



**B**ugünkü dünyada smartfonlarımız həyatımızın mərkəzindədir - mesajlaşmadan tutmuş bank əməliyyatlarına, foto və sənədlər saxlamağa qədər hər şey telefonlarımızda olur. Lakin hər mobil yaddaş təhlükəsiz deyil. Telefonlara düzgün yanaşmadıqda şəxsi və maliyyə məlumatlarımız riskə atılmış oluruq - bu məlumatlar oğurlana, sui-istifadə edilə, şəxsiyyət oğurluğu və maliyyə fırıldaqçalarına yol açə bilər. SİA mövzu ilə bağlı araşdırma edib.

## Telefonunuzda saxlandıqda risk yaradan əsas məlumatlar

Şəxsi sənədlərin şəkilləri  
Pasport, şəxsiyyət vəsiqəsi, sürücülük

vəsiqəsi, VÖEN, bank kartının şəklə kimi sənədlər çox kritik məlumatlar daşıyır (ad, doğum tarixi, nömrə və s.).

Bu cür şəkillər hakerlər və fırıldaqçılar üçün "xəzinə"dir - onlar bu məlumatlarla kimliyinizlə saxta hesablar açə, bank əməliyyatları həyata keçirə, kreditlər götürə bilərlər. Belə sənədləri telefonda çəkmək belə təhlükəli hesab edilir.

## Maliyyə məlumatları və bank PIN-ləri

Bank hesab nömrələri, kart nömrələri, PIN-lər, mobil bank tətbiqlərində açıq giriş məlumatları - bunlar telefondakı əsas hədəflərdən biridir.

Əgər telefonunuz kimsənin əlinə keçərsə, bu məlumatlar vasitəsilə hesabınıza asanlıqla girilə bilər.

Təvsiyə: PIN- və şifrə kimi həssas məlu-

# Cibdə "bomba": şəxsi məlumatlar smartfonda niyə təhlükəlidir?

matları şifrə meneceri tətbiqlərində saxlayın (bu tətbiqlər əsas təhlükəsizlik standartlarına cavab verir).

## Məhrəm və intim fotoşəkillər

Telefon itdikdə və ya zərərli proqram daxil olduqda bu şəkillər qara poçt və şantaj üçün istifadə oluna bilər. Bu tip şəkillər yalnız telefon yaddaşında deyil - buludda da saxlanarkən təhlükə yarada bilər.

## Şifrələr, parollar və hesab məlumatları

Simsiz şəkildə yazılmış şifrələr (yaddaşda not kimi saxlanmış) çox risklidir - kimse cihazınıza girə bilsə, bu şifrələrlə bütün onlayn hesablarınıza daxil ola bilər.

Şifrələri telefona yazmaq əvəzinə, güclü parol meneceri istifadə etmək daha təhlükəsizdir.

## İş və korporativ məlumatlar

Əgər şəxsi telefonunuzda işə aid məxfi sənədlər, layihələr və ya məlumatlar varsa, onların sızması həm sizin, həm də iş yerinizin zərərinə ola bilər.

## Ünvan, əlaqə siyahısı və şəxsi qeyd məlumatları

Telefon kontaktlarınızda ev ünvanları və ailə üzvlərinin məlumatları varsa, bu məlumatlar fırıldaqçılar tərəfindən sosial mühəndislik (phishing) hücumları üçün istifadə edil-

lə bilər.

## Telefonun özündə və buludda saxlanma - risk necə yaranır?

Telefonun itməsi və oğurlanması: Cihaz fiziki olaraq əldən çıxanda içindəki məlumatlar da təhlükə altındadır - xüsusilə şifrə və biometrik yoxlama zəifdirsə.

Zərərli proqramlar və hacker hücumları: Malware və spyware tətbiqləri telefonunuza gizli yüklənərək foto, sənəd və mesajlarınıza giriş əldə edə bilər.

## Təhlükəsizliyiniz üçün tövsiyələr

- Telefon parolunu güclü və unikal edin (rəqəm + hərf).
- 2-faktorlu təsdiqi aktiv edin (SMS və ya autentifikator tətbiqi).
- Mümkünsə şifrələnmiş qovluqlar və ya təhlükəsizlik tətbiqlərindən istifadə edin.
- Sənədləri telefonda deyil - fiziki qovluqda və ya təhlükəsiz buludda saxlayın.
- Şübhəli linklərə klik etməyin və qeyri-rəsmi tətbiqlərdən uzaq durun.

Smartfon həyatımızı asanlaşdırır, amma onun yaddaşında saxladığımız bəzi məlumatlar şəxsi və maliyyə təhlükəsizliyi üçün böyük risk yarada bilər. Sənəd şəkillərindən tutmuş şifrələrə qədər bütün bu məlumatları ehtiyatla idarə etmək və lazım olduqda yığcam, təhlükəsizliklə qorunan üsullardan istifadə etmək vacibdir.