

**Bank  
Respublika**



# **R q msal Bank ılıq v  Kibert hl k sizlik**

Cibinizd ki bankı idar  etmək v  qorumaq   n m asir b l d iniz.

# Rəqəmsal bankçılıq nədir?

Ənənəvi filial



Müasir dövr:  
Cibinizdəki bank

Bank xidmətlərinin internet və mobil texnologiyalar vasitəsilə təqdim olunmasıdır. Artıq maliyyə əməliyyatlarını bank filialına getmədən, birbaşa cihazınızdan həyata keçirə bilərsiniz.



# Cibinizdəki Bank: Əsas Əməliyyatlar



## Hesab balansı

Hesab balansının yoxlanılması.



## Köçürmələr

Sürətli pul köçürmələri.



## Ödənişlər

Kommunal və digər ödənişlər.



## Kredit və Depozit

Kredit və depozit əməliyyatlarının idarə olunması.



## Kart Mərkəzi

Kart əməliyyatlarının idarə olunması.

# Niyə Rəqəmsal? Əsas Üstünlüklər



## 24/7 ÇIXIŞ

Bank xidmətlərinə  
fasiləsiz, istənilən an çıxış  
imkanı.



## Sürət

Əməliyyatların anında,  
gecikmədən həyata  
keçirilməsi.



## Qənaət

Vaxta və fiziki resurslara  
tam qənaət.



## Əlçatanlıq

Xidmətlərin hər yerdə və hər  
kəs üçün daha əlçatan olması.

Bu səbəbdən son illərdə bank əməliyyatlarının böyük hissəsi məhz rəqəmsal kanallara keçmişdir.

# Toxun, Oxut, Ödə: Müasir Ödəniş Ekosistemi

## Mobil Sistemlər



Kart məlumatlarını telefona əlavə edərək daxili rəqəmsal pul kisəsindən istifadə.

## QR Ödənişlər



Xüsusilə elektron ticarətdə istifadə olunan, kameranın QR kodu oxuması ilə anında ödəniş

## NFC Ödənişlər



Kartı və ya telefonu terminala sadəcə yaxınlaşdırmaqla sürətli ödəniş.

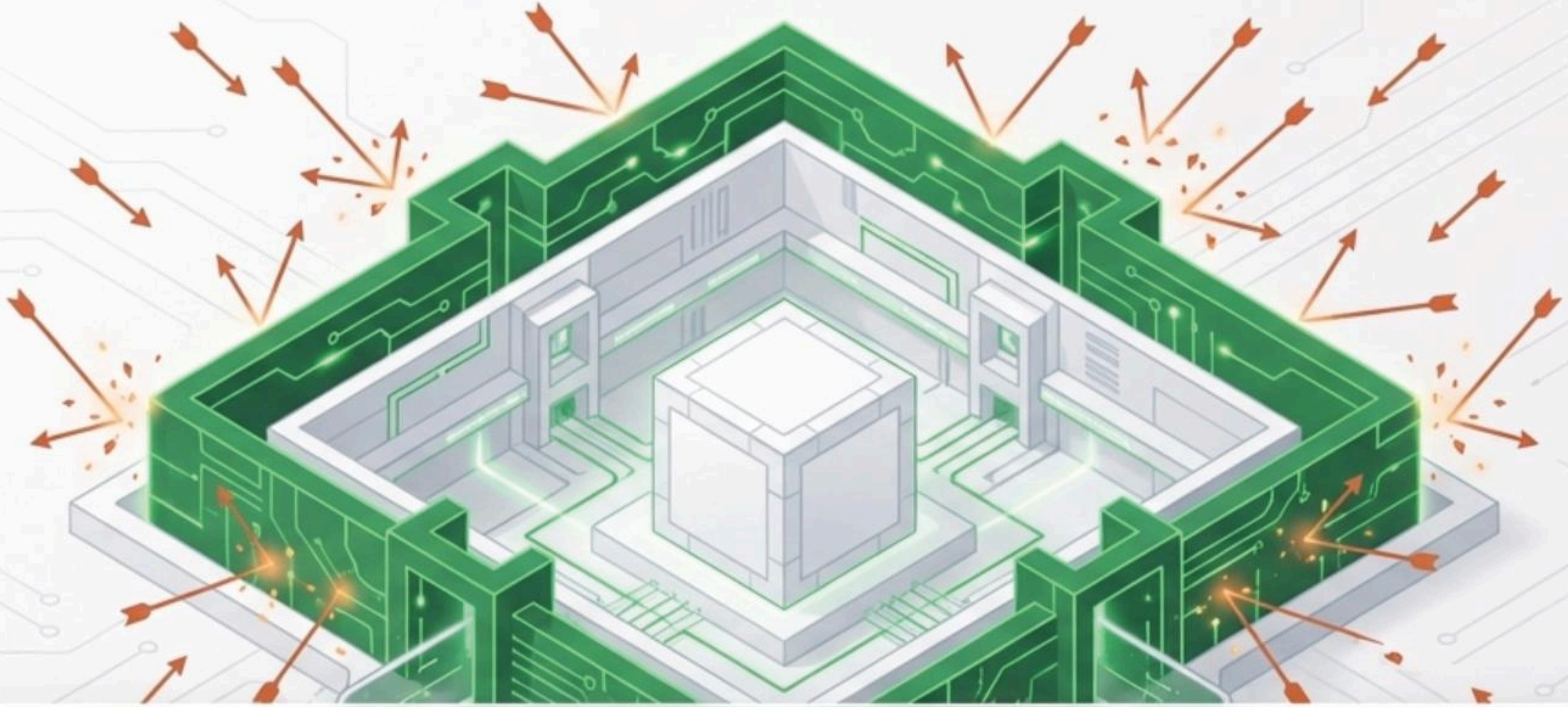


# Rəqəmsal Tərəzi: Güc və Məsuliyyət






Rəqəmsal bank xidmətlərinin inkişafı fırldaqçılıq risklərini də artırır. Əsl maliyyə savadlılığı həm texnologiyadan istifadə etməyi, həm də ondan qorunmağı tələb edir.

# Kibertəhlükəsizlik Nədir?



Rəqəmsal mühitdə şəxsi məlumatların və maliyyə əməliyyatlarının qorunmasını təmin edən təhlükəsizlik tədbirlərinin məcmusudur.

# Təhlükə Radarı: Fırıldaqçılığın Növləri

Növ	Vektor	Metod	Məqsəd
<b>Fişinq (Phishing)</b> 	E-poçt / Veb-sayt	Bank adından göndərilən saxta elektron məktublar və ya saxta səhifələr.	Şəxsi məlumatların əldə edilməsi.
<b>Smishing</b> 	SMS	Telefonunuza gələn saxta mesajlar.	Linkə kliklədərək bank məlumatlarını çəkmək.
<b>Vishing</b> 	Səsli Zəng	Özünü bank əməkdaşı kimi təqdim edən zənglər.	Müştəridən birbaşa kart məlumatlarını tələb etmək.

# Hücümün Anatomiyası: Real Ssenari



## 1. Qarmaq

Şəxs telefonuna bank adından saxta SMS alır.



## 2. Yem

Mesajda kart məlumatlarını təsdiqləmək bəhanəsi ilə şübhəli bir linkə daxil olmaq tələb olunur.



## 3. Tələ

İstifadəçi linkə daxil olaraq şifrə və ya kart məlumatlarını saxta sistemə daxil edir.



## 4. Nəticə

Fırıldaqqılar bu məlumatlardan istifadə edərək hesabdan pul vəsaitini oğurlayır.

Şübhəli mesajlara və linklərə qarşı daim diqqətli olun — tələyə düşməyin tək yolu məlumatı daxil etməkdir.

# Təhlükəsizlik Qalxanı: 5 Qızıl Qayda



## Məxfilik

Kart məlumatlarını və PIN kodunu heç kimlə paylaşmayın.

## Sayıqlıq

Şübhəli mesaj və naməlum linklərə əsla daxil olmayın.

## Rəsmilik

Bank tətbiqlərini yalnız rəsmi mənbələrdən yükləyin.

## Nəzarət

Hesabınızdakı əməliyyat tarixçəsini müntəzəm yoxlayın.

## Güc

Yalnız güclü və təxmin edilməsi çətin olan təhlükəsiz şifrələrdən istifadə edin.

Bu qaydalar maliyyə məlumatlarınızın toxunulmazlığını təmin edir.

# Nəticə: Savadlı İstifadəçi, Təhlükəsiz Maliyyə



Rəqəmsal bankçılıq müasir maliyyə sisteminin vacib, rahat və əlçatan hissəsidir. Lakin bu sistemin qapısı texnologiya ilə açılırsa, kilidi sizin rəqəmsal savadlılığınızdır.

Maliyyə savadlılığının ən vacib elementi kibertəhlükəsizlik barədə məlumatlı olmaq və şəxsi məlumatları qoruya bilməkdir. Rəqəmsal dünyada ən güclü antivirus — sizin öz biliklərinizdir.