PEŞƏKAR İNKIŞAF TƏLIMI

Cyberforward: Təhlükəsiz Rəqəmsal Gələcəyə Doğru

Təhdid landşaftından süni intellektə qədər — müasir kibertəhlükəsizlik mənzərəsinin əhatəli icmalı

Təlimçi: Tahir Qurbanov

TƏLIM PLANI

Bugünkü Gündəlik

01 Müasir Kiber Təhdid Landşaftı və Hücum Trendləri

Cari mənzərə və statistika

02 Sosial Mühəndislik: İnsan Faktorunun İstismarı

Psixologiya və manipulyasiya taktikaları

03 Rəqəmsal Şəxsiyyət və Məlumat Təhlükəsizliyi

Autentifikasiya və məlumatların qorunması

04 Süni İntellekt: Yeni Risklər və Müdafiə İmkanları

AI-əsaslı hücumlar və müdafiə

05 Kiberdayanıqlılıq və Təhlükəsizlik Mədəniyyəti

Təşkilati hazırlıq və davamlılıq

01 Müasir Kiber Təhdid Landşaftı və Hücum Trendləri

Kibertəhlükəsizlik mühitinin necə dəyişdiyini və bu gün ən çox rast gəlinən hücum formalarını nəzərdən keçiririk

GIRIŞ

Təhdid Landşaftı Niyə Sürətlə Dəyişir?

KONTEKST

Rəqəmsal transformasiya, süni intellektin inkişafı, uzaqdan iş modeli və bulud xidmətlərinin artması hücum səthini genişləndirib.
Kibercinayətkarlar artıq daha mütəşəkkil, maliyyə baxımından güclü və texnoloji cəhətdən inkişaf etmiş qruplar şəklində fəaliyyət göstərir.

ƏSAS AMILLƏR

- **Genişlənən hücum səthi**

  Bulud, mobil və IoT cihazları yeni zəiflik nöqtələri yaradır.

- **Kibercinayətin sənayeləşməsi**

  Ransomware-as-a-Service kimi modellər hücumları asanlaşdırır.

- **Geosiyasi gərginlik**

  Dövlət dəstəkli qruplar kritik infrastrukturu hədəf alır.

HİSSƏ 1

Bugünkü təhdid landşaftı: 5 əsas istiqamət

Müasir hücumlar tək vektorla deyil, kombinə olunmuş ssenarilərlə gəlir.

01 Ransomware + data extortion

Faylların şifrələnməsi ilə yanaşı məlumat sızdırma təzyiqi artır.

02 Credential abuse

Zəif/yenidən istifadə olunan parollar və token/sessiya oğurluğu giriş qapısıdır.

03 Exploited vulnerabilities

VPN, edge cihazları və internetə açıq servislər sürətli hədəfə çevrilir.

04 Supply-chain compromise

Bir vendor və ya inteqrasiya xətası bir çox təşkilata təsir edə bilər.

05 AI-enabled attacks

Phishing, deepfake və avtomatlaşdırılmış kəşfiyyat daha inandırıcı olur.

Mənbələr: ENISA Threat Landscape 2025; Verizon DBIR 2025; IBM Cost of a Data Breach 2025.

TƏSNIFAT

Əsas Hücum Növləri

1

Ransomware

Məlumatları şifrələyib fidyə tələb edən zərərli proqram növü; biznes fəaliyyətini tam dayandıra bilir.

2

Fişinq və Sosial Mühəndislik

İstifadəçini aldadaraq həssas məlumat və ya giriş icazəsi əldə etmək.

3

DDoS Hücumları

Xidməti həddindən artıq trafiklə yükləyərək əlçatmazlığa səbəb olmaq.

4

Tədarük Zənciri Hücumları

Etibarlı üçüncü tərəf proqram və ya xidmət vasitəsilə sistemə sızma.

HİSSƏ 1

Trend siqnalları: nəyə görə ciddi yanaşmalıyıq?

Rəqəmlər təhlükənin “abstrakt” olmadığını göstərir.

44%

ransomware breach-lərdə görünür

~60%

human element breach-lərdə rol oynayır

30%

third-party involvement səviyyəsinə çatıb

97%

AI breach-lərdə access control çatışmazlığı

→ Təlim üçün interpretasiya

Bu göstəricilər “hamı riskdədir” demək deyil; daha dəqiq olaraq riskin insan davranışı, giriş hüquqları, təchizat zənciri və AI idarəetməsi ətrafında cəmləndiyini göstərir.

★ Rəhbərlik üçün interpretasiya

Büdcə yalnız alətə deyil, ölçülə bilən risk azaltmağa yönəlməlidir: MFA, patching, loglama, backup, təlim, vendor nəzarəti və incident response.

Verizon DBIR 2025; IBM Cost of a Data Breach 2025.

STATISTIKA

Rəqəmlərlə Qlobal Mənzərə

+72%

Son illərdə məlumat sızması hadisələrinin sayında artım

11 san.

Dünyada hər 11 saniyədə bir yeni ransomware hücumu baş verir

82%

Uğurlu hücumların insan səhvi ilə əlaqəli olması

Qeyd: Rəqəmlər sənaye hesabatlarının ümumi tendensiyalarını əks etdirən illüstrativ göstəricilərdir və təlim məqsədləri üçün təqdim olunur.

HİSSƏ 1

Hücum necə inkişaf edir?

Tək klik hadisə deyil; çoxmərhələli zəncirin başlanğıcı ola bilər.

Recon
Açıq mənbələrdən məlumat toplanır

Initial Access
Phishing, zəiflik, credential

Execution
Malware, script, token istifadə

Privilege
İcazələr artırılır

Lateral
Daxildə hərəkət

Impact
Şifrələmə/sızma /dayanma

Müdafiə fikri

Zəncirin hər mərhələsində “aşkarlama və kəsmə nöqtəsi” olmalıdır: istifadəçi xəbərdarlığı, MFA, EDR, SIEM use-case, segmentasiya, backup və playbook.

HİSSƏ 1

Ransomware artıq sadəcə şifrələmə deyil

Məqsəd yalnız sistemləri bağlamaq yox, reputasiya və hüquqi təzyiq yaratmaqdır.

1. Giriş

Phishing, zəif VPN, sızmış parol, vendor hesabı və ya açıq zəiflikdən başlanır.

2. Səssiz hazırlıq

Backup axtarılır, admin hüquqları toplanır, kritik sistemlər xəritələnir.

3. Data extortion

Məlumat əvvəlcə çıxarılır; sonra şifrələmə və ya sızdırma təhdidi gəlir.

4. Dayanma

Xidmət, əməliyyat, etibar və qərarvermə zərbə alır.

5. Bərpa testi

Əsl sual: backup var? yoxsa işlək, ayrılmış və sınaqdan keçmiş backup var?

6. Kommunikasiya

Texniki bərpa qədər hüquqi, reputasiya və daxili kommunikasiya da vacibdir.

DƏRIN BAXIŞ

Ransomware-as-a-Service Modeli

NECƏ İŞLƏYIR

Bu model kibercinayətkarlığı 'xidmət' şəklinə salır: təcrübəli qruplar zərərli alətlər hazırlayıb az təcrübəli hücumçulara icarəyə verir və gəlirin bir hissəsini əldə edirlər. Bu, texniki bilik tələbini aşağı salaraq hücumların sayını artırır.

NƏTICƏLƏR

- **Aşağı giriş bariyeri**

  Az texniki bilikli şəxslər belə mürəkkəb hücumlar həyata keçirə bilir.

- **İkiqat şantaj taktikası**

  Məlumat həm şifrələnir, həm də ictimailəşdirilməklə hədələnir.

- **Sürətli yayılma**

  Hazır alətlər hücumların miqyasını qısa müddətdə artırır.

