərindən əlçatan oldu.

Bu konfigurasiya nəticəsində istifadəçi linkə daxil olduqda Tilda platformasında hazırlanmış fişinq səhifəsinə yönləndirilir, lakin bu qurbanların gözündə real və orijinal kampaniya səhifəsi kimi görünür.

4.5. Məlumatların İnformasiya Kanallarına İnteqrasiyası

Fişinq səhifəsinin effektivliyini artırmaq və istifadəçilərin daxil etdiyi şəxsi məlumatların (ad, soyad, kart nömrəsi, CVV və s.) real vaxtda əldə olunması üçün **Tilda** platformasının **form builder** funksiyasından istifadə olunmuşdur. Səhifəyə əlavə edilmiş bu forma, “Bravo” marketin hədiyyə kartı qazanılması üçün doldurulmalı olan qeydiyyat forması kimi təqdim edilmişdir.

4.5.1 Telegram ilə əlaqələndirmə

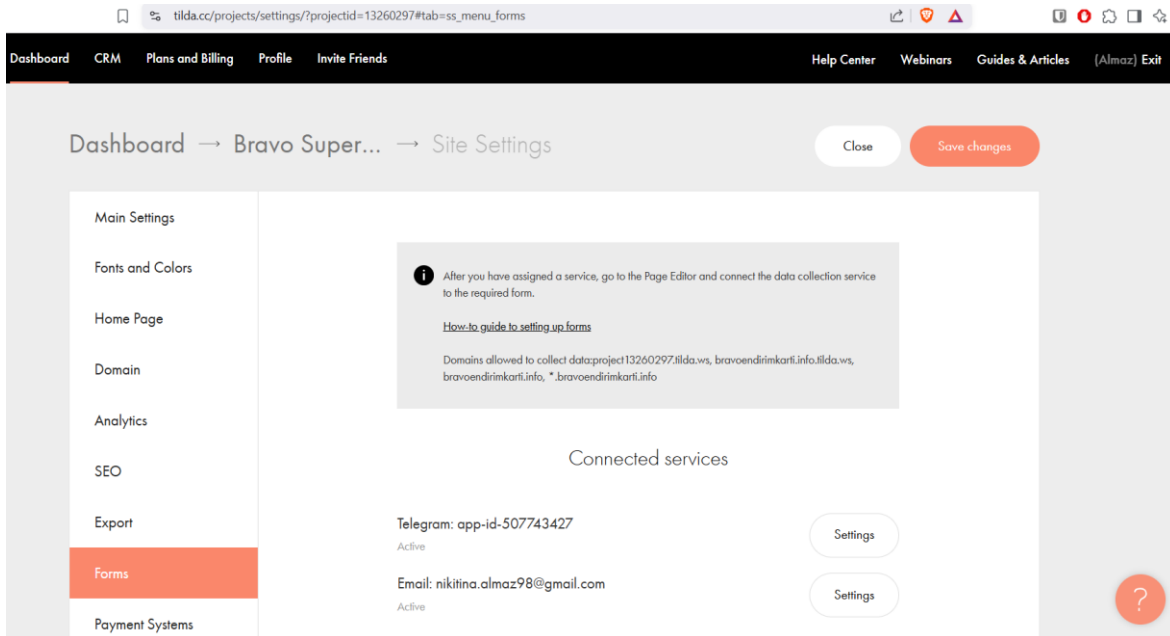
- Tilda-nın forma ayarlarında “Connect Telegram bot” funksiyası aktiv edildi.
- Telegram botun API token-i Tilda hesabına daxil edilərək məlumatlar real vaxtda öz şəxsi Telegram hesabına yönləndirildi.
- Bu sayədə, kimsə formu doldurduğu an ani bildiriş şəklində məlumatlar mənə çatırdı.

4.5.2 Gmail hesabı ilə əlaqələndirmə

- Tilda form ayarlarında “Send to Email” seçimi aktiv edildi.
- Qurbanlardan gələn məlumatların ikinci nüsxəsi təsis etdiyim Gmail ünvanına yönləndirildi.

- Bu üsulla, məlumatlar həm təhlükəsizlik baxımından arxivləndi, həm də əgər Telegram işləməsə alternativ kanal kimi xidmət göstərdi.

Bu konfigurasiya nəticəsində qurbanların daxil etdiyi həssas məlumatlar heç bir təhlükəsizlik xəbərdarlığı ilə qarşılaşmadan güvənli interfeys vasitəsilə mənim nəzarətimdə olan kanallara ötürülürdü.



4.6. Fişinq Hücümünün Yayılması (SMS vasitəsilə linkin ötürülməsi)

Sosial mühəndislik hücumunun əsas məqsədi hədəf şəxsləri fişinq səhifəsinə yönləndirmək və onların şəxsi/kart məlumatlarını könüllü şəkildə təqdim etməsinə nail olmaq idi. Bu məqsədlə hücumun yayılma mərhələsi aşağıdakı kimi həyata keçirildi:


4.6.1. e-SIM Alınması

- Hücumun anonim həyata keçirilməsi və şəxsi nömrənin ifşa olunmaması üçün Azercell mobil operatorunun rəsmi veb saytı üzərindən e-SIM əldə olundu.
- Bu e-SIM aktivləşdirildikdən sonra “Azercell Kabinetim” tətbiqinə daxil olundu və həmin nömrə üçün “vəb SMS” funksiyası istifadə edildi.

Veb SMS

Bu günə **92** ölkədaxili **mesajların** (1 SMS = 0.10 ₼) qalıb. Onlardan **4** şəbəkədaxili mesaj **pulsuzdur**.

 +994

Telefon nömrəsi 

0/9

Latin əlifbasından istifadə edərək mesaj yaz

148/148

4.6.2. Mesajın Hazırlanması və Yayılması

- Fişinq linkinin yerləşdiyi SMS mətnində şəxsi məlumat istənilməmiş, əksinə qurbanın hədiyyə qazandığı vurğulanmışdı.
- Mesaj məzmunu belə idi:

"Təbriklər! Bravo Supermarket sizə 200 AZN-lik Hədiyyə Kartı təqdim edir! Kartınızı əldə etmək üçün linkə daxil olun: <https://bravoendirimkarti.info/>"

- Bu cür yazı tərzini istifadəçidə təhlükə təəssüratı yaratmır, əksinə sürətli reaksiya və maraq doğurur.

4.6.3. Mesajların Göndərilməsi

- Azercell-in Web SMS sistemi vasitəsilə eyni anda bir neçə kontakt nömrəsinə bu mesaj göndərildi.
- Mətn qısa və inandırıcı tərzdə yazıldığından, etibar doğurdu və klikləmə faizi yüksək oldu.

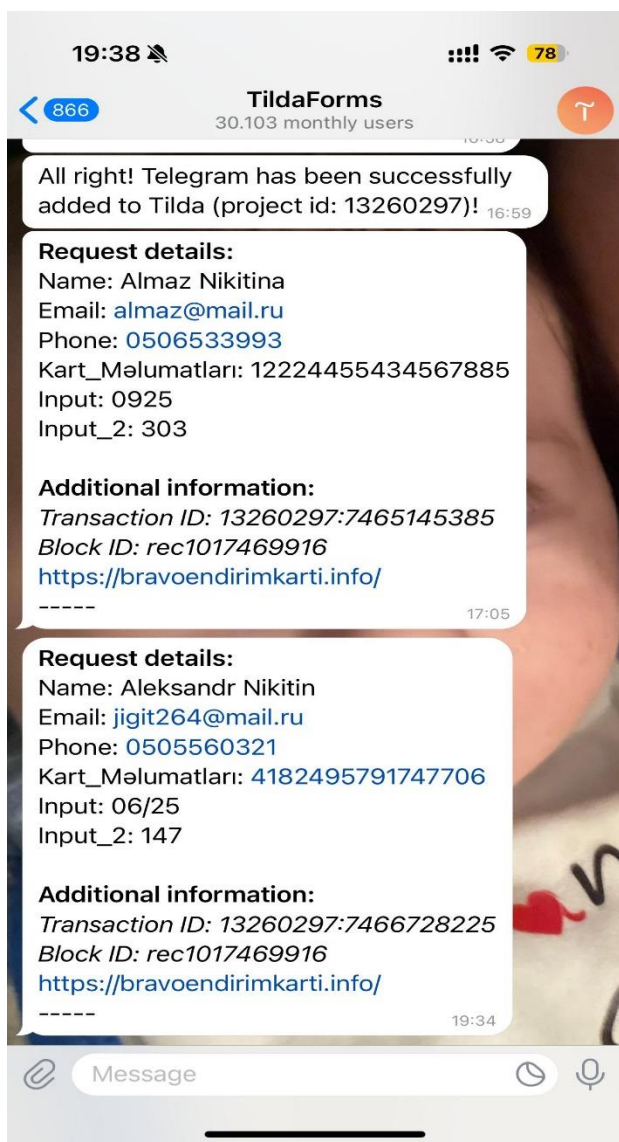


5. Qurbanların reaksiyaları

Hazırlanmış fişinq səhifəsi və yönləndirmə üsulu nəticəsində müxtəlif reaksiyalar müşahidə olundu. Bu reaksiyalar təhlil edilərək gələcəkdə sosial mühəndislik və istifadəçi maarifləndirilməsi sahəsində hansı boşluqların olduğunu aydın görmək mümkün oldu.

5.1 Reallaşan Fişinq Hadisəsi

- Göndərilən SMS-lərdən biri yaxın tanışlardan birinə çatdı və o, linkə klik edərək fişinq səhifəsinə daxil oldu.
- Fişinq səhifəsində ona 200 AZN-lik hədiyyə kartını əldə etmək üçün ad, soyad, email ünvanı və kart məlumatlarını daxil etməsi təklif olundu.
- İstifadəçi heç bir əlavə şübhəyə düşmədən bütün tələb olunan məlumatları təqdim etdi.
- Daxil edilən kart məlumatları (ad, kart nömrəsi, son istifadə tarixi və CVV) tərtibçi tərəfindən əvvəlcədən təyin edilmiş Telegram və Gmail hesabına avtomatik göndərildi.



 **noreply@tilda.ws** 19:34 [Unsubscribe](#) ...
to me ▾

Request details:

Name: Aleksandr Nikitin
Email: jigit264@mail.ru
Phone: 0505560321
Kart_Məlumatları: 4182495791747706
Input: 06/25
Input_2: 147

 **noreply@tilda.ws** 17:05 [Unsubscribe](#) ...
to me ▾

Request details:

Name: Almaz Nikitina
Email: almaz@mail.ru
Phone: 0506533993
Kart_Məlumatları: 12224455434567885
Input: 0925
Input_2: 303

5.2. Reaksiyaların Təhlili

Fişinq linkini alan şəxslərin reaksiyaları əsasən aşağıdakı kateqoriyalara bölündü:

Reaksiya növü	Təxmini faiz	Müşahidə
Linkə klik edib məlumat daxil edənlər	10-15%	Aşağı məlumatlılıq və etibar
Linkə klik edib tezliklə tərk edənlər	40%	Ehtiyatlılıq və şübhə
Heç klik etməyənlər	45-50%	Qətiyyətli və məlumatlı istifadəçilər

6. Nəticə

Aparılan fişinq simulyasiyası göstərdi ki, sosial mühəndislik üsulları vasitəsilə istifadəçiləri aldadaraq onların şəxsi və maliyyə məlumatlarını əldə etmək real və effektiv bir təhdiddir. Təcrübə göstərdi ki, tanınmış brend adı (Bravo), cazibədar və inandırıcı təklif (200 AZN-lik hədiyyə kartı) və vizual olaraq orijinala bənzəyən veb sahifə istifadəçilərdə güvən hissi yaradaraq onların diqqətini azaltmağa və məlumat paylaşmasına səbəb ola bilər.

Simulyasiyanın nəticələrinə əsasən:

- Məlumat daxil edən istifadəçilərin sayı az olsa da, bu onların fişinq riskinə qarşı yetərinə məlumatlandırma işlərini göstərdi.
- Təhlükəsizliklə bağlı kritik məlumatların qorunması üçün məlumatlandırma işləri daha çox fərdi və situasiya əsaslı olmalıdır.
- İstifadəçilərin bu kimi hücumlara qarşı həm texniki, həm də psixoloji olaraq hazır olması vacibdir.

Bu praktika real dünyada istifadə olunan fişinq hücumlarını modeləşdirərək gələcəkdə belə hallar qarşısında daha ayıq və təmkinli davranmaq üçün əhəmiyyətli bir təlim funksiyası yerinə yetirdi.