HİSSƏ 1

Təhdidləri prioritetləşdirməsi

Hədəf Sektorlar və Əsas Risklər

Sektor	Əsas Hədəf Səbəbi	Tipik Hücum Növü
Maliyyə xidmətləri	Birbaşa maliyyə mənfəəti	Fişinq, hesab ələ keçirmə
Dövlət qurumları	Strateji və siyasi məlumat	Casusluq, DDoS
Səhiyyə	Həssas şəxsi məlumatlar	Ransomware
Təhsil	Zəif təhlükəsizlik infrastrukturu	Fişinq, məlumat sızması
İstehsalat	Əməliyyat kəsintisinin ağır nəticələri	Tədarük zənciri hücumları

HİSSƏ 1

Hissə 1 üzrə əsas nəticə

Landşaft dəyişsə də, yaxşı müdafiənin əsasları hələ də kritikdir.

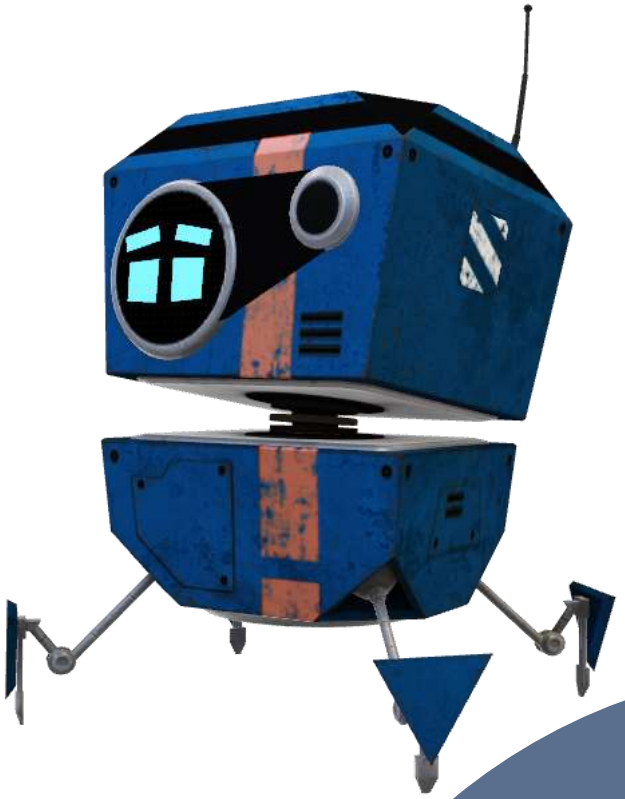
- Hücumlar daha sürətli və kombinə olunmuş olur: zəiflik + credential + social engineering + vendor riski.
- İdentifikasiya və giriş hüquqları yeni “perimetr” kimi düşünülməlidir.

- Ransomware dayanıqlılıq testidir: backup, segmentasiya, kommunikasiya və qərarvermə birlikdə işləməlidir.
- Təhdid trendləri alət seçimi üçün yox, prioritetləşdirmə və resurs bölgüsü üçün oxunmalıdır.

Keçid mesajı **Növbəti hissədə hücumların ən güclü qapısını — insan qərarını — analiz edirik.**

02

Sosial Mühəndislik: İnsan Faktorunun İstismarı



Texniki müdafiə nə qədər güclü olsa da, insan amili çox zaman ən zəif həlqə olaraq qalır

HİSSƏ 2

Sosial mühəndislik nədir?

Psixoloji təsir və kontekstdən istifadə etməklə insanın təhlükəsizlik davranışını dəyişdirmək.

Manipulyasiya

Qorxu, təciliyyət, etibar, avtoritet, maraq və ya fayda vədi ilə qərarvermə zəiflədilir.

Kontekst

Hücumçu iş yeri, layihə, rəhbər, vendor, tədbir və ya gündəlik prosesi imitasiya edir.

Nəticə

Parol, OTP, token, fayl, ödəniş, icazə və ya daxili məlumat əldə edilir.

Qızıl qayda **Mesajın məzmunundan əvvəl onun niyyətini, kanalını və təsdiqlənmə yolunu yoxla.**

ƏSASLAR

Sosial Mühəndisliyin Psixoloji Əsasları

PRINSIP

Sosial mühəndislik texniki zəifliklərdən deyil, insan psixologiyasından — etibar, aciliyyət hissi, nüfuza tabeçilik və maraq kimi təbii reaksiyalardan — istifadə edir. Hücumçular bu emosional tətikləri məqsədyönlü şəkildə aktivləşdirir.

MANIPULYASIYA PRINSIPLƏRI

- **Nüfuz**

  Rəhbər və ya rəsmi qurum kimi görünərək etimad qazanmaq.

- **Aciliyyət**

  Təxirəsalınmaz vəziyyət yaradaraq düşünmə vaxtını azaltmaq.

- **Sosial sübut**

  'Başqaları da belə edib' deyərək davranışı normallaşdırmaq.

HİSSƏ 2

Manipulyasiyanın 6 psixoloji qolu

Hücumçu texniki zəiflik tapmasa belə, insan reflekslərini hədəfə alır.

Təciliyyət

“İndi təsdiqlə, yoxsa hesab bağlanacaq”

Avtoritet

“Rəhbərlik tapşırıb”

Qorxu

“Cərimə / bloklanma / araşdırma”

Mükafat

“Hədiyyə, bonus, endirim”

Etibar

“Tanınmış şəxs və ya vendor adı”

Maraq

“Bu sənədə bax, adın keçir”

Uşaqların internetdə təhlükəsizliyinin təmin edilməsini ifadə edən bir çox termin mövcuddur. Bunlara **onlayn mühafizə (online safeguarding)**, **onlayn təhlükəsizlik (online safety)**, **rəqəmsal təhlükəsizlik (digital safety)**, **e-təhlükəsizlik (e-safety)** və **internet təhlükəsizliyi (internet safety)** daxildir.

Son 10 il ərzində uşaqların internetdən istifadəsinin əhəmiyyətli dərəcədə artması ilə əlaqədar bir çox yeni risk və problemlər ortaya çıxmışdır. **COVID-19 pandemiyası** isə bütün dünyada onlayn təhsili daha da genişləndirmişdir. Bu sahədə kifayət qədər təcrübəsi olmayan ölkələrdə isə uşaqların təhlükəsizliyinin qorunması istiqamətində tədbirlər gücləndirilmədikdə risklər daha da artır.

Əsas risklərə aşağıdakılar daxildir:

Cinsi istismar (Sexual Exploitation)	**Manipulyativ yaxınlaşma və etimad qazanma (Grooming)**	**Kiber zorakılıq (Cyberbullying)**	**Seksual məzmunlu mesaj və materialların paylaşılması (Sexting)**	**Radikallaşma (Radicalization)**

Uşaqların Müdafiəsi (Child Safeguarding)

Uşaqların müdafiəsi təşkilatların öz əməkdaşlarının, əməliyyatlarının və proqramlarının uşaqlara və böyüklərə zərər verməməsini, onları istismar və ya sui-istifadə riskinə məruz qoymamasını təmin etmək məsuliyyətidir. Bu məsuliyyət həmçinin internet mühiti və mobil telefonlar vasitəsilə baş verə biləcək risklərin qarşısının alınmasını da əhatə edir.

"Uşaqların müdafiəsi təşkilatların fəaliyyətləri nəticəsində uşaqların və həssas şəxslərin hər hansı fiziki, psixoloji və ya rəqəmsal zərərə məruz qalmamasını təmin edən sistemli tədbirlər toplusudur."

NÖVLƏR

Fişinqin Formaları

1

Fişinq (Phishing)

Kütləvi göndərilən saxta e-poçtlarla giriş məlumatlarının oğurlanması.

2

Nizələnmiş Fişinq (Spear Phishing)

Konkret şəxsə yönəlmiş, fərdiləşdirilmiş və daha inandırıcı hücum.

3

Whaling

Yüksək vəzifəli rəhbərləri hədəf alan xüsusi fişinq növü.

4

Vişinq və Smişinq

Telefon zəngi (vishing) və ya SMS (smishing) vasitəsilə aparılan aldatma.

HİSSƏ 2

Phishing mesajını necə oxumaq lazımdır?

Mesajı “maraqlıdırmı?” yox, “təsdiqlənə bilirmi?” sualı ilə yoxlayın.

From: it-support@secure-login.az

Subject: Hesabınız 30 dəqiqəyə bağlanacaq

Hörmətli istifadəçi, təhlükəsizlik yoxlaması üçün linkə daxil olaraq parolunuzu təsdiqləyin. Əks halda hesab bloklanacaq.

Giriş et

- Göndərən domeni oxşardır, amma rəsmi olmaya bilər.
- Təciliyyət və qorxu ilə klik təzyiqi yaradılır.
- Linki açmadan əvvəl üzərinə gətirib ünvanı yoxlayın.
- Parol/MFA kodu heç vaxt mesajla təsdiqlənmir.

✓ **Ən təhlükəsiz davranış**

Linkə basmadan rəsmi portalı ayrıca açın və ya sorğunu ikinci kanalla təsdiqləyin.

Fişinq mesajını necə tanımaq olar?

5 saniyəlik yoxlama modeli

SMS nümunəsi

“Hörmətli vətəndaş, sosial yardımınız dayandırılacaq. Təcili təsdiq üçün linkə daxil olun: az-gov-help.net/verify”

1. **Göndərən kimdir?**
2. **Link rəsmi domendirmi?**
3. **Təcili qorxu yaradırmı?**
4. **Kart/OTP tələb edirmi?**
5. **Rəsmi portaldan ayrıca yoxladınmı?**

Qayda: linkə yox, rəsmi portala özünüz daxil olun.

FİŞİNQ

Fişinq Hücumlarını Necə Tanımaq Olar?

ŞÜBHƏLI E-POÇT NÜMUNƏSİ

Göndərən: noreply@aztv-news-update.net ← saxta domen!

Mövzu: ACİL: Hesabınız bloklanacaq — 24 saat ərzində tədbip görün

Məzmun: Əziz istifadəçi, hesabınızda şübhəli fəaliyyət aşkarlanıb...

Keçid: http://aztv.verify-account-now.ru/login ← HECDƏN basmayin!

Qırmızı bayraqlar: Göndərən adresi rəsmi domen deyil • Təcililik yaradır, vaxt təzyiqi edir • Keçid URL-i şübhəli (başqa domen) • Hesab bloku, pul ödənişi, mükafat vədi

Mon 4/3/2017 4:26 PM

Chris Colbert <chris.colbert@kpu.ca>

H.R MSVU

To Ken Munro

Greetings,

You have a message from the Human Resources Department.

Click here to view your message

http://sadfwx.com/redo/outlookweb/outlookwebapp.html
Click or tap to follow link.

amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID: [redacted]

HİSSƏ 2

Emaildən kənara çıxan sosial mühəndislik

Mobil, səs və QR kodlar hücumçular üçün daha rahat vektor olub.

SMS

Smishing

SMS/WhatsApp/Telegram üzərindən saxta linklər və “çatdırılma, bank, cərimə” mesajları.

☎

Vishing

Telefonla özünü bank, dövlət qurumu, rəhbər və ya vendor kimi təqdim etmə.

QR

QR phishing

Poster, tədbir, menyu və ya ödəniş QR kodu ilə saxta saytın açılması.

→

Davranış modeli

Kanal dəyişirsə, risk də dəyişir: mesajdan gələn link, zəngdə verilən tapşırıq və QR kod həmişə müstəqil təsdiq tələb edir.

HİSSƏ 2

Business Email Compromise: “rəhbər yazdı” tələsi

Texniki malware olmadan da maliyyə və reputasiya itkisi yarana bilər.

Saxta identitet

Rəhbər/vendor kimi görünür

Kontekst

Real layihə və ödəniş məlumatı istifadə edir

Təzyiq

Təcili və gizli icra tələb edir

Dəyişiklik

IBAN, müqavilə və ya fayl dəyişir

İcra

Ödəniş, məlumat və ya icazə verilir

✓ Nəzarət

Maliyyə, müqavilə, IBAN, hüquq və kritik giriş sorğuları üçün “ikinci kanal təsdiqi” mütləq olmalıdır.

! Red flag

“Bunu heç kimə demə”, “indi et”, “sonra izah edərəm”, “telefonum işləmir” kimi ifadələr manipulyasiya siqnalıdır.

HİSSƏ 2

Fiziki sosial mühəndislik: ofis də hücum səthidir

Kart, qapı, printer, ziyarətçi və masaüstü məlumatlar texniki sistem qədər önəmlidir.

Tailgating

Kiminsə arxasınca kart olmadan içəri daxil olmaq.

Shoulder surfing

Ekran, PIN, sənəd və ya badge məlumatını müşahidə etmək.

Pretexting

Saxta ziyarətçi, texniki dəstək və ya kuryer rolu yaratmaq.

Clean desk

Açıq sənədlər, post-it parollar, çap olunmuş siyahılar və açıq ekranlar risk yaradır.

Badge culture

Kimlik kartı mədəniyyəti nəzakətsizlik deyil, təhlükəsizlik davranışıdır.

Report early

Şübhəli şəxs və davranış dərhal, qorxmadan bildirilməlidir.

HİSSƏ 2

“Human firewall” nə deməkdir?

İnsan firewall deyil, amma düzgün proseslə risk sensoruna çevrilə bilər.

1. Dayan
2. Yoxla
3. Təsdiqlə
4. Bildir
5. Öyrən

→

Məqsəd

İstifadəçini günahlandırmaq yox, doğru anda doğru qərar verməyə kömək edən sadə davranış modelini yaratmaqdır.

KPI

Təlim ölçüsü

Yalnız “kim kliklədi?” yox, “kim bildirdi?”, “nə qədər tez bildirdi?”, “təkrar risk azaldımı?” ölçülməlidir.

MÜDAFIƏ

Sosial Mühəndislikdən Qorunma Tədbirləri

Effektiv müdafiə texnologiya ilə davranış vərdişlərinin birləşməsindən ibarətdir

✓ **Göndərəni yoxlayın**

E-poçt ünvanını və domeni diqqətlə yoxlayın, tələsik qərar verməyin.

✓ **İkinci kanaldan təsdiqləyin**

Şübhəli sorğuları alternativ kanal vasitəsilə birbaşa təsdiqləyin.

✓ **Linklərə ehtiyatla yanaşın**

Kliklәmədən əvvəl keçidin əsl ünvanını yoxlayın.

✓ **Hadisəni dərhal bildirin**

Şübhəli fəaliyyəti gecikmədən təhlükəsizlik komandasına çatdırın.

HİSSƏ 2

Mini-məşq: 60 saniyədə red flag tapın

Aşağıdakı sorğuda hansı risk siqnalları var?

“Salam, mən yeni audit komandasıyam. Rəhbərlik bu günə qədər istifadəçi siyahısını və admin hesabları olan Excel faylını istəyir. Vaxt azdır, zəhmət olmasa WhatsApp-la göndərin. Bu məsələni hələlik yaymayın.”

- Təsdiqlənməmiş şəxs və kanal
- Həssas məlumat sorğusu
- Təciliyyət və gizlilik təzyiqi
- Qeyri-rəsmi paylaşım kanalı
- Rəhbərlik adına avtoritet manipulyasiyası

✓ **Doğru cavab**

Məlumatı göndərməyin. Rəsmi audit planını, yazılı sorğunu və təsdiqlənmiş paylaşım kanalını tələb edin; şübhəni təhlükəsizlik komandasına bildirin.

03

Rəqəmsal Şəxsiyyət və Məlumat Təhlükəsizliyi

Şəxsi və institusional məlumatların qorunması müasir təhlükəsizlik strategiyasının mərkəzi elementidir

KONSEPSIYA

Rəqəmsal Şəxsiyyət Nədir?

TƏRIF

Rəqəmsal şəxsiyyət — istifadəçini onlayn mühitdə təmsil edən məlumatlar toplusudur: istifadəçi adları, parollar, biometrik göstəricilər, davranış izləri və rəqəmsal sertifikatlar. Bu şəxsiyyətin qorunması fiziki sənədlərin qorunması qədər vacibdir.

KOMPONENTLƏR

- **Autentifikasiya məlumatları**

  İstifadəçi adı, parol və çoxfaktorlu təsdiq vasitələri.

- **Davranış izləri**

  Onlayn fəaliyyət, giriş yerləri və istifadə vərdişləri.

- **Rəsmi rəqəmsal sənədlər**

  Elektron imza, sertifikatlar və rəsmi identifikasiya vasitələri.

HİSSƏ 3

Rəqəmsal şəxsiyyət yeni perimetrdir

Bulud, mobil və uzaq iş mühitində hesabın təhlükəsizliyi sistemin təhlükəsizliyinə bərabərdir.

ID

Hesab

Kim daxil olur? İnsan, servis hesabı, vendor, admin, tətbiq?

Cihaz

Hansı cihazdan daxil olur? Qorunurmu, yenilənibmi, itirilibmi?

Kontekst

Haradan, nə vaxt, hansı davranışla, hansı risk göstəricisi ilə?

KEY

İcazə

Bu hesab bu məlumatı görməlidirmi? Müvəqqəti icazə bitibmi?

Sessiya

Token oğurlanıbsa parol dəyişmək kifayət etməyə bilər.

LOG

Log

Anormal davranışı görmək üçün audit izi varmı?

RISKLƏR

Şəxsi Məlumatların Sızması Riskləri

277 gün

Orta hesabla bir məlumat sızmasının aşkarlanması üçün tələb olunan vaxt

1 hesab

Yenidən istifadə edilən parol bir platformada sızarsa, digər hesablar da risk altına düşür

3 ay+

Şəxsiyyət oğurluğunun nəticələrinin aradan qaldırılması üçün tələb oluna biləcək orta müddət

Qeyd: Göstəricilər sənaye üzrə ümumi tendensiyaları əks etdirən illüstrativ rəqəmlərdir.

PAROL TƏHLÜKƏSİZLİYİ

Güclü Parol & Hesab Qorunması

✕ ZƏIF PAROLLAR

- 123456 (300M+ hesabda)
- password123
- Ad + doğum tarixi
- Eyni parol hər yerdə
- Qısa (<8 simvol)

✓ GÜCLÜ PAROLLAR

- 16+ simvol, hərflər+rəqəm
- Parol meneceri istifadəsi
- Hər hesab üçün fərqli
- Cümləyə əsaslı: 'Ev2Şəhər@Gəl!'
- İki addımlı doğrulama (2FA)

2FA / MFA

İki Addımlı Doğrulama (2FA) — Ən Vacib Qoruma

Hesabınız sındırılsa belə, 2FA olmadan daxil ola bilmirlər.

1

Şifrəni daxil edirsiniz

Adi parolunuzla ilk addım

→

2

Kod tələb olunur

Telefonunuza SMS, ya uygulama kodu

→

3

Giriş mümkün olur

Yalnız hər iki faktor doğrulandıqda

Autentikator App

Google Authenticator, Microsoft Authenticator — ən yaxşı seçim

SMS Kodu

Telefona göndərilən kod — rahat, lakin SIM swap riski var

Hardware Açar

YubiKey kimi fiziki cihaz — ən güclü qoruma

E-poçt Kodu

Ən az tövsiyə edilən — e-poçt özü sındırılmış ola bilər

SOSİAL MEDİA

Sosial Media Hesablarınızı Qoruyun

Sosial media hesabınız sizin professional kimliğinizdir — onu qorumaq peşəkar borcunuzdur.

Gizlilik parametrləri

Şəxsi məlumatları, yer xidmətlərini məhdudlaşdırın

2FA aktiv edin

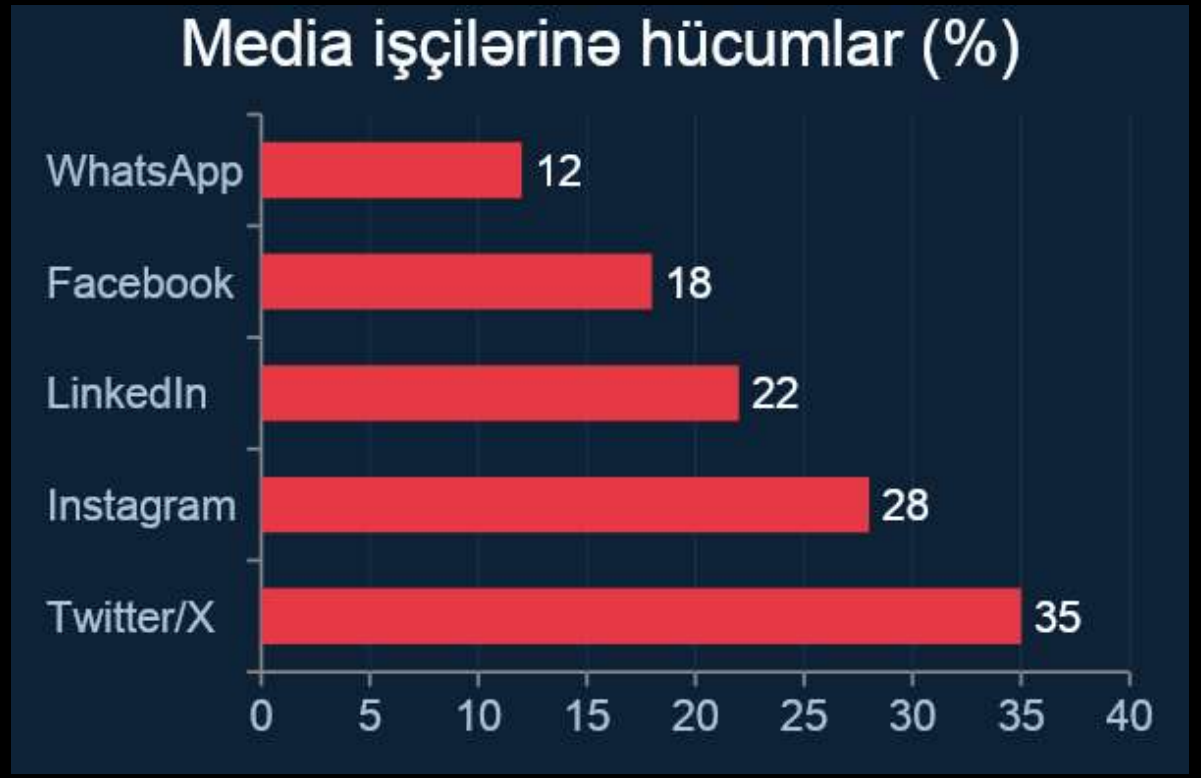
Bütün hesablarda məcburi iki addımlı doğrulama

Saxta profil yoxlayın

Sizin adınıza saxta hesablar yaradıla bilər

Üçüncü tərəf applar

Hesabınıza bağlı naməlum appları silin



MƏNBƏ QORUNMASI

Mənbənizin Həyatı Sizin Əlinizdədir

Mənbənizi qorumaq etik vəzifə deyil — bu onun HƏYATINI qorumaq ola bilər.

Signal Messencer

Uçdan-uca şifrələnmiş mesajlaşma. Mənbə üçün tövsiyə №1.

ProtonMail

Şifrələnmiş e-poçt. İsveçrə serverlərindən işləyir.

Tor Browser

IP adresinizi gizlədən brauzer. Riskli müstəntiqlik üçün.

SecureDrop

Sızdırıcılar üçün anonim fayl göndərmə platformu.

Şifrəli Zəng

Signal, WhatsApp E2E — adi zənglər dinlənilə bilər.

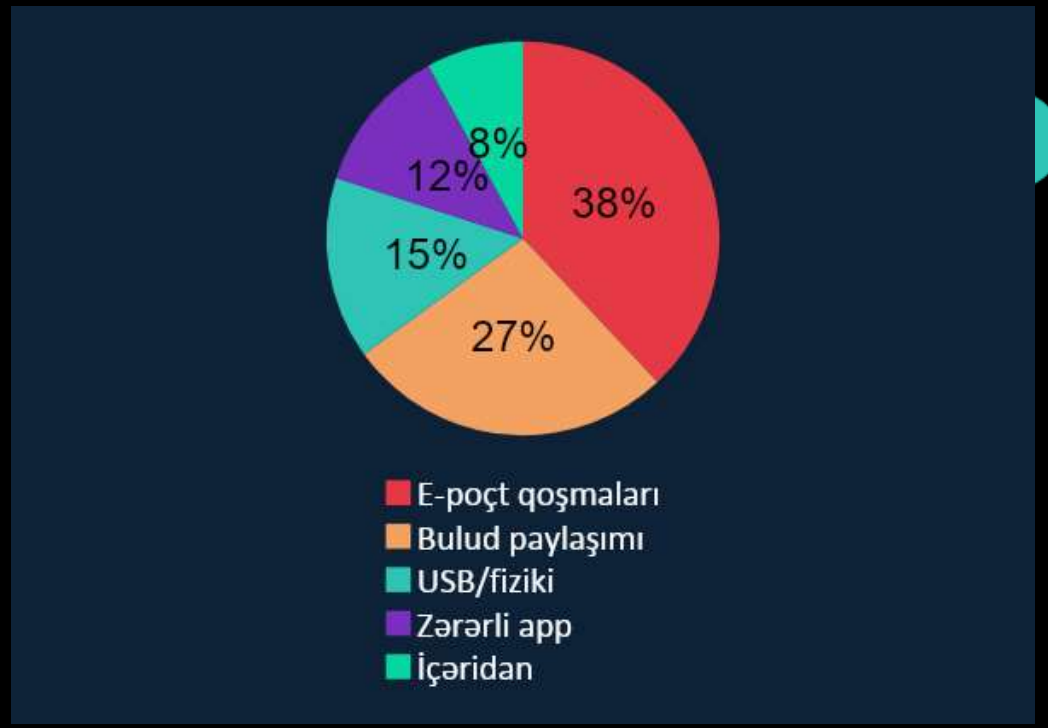
Fiziki Görüş

Çox həssas hallarda — telefonsuz, offline görüş.

BULUD & FAYL

Sənəd & Fayl Paylaşımı Qaydaları

1. Həssas sənədləri şifrəli paylaşın (Tresorit, Cryptomator)
2. Google Drive/Dropbox-da icazə parametrlərini yoxlayın
3. Keçidlə paylaşım: müddət məhdudiyyəti qoyun
4. E-poçt qoşması: şifrəli ZIP ya ProtonMail
5. Naməlum mənbədən gələn fayllara antivirus tətbiq edin
6. Fayl adlarında mənbə adı HECDƏN yazmayın



MÜQAYISƏ

Autentifikasiya Üsulları

Üsul	Üstünlük	Məhdudiyyət
Sadə parol	Tətbiqi asandır	Ən zəif təhlükəsizlik səviyyəsi
Güclü, unikal parol	Brute-force hücumlarına davamlıdır	Yadda saxlamaq çətindir, menecer tələb edir
Çoxfaktorlu autentifikasiya (MFA)	Parol sızsa belə əlavə qoruma təmin edir	Əlavə addım tələb edir
Biometrik autentifikasiya	Yüksək təhlükəsizlik və istifadə rahatlığı	Biometrik məlumat sızarsa dəyişdirilə bilməz

HİSSƏ 3

MFA vacibdir, amma səhv tətbiq olunarsa zəifləyir

MFA “sehrli qalxan” deyil; push fatigue, token oğurluğu və recovery boşluqları nəzərə alınmalıdır.

MFA riski	Nə baş verir?	Müdafiə davranışı
Push fatigue	İstifadəçiyə çoxlu təsdiq sorğusu göndərilir	Sorğunu rədd et və bildir
OTP phishing	Kod saxta səhifədə daxil edilir	Kodu heç vaxt linkdən gələn səhifəyə yazma
Recovery bypass	Bərpa emaili/telefonu zəifdir	Recovery kanallarını qoruyun
Device loss	Telefon/cihaz itir	Dərhal bloklama və sessiya çıxışı

✓ **Ən yaxşı yanaşma**

MFA ilə yanaşı risk əsaslı giriş, cihaz vəziyyəti, sessiya idarəetməsi və istifadəçi təlimi birlikdə işləməlidir.

HİSSƏ 3

Məlumat təhlükəsizliyi: əvvəlcə nəyi qoruduğunu bil

Bütün məlumat eyni səviyyədə qorunmur; amma hər məlumatın sahibi və qaydası olmalıdır.

PUBLIC	Açıq paylaşım mümkündür, amma dəqiqlik vacibdir
INTERNAL	Daxili istifadə; xaricə nəzarətsiz çıxmamalıdır
CONFIDENTIAL	Şəxsi, maliyyə, müqavilə, audit və təhlükəsizlik məlumatları
RESTRICTED	Kritik sistem, identifikasiya, açar, sirr və əməliyyat məlumatları

? **Praktiki sual**

Bu məlumat yanlış adama getsə, dəyişdirilsə və ya əlçatan olmasa nə baş verər?

HİSSƏ 3

Məlumat minimizasiyası: az məlumat, az risk

Lazımsız saxlanan məlumat breach zamanı zərəri böyüdür.

1 Toplama

Həqiqətən lazımdırmı? Məqsəd, hüquqi əsas və müddət aydındırmı?

2 Saxlama

Kim görür, nə qədər saxlanır, harada ehtiyat nüsxəsi var?

3 Paylaşma

Məlumat tam lazımdır, yoxsa maskalanmış/anonim versiya kifayətdir?

4 Silinmə

Retention bitəndə silinmə sadəcə faylı delete etmək deyil; sübutlu və bərpa olunmaz proses olmalıdır.

L O G Audit izi

Hər kritik məlumat əməliyyatı üçün kim, nə vaxt, nə etdi sualının cavabı qalmalıdır.

HİSSƏ 3

Məlumat sızmasının gündəlik ssenariləri

Böyük hadisələr çox vaxt kiçik gündəlik rahatlıqlardan başlayır.

Yanlış alıcı

Email autocomplete səhvi

Şəxsi cloud

Faylı evdə işləmək üçün yükləmə

Açıq ekran

İclas, kafe, taksi, aeroport

USB

USB

Nəzarətsiz kopyalama

AI

Chatbot

Məxfi məlumatı AI alətinə daxil etmə

Screenshot

Etiket və kontekst itir

HİSSƏ 3

Hissə 3 üzrə əsas nəticə

Rəqəmsal şəxsiyyət qorunmasa, məlumat təhlükəsizliyi yalnız kağız üzərində qalır.

- Identity = istifadəçi + cihaz + sessiya + icazə + kontekst.
- MFA vacibdir, amma istifadəçi davranışı və recovery mexanizmləri də qorunmalıdır.
- Məlumat həyat dövrü boyunca izlənməlidir: yaratma, saxlama, paylaşma, arxiv, silmə.
- Minimallaşdırma və klassifikasiya breach təsirini azaldan ən praktik idarəetmə alətləridir.

→ **Keçid mesajı**

Növbəti hissədə bu risklərin AI ilə necə dəyişdiyini və AI-dan müdafiə üçün necə məsuliyyətlə istifadə etməyi müzakirə edirik.

04 Süni İntellekt: Yeni Risklər və Müdafiə İmkanları

Süni intellekt həm hücum vasitəsi, həm də ən güclü müdafiə alətlərindən birinə çevrilib

YENI TƏHDIDLƏR

AI-Əsaslı Hücumların Yüksəlişi

DƏYIŞƏN MƏNZƏRƏ

Süni intellekt alətləri hücumçulara daha inandırıcı, miqyaslana bilən və aşkarlanması çətin olan hücumlar hazırlamaq imkanı verir. Generativ AI mətn, səs və video kimi formatlarda yüksək keyfiyyətli saxta məzmun yaratmağı kütləviləşdirib.

KONKRET TƏHLÜKƏLƏR

- **AI-təkmilləşdirilmiş fişinq**

  Qrammatik səhvsiz, fərdiləşdirilmiş və inandırıcı mesajların avtomatik yaradılması.

- **Deepfake texnologiyası**

  Real insanın səsini və ya görüntüsünü təqlid edən saxta media.

- **Avtomatlaşdırılmış zəiflik axtarışı**

  AI vasitəsilə sistemlərdə boşluqların sürətli aşkarlanması.

NÜMUNƏ

Deepfake Riskləri: Praktiki Ssenari

SSENARİ

Maliyyə əməkdaşı rəhbərin səsini təqlid edən zəng alır. Zəngdə 'təcili' bir tədarükçüyə ödəniş edilməsi tələb olunur. Səs real görünsə də, əslində süni intellekt vasitəsilə yaradılmış saxta audiodur və ənənəvi təhlükəsizlik nəzarətlərini keçməyə çalışır.

ƏSAS NƏTİCƏLƏR

Səs və ya video tək başına kifayət edən təsdiq vasitəsi deyil

Yüksək məbləğli əməliyyatlar üçün çoxmərhələli təsdiq prosedurları qurulmalıdır

Komanda üzvləri deepfake risklərindən mütəmadi məlumatlandırılmalıdır

AI-Əsaslı Müdafiə Mexanizmləri

POTENSIAL

Eyni texnologiya müdafiə tərəfində də güclü üstünlük yaradır. AI sistemləri böyük həcmli məlumatı real vaxtda analiz edərək adi qaydalara əsaslanan sistemlərin gözdən qaçırdığı anomaliyaları aşkarlaya bilir və insident cavabını sürətləndirir.

TƏTBIQ SAHƏLƏRI

- **Anomaliya aşkarlanması**

  Şəbəkə trafikində qeyri-adi davranışların avtomatik müəyyən edilməsi.

- **SOC avtomatlaşdırması**

  Təhlükəsizlik əməliyyat mərkəzlərində təkrarlanan tapşırıqların sürətləndirilməsi.

- **Fişinq filtrasiyası**

  Gələn e-poçtların məzmun və nümunə əsasında real vaxtda skrininqi.

HİSSƏ 4

Shadow AI: görünməyən istifadə, görünən risk

İşçilər AI alətlərindən istifadə etdikcə məxfi məlumat və qərarvermə riski yaranır.

AI

Nədir?

Təsdiqlənməmiş AI alətləri, şəxsi hesablar, qeyri-rəsmi chatbotlar və nəzarətsiz inteqrasiyalar.

DATA

Nə sızır?

Müqavilələr, source code, incident məlumatı, personal data, daxili strategiya və konfiqurasiya detalları.

✓

Nəzarət

Approved tools, data classification, DLP, logging, istifadə qaydası və təlim lazımdır.

Prinsip **AI-a daxil etdiyiniz məlumatı internetə göndərilmiş kimi yox, idarə olunan risk obyekti kimi düşünün.**

Mənbə: IBM Cost of a Data Breach 2025 – shadow AI riskləri.

HİSSƏ 4

Məsuliyyətli AI idarəetməsi: minimum kontrol modeli

AI innovasiyası sürətli ola bilər, amma nəzarətsiz olmamalıdır.

1 **İcazə siyahısı**

Təsdiqlənmiş alətlər və istifadə halları

2 **Data qaydası**

Nə daxil etmək olar/olmaz

3 **Access control**

Model, data və prompt girişləri

4 **Logging**

Sorğuların audit izi

5 **Human review**

Yüksək riskli cavablarda insan təsdiqi

6 **Vendor review**

Saxlama, təlim, paylaşma şərtləri

HİSSƏ 4

AI risk register: rəhbərlik üçün sadə baxış

AI layihəsi təhlükəsizlik, hüquq, data və biznes riski kimi birlikdə qiymətləndirilməlidir.

Risk	Nümunə	Təsir	Kontrol
Məxfilik	Məxfi məlumat promptda	Data sızması	DLP + policy
Dəqiqlik	Hallucination	Səhv qərar	Human review
Bias	Uyğunsuz nəticə	Etibar itkisi	Test + monitorinq
Təchizat	Model/vendor riski	Asılılıq	Vendor review

HİSSƏ 4

AI istifadə etməzdən əvvəl 7 sual

Bu checklist işçilər üçün gündəlik qərar modelidir.

- Bu alət təşkilat tərəfindən təsdiqlənibmi?
- Daxil etdiyim məlumatın klassifikasiyası nədir?
- Cavab qərar üçün istifadə olunacaqsa, kim yoxlayacaq?
- Alət məlumatı saxlayır və ya təlim üçün istifadə edirmi?
- Nəticə yanlış olsa, təsir nə olacaq?
- Bu tapşırıq üçün AI-a həqiqətən ehtiyac varmı?
- Hadisə və ya səhv görsəm, hara bildirəcəyəm?

05

Kiberdayanıqlılıq və Təhlükəsizlik Mədəniyyəti

Texnologiya təkbaşına kifayət etmir — davamlılıq təşkilati mədəniyyət və hazırlıqdan asılıdır

HİSSƏ 5

Kiberdayanıqlılıq nədir?

Məqsəd yalnız hücumu bloklamaq deyil; zərbəni udmaq, bərpa olmaq və daha güclü qayıtmaqdır.

Prepare
risk, asset, plan

Protect
kontrol və gigiyena

Detect
monitorinq və siqnal

Respond
playbook və qərar

Recover
backup və DR

Improve
lessons learned

↻ **Əsas mesaj**

Dayanıqlılıq “IT backup var” demək deyil. İnsan, proses, rəhbərlik qərarı, kommunikasiya, hüquqi tələb və texniki bərpa birlikdə işləməlidir.

KONSEPSIYA

Kiberdayanıqlılıq Nədir?

TƏRIF

Kiberdayanıqlılıq — təşkilatın kiberhücumun qarşısını almaq, ona reaksiya vermək və nəticələrindən sürətlə bərpa olunmaq bacarığıdır. Bu, yalnız hücumların qarşısını almaqla deyil, hadisə baş verdikdə fəaliyyətin davamlılığını təmin etməklə ölçülür.

ƏSAS ÖLÇÜLƏR

- **Qarşısını alma**

  Zəifliklərin azaldılması və proaktiv müdafiə tədbirləri.

- **Aşkarlama və reaksiya**

  Hadisələrin tez müəyyən edilməsi və düzgün cavab prosedurları.

- **Bərpa qabiliyyəti**

  Fəaliyyətin minimal kəsinti ilə normal rejimə qaytarılması.

PROSEDUR

İnsidentə Cavab Planının Mərhələləri

01

Hazırlıq

Prosedurların və komandanın əvvəlcədən müəyyən edilməsi

02

Aşkarlama

Hadisənin vaxtında müəyyən edilməsi və qiymətləndirilməsi

03

Təcrid Etmə

Zərərin yayılmasının qarşısının alınması

04

Bərpa

Sistemlərin təhlükəsiz şəkildə normal rejimə qaytarılması

05

Dərs Çıxarma

Hadisənin təhlili və gələcək üçün təkmilləşdirmə

TƏŞKILATI YANAŞMA

Təhlükəsizlik Mədəniyyətinin Qurulması

Güclü təhlükəsizlik mədəniyyəti hər səviyyədə məsuliyyət tələb edir

✓ **Rəhbərliyin nümunəsi**

Yüksək rəhbərlik təhlükəsizlik prioritetlərinə əməl etməli və dəstəkləməlidir.

✓ **Aydın siyasətlər**

Qaydalar hər kəs üçün başa düşülən və əlçatan olmalıdır.

✓ **Açıq bildiriş mühiti**

İşçilər səhvləri cəza qorxusu olmadan bildirə bilməlidir.

✓ **Davamlı təkmilləşdirmə**

Mədəniyyət mütəmadi qiymətləndirilməli və yenilənməlidir.

İNKIŞAF

Təlim və Maarifləndirmə Proqramları

ƏHƏMIYYƏTI

Mütəmadi təlim proqramları işçiləri son təhdidlərdən xəbərdar saxlayır və nəzəri biliyi praktiki vərdişə çevirir. Ən effektiv proqramlar bir dəfəlik tədbir deyil, davamlı prosesdir və real ssenarilər üzərində simulyasiyaları əhatə edir.

EFFEKTIV ELEMENTLƏR

- **Simulyasiya təlimləri**

  Real fişinq ssenarilərinin təcrübə mühitində sınanması.

- **Rol-əsaslı yanaşma**

  Hər vəzifə üçün uyğunlaşdırılmış təlim məzmunu.

- **Mütəmadi yenilənmə**

  Təlim materiallarının yeni təhdidlərə uyğun davamlı təkmilləşdirilməsi.

Real Case 1 – ABŞ (Atlanta şəhəri)

Şəhər əməkdaşı sosial yardım məlumatlarını dəyişdirirdi: Bir dövlət qurumunun əməkdaşı sistemdə müəyyən şəxslərə üstünlük vermək üçün sosial yardım məlumatlarını dəyişdirirdi.

Araşdırma nəticəsində:

- Audit loglar yoxlanıldı
- Sistem fəaliyyətləri təhlil edildi
- Dəyişikliklər aşkarlandı

Dərs: Audit loglar və rəqəmsal izlənilə bilənlik korrupsiyanın qarşısının alınmasında əsas vasitədir.

Real Case 2 – Braziliya Elektron Satınalma Sistemi

Pandemiya dövründə bəzi dövlət qurumlarında satınalma sənədləri manipulyasiya edilirdi.

Problemlər:

- Qeyri-rəqabətli seçimlər
- Sənədlərin dəyişdirilməsi
- Maraqların toqquşması

Sonra:

- Tam elektron satınalma sistemi quruldu
- Bütün əməliyyatlar açıq platformaya çıxarıldı

Nəticə:

- Şəffaflıq artdı
- Korrupsiya riski azaldı
- İctimai nəzarət gücləndi

Real Case 3 – Estoniya

Dünyanın ən şəffaf rəqəmsal dövlətlərindən biri

Estoniyada vətəndaş görə bilir:

- Məlumatına kim baxıb
- Nə vaxt baxıb
- Hansı məqsədlə baxıb

Əgər dövlət əməkdaşı məlumatlara səbəbsiz baxırsa:

- Sistem xəbərdarlıq yaradır
- Araşdırma başlanır

Nəticə

- Digital Trust və dövlətə etimad yüksəkdir.

DATA SNAPSHOT

Qlobal statistikalar: risk real, ölçülə bilən və sosial təsirlidir

Bu rəqəmlər təqdimata gender və uşaq müdafiəsi “business case” verir.

82%

15–24 yaşlıların 2025-də internetdən istifadəsi

UN

>1/3

30 ölkədə gənclər cyberbullying yaşadığını bildirir

UN/UNICEF

16–58%

Qadın və qızlarda texnologiya vasitəli zorakılıq diapazonu

UN Women

59.9%

İnternetə çıxışı olan qadınlarda TFV təcrübəsi

UNFPA

300M+

İldə online cinsi istismar və zorakılıqdan təsirlənən uşaqlar

Childlight

1/10

Cyberbullying bəzi qlobal ölçmələrdə uşaqların 10-da 1-nə təsir edir

UNESCO

1/17

Yeniyetmələr arasında deepfake imagery qurbanlığı

WeProtect/Thorn

291k

2024-də aşkarlanan CSAM veb-səhifələri

IWF/Safe Online

! **Nəticə**

Mövzunu sadəcə “parol və phishing” kimi deyil, qadın və uşaq təhlükəsizliyi prizmasından təqdim etmək lazımdır.

UN child safety online; UNESCO; UN Women; UNFPA; Childlight; WeProtect GTA 2025; IWF/Safe Online

Cyberbullying: məktəb problemi ekranlardan davam edir

Online zorakılıq dərs davamiyyəti, psixoloji sağlamlıq və ailə etimadına təsir edir.

1/10

Uşaqlarda cyberbullying qlobal narahatlıqdır

58%

Qızlar/gənc qadınlar online harassment ilə üzləşə bilir

16%

Təhsil üzərindən cyberbullying qanunvericiliyi olan ölkələr

→ **Təlimə bağlama**

Sosial mühəndislikdəki “qorxu və qrup təzyiqi” uşaqların davranışına təsir edir.

! **Risk siqnalı**

Uşaq cihazdan qaçır, hesabını bağlayır, məktəbdən yayınır və ya susqunlaşır.

✓ **Doğru cavab**

Sübutu qorumaq, uşağı günahlandırmamaq, məktəb və platforma reporting mexanizmlərini işə salmaq.

Mənbə: UNESCO safe learning environments; UNESCO anti-bullying day materials

AI ilə yeni risk formatları

Deepfake, sintetik məzmun və chatbot manipulyasiyası uşaqlar üçün yeni təhdid səviyyəsi yaradır.

AI Deepfake imagery

Sosial media fotosundan zərərli sintetik görüntü yaradılması və şantaj.

♪ Voice cloning

Valideyn, müəllim və ya tanış səsinin imitasiya olunması.

BOT AI companion

Emosional asılılıq, yanlış məsləhət və davranış manipulyasiyası.

✓ Safety-by-design

Platforma və AI alətlərində uşaq təhlükəsizliyi dizayn mərhələsindən düşünülməlidir.

1/17

Yeniyetmələr deepfake imagery qurbanlığı bildirmişdir

1,325%

AI-generated CSAM reportlarında 2023–2024 artım

Mənbə: WeProtect Global Threat Assessment 2025; NCMEC-linked AI-generated CSAM reporting

Qadınlara qarşı kiber zorakılığın formaları

Bu zərərlər hüquq, təhlükəsizlik, psixoloji sağlamlıq və sosial iştirak məsələsidir.

Cyberstalking

Davamlı izləmə, mesaj, hesabların monitorinqi

Doxxing

Ünvan, telefon, iş yeri və şəxsi məlumatların yayılması

Image-based abuse

Razılıqsız intim görüntü paylaşımı və şantaj

Deepfake abuse

AI ilə yaradılmış reputasiya və cinsi zorakılıq məzmunu

Impersonation

Saxta profil, adından mesaj, reputasiya manipulyasiyası

Spyware / tracking

Cihaz, lokasiya və sosial hesabların nəzarəti

Mühazirəyə əlaqə

Bu slayd sosial mühəndislik, reqemsal şəxsiyyət və AI riskləri qədərincə real təhlükəsizlik təcrübəsinə bağlayır.

Mənbə: UNFPA TFGBV glossary; UN Women digital abuse FAQ; UNDP TFGBV resources

Online zərər offline təhlükəyə çevrilə bilər

Rəqəmsal zorakılıq fiziki izləmə, reputasiya itkisi, iş riski və sosial təcridə keçid edə bilər.

2/3+

Qadın jurnalist/aktivistlər arasında online abuse təcrübəsi

41%

Online abuse sonrası offline harassment/attack bildirənlər

1 Online harassment

Təhdid, təhqir, koordinasiyalı hücum

2 Doxxing

Şəxsi məlumatın yayılması

3 Offline risk

İzləmə və fiziki təhlükə

! Təlim üçün mesaj

Online zorakılıq “şərh yazılıb keçdi” deyil; risk qiymətləndirməsində fiziki təhlükəsizlik və sosial dəstək də olmalıdır.

Mənbə: UN Women partner report coverage/AP 2025; UNFPA TFGBV

Sosial mühəndislik: qadın və uşaq kontekstində

Hücumçu emosional trigger-ləri və sosial rolları hədəfə alır.

Valideyn qorxusu

“Uşağınızın hesabı bloklanacaq”, “məktəb ödənişi”, “təcili məlumat”.

Saxta imkanlar

Fake job, scholarship, grant, aid və sosial yardım mesajları.

Uşağın marağı

Oyun bonusu, influencer mesajı, challenge, qrup statusu.

Utanc və susdurma

“Heç kimə demə”, “yayaram”, “özün günahkarsan”.

Təsdiq qaydası

Yüksək riskli mesajlar üçün ikinci kanal, rəsmi portal, valideyn/məktəb/kurum təsdiqi və reporting xətti.

Mənbə: UNICEF online safety; UNFPA TFGBV; WeProtect GTA 2025

Şəkil, lokasiya, məktəb adı və ailə paylaşımı hücumçu üçün kəşfiyyat məlumatıdır.

Oversharing

Məktəb, forma, ev ünvanı, real-time lokasiya və gündəlik rutin.

Ailə fotoları

AI üz tanıma, deepfake və saxta profil üçün xammal ola bilər.

KEY Recovery məlumatları

Ana adı, doğum tarixi, məktəb və şəxsi suallar hesab bərpasında istifadə olunur.

GPS Location tracking

Yaxın münasibət zorakılığı kontekstində texnologiya izləmə vasitəsinə çevrilə bilər.

✓ Minimum davranış

Real-time paylaşım əvəzinə gecikdirilmiş paylaşım, məxfilik ayarları, 2FA, device lock və uşaq razılığı mədəniyyəti.

Mənbə: UNFPA technology-facilitated GBV; UNICEF online safety; UN Women TFVAWG

Platforma xəritəsi: risk kanalları harada yaranır?

Eyni risk müxtəlif kanallarda fərqli görünür; təlim real nümunələr verməlidir.

1 WhatsApp / Telegram

Smishing, fake aid, private group pressure, image forwarding

2 Instagram / TikTok

Doxxing, fake profile, harmful challenge, public shaming

3 Discord / Gaming

Grooming, gift scam, voice chat manipulation, peer pressure

4 School platforms

Fake login, report-card phishing, parent payment scam

5 AI chatbots

Overtrust, emotional manipulation, confidential data input

6 Cloud / photos

Family album leakage, shared link exposure, AI reuse risk

✓ Praktiki təlim ideyası

Hər platforma üçün "red flag", "düğmə davranışı" və "hərəkətdirmək" üçlüyü verilməlidir.

Mənbə: UNICEF, UNESCO, UNFPA, WeProtect risk taxonomies

Qadın və uşaq təhlükəsizliyi üçün 6 tərəfli müdafiə modeli

Kiberdayanıqlılıq ailə, məktəb, dövlət, platforma, hüquq və texniki komandanın koordinasiyasıdır.

✓ Uşaq / qadın

Bildir, sübutu saxla, özünü günahlandırma

✓ Valideyn / ailə

Dinlə, cihazı qoparma, dəstək göstər

✓ Məktəb / sosial xidmət

Protokol, psixoloji dəstək, yönləndirmə

✓ Kibertəhlükəsizlik

Hesab bloklama, sübut, log, risk analizi

✓ Hüquq / dövlət qurumu

Müdafiə mexanizmi, reporting, qanuni tədbir

✓ Platforma

Report, takedown, privacy, safety-by-design

★ Mərkəzi prinsip

Hadisənin yalnız texniki problem kimi yox, insan təhlükəsizliyi və etimad hadisəsi kimi idarə etmək.

Mənbə: UNICEF child protection approach; UNFPA survivor-centred response; WeProtect prevention framework

İnsident olduqda: 5 addımlıq insan-mərkəzli playbook

Məqsəd qurbanı qorumaq, sübutu itirməmək və cavabı koordinasiyalı etməkdir.

1. Dayan

Panik qərar, pul köçürmə və ya silmə etmə

2. Qoru

Sübutu saxla: ekran görüntüsü, link, tarix, istifadəçi adı

3. Kəs

Əlaqəni dayandır, hesab/vəsaiyə təhlükəsizliyini təmin et

4. Bildir

Ailə, məktəb, sosial xidmət, platforma və cyber komandaya eskalasiya

5. Dəstək ver

Psixoloji, hüquqi və texniki dəstək; qurbanı günahlandırma

★ **Qızıl prinsip**

"Sən niyə etdin?" deyil — "Təhlükəsizsən, birlikdə həll edirik."

✓ **Təlimə əlavə edin**

Reporting kanalı, məsul şəxs və eskalasiya vaxtı əvəlcədən göstərilməlidir.

Mənbə: UNICEF/UNFPA survivor-centred and child protection principles

İNCİDENT CAVABI

Hacked? Bu Addımları Dərhal Atın!

Sakit qalın — tez hərəkət edin — redaksiyanızı xəbərdar edin.

1 **Şəbəkədən Ayrılın**

Cihazı WiFi/Ethernet-dən dərhal ayırın. Hücum yayılmasın.

2 **Parolları Dəyişdirin**

Başqa cihazdan həssas hesabların parollarını dəyin.

3 **Redaksiyanı Xəbərdar Et**

IT & redaktor rəhbərliyinə dərhal bildirin.

4 **Sübut Toplayın**

Ekran görüntüsü, log faylı — silməyin, sübut saxlayın.

5 **CERT-AZ-a Bildirin**

cert.az — milli kibertəhlükəsizlik hadisə mərkəzi.

6 **Sistemlərə Baxış**

IT mütəxəssisi tam forensik analiz aparacaq.

FAKT YOXLAMA

Rəqəmsal Fakt Yoxlama Alətləri

Xəbər yayımlamadan əvvəl bu alətləri məcburi istifadə edin:

Şəkil Yoxlama

- Google Reverse Image Search
- TinEye — şəkil tarixi
- InVID / WeVerify — video analizi

Sayt Yoxlama

- WHOIS — domen yaşı & sahibi
- URLScan.io — link analizi
- VirusTotal — link zərərliliyi

Mətn Analizi

- ChatGPT Detector alətləri
- Botometer — sosial bot aşkarı
- NewsGuard — xəbər mənbəsi reyting

Video/Audio

- Deepware Scanner
- Sensity AI
- Adobe Content Authenticity

XÜLASƏ

Əsas Mesajlar

1. Təhdid landşaftı sürətlə dəyişir və kibercinayət getdikcə daha mütəşəkkil xarakter alır
2. İnsan faktoru həm ən böyük zəiflik, həm də ən güclü müdafiə xəttidir
3. Rəqəmsal şəxsiyyətin və məlumatların qorunması hər səviyyədə diqqət tələb edir
4. Süni intellekt yeni risklər yaratsa da, eyni zamanda güclü müdafiə imkanları təqdim edir
5. Kiberdayanıqlılıq texnologiya, proses və mədəniyyətin birgə nəticəsidir

TƏŞƏKKÜRLƏR!

Suallar